2004

MAC-layer approaches for security and performance enhancement in IEEE 802.11

Hao-Li Wang
Iowa State University

MAC-layer approaches for security and performance enhancement in IEEE 802.11

by

Hao-Li Wang

A dissertation submitted to the graduate faculty
in partial fulfillment of the requirements for the degree of
DOCTOR OF PHILOSOPHY

Major: Computer Engineering

Program of Study Committee:
Doug Jacobson, Major Professor
James Davis
Lu Ruan
Manimaran Govindarasu
Yong Guan

Iowa State University

Ames, Iowa

2004

Graduate College
Iowa State University

This is to certify that the doctoral thesis of

Hao-Li Wang

has met the thesis requirements of Iowa State University

Signature was redacted for privacy.

Major Professor

Signature was redacted for privacy.

For the Major Program

DEDICATION

To my parents

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Over the past few years, wireless networks are becoming increasingly popular. The dominant question facing the wireless network today is: how can the network meet the needs of various users and applications? Two basic and primary needs for users are efficiency and security. To deal with these two concerns, this dissertation investigates the two areas and proposes four MAC-level approaches for security and performance enhancement in IEEE 802.11.

In the first part, we propose three MAC-level approaches to improve the throughput performance in wireless LANs, i.e., the Freeze Counter scheme (FC), the Dynamically Adaptive Retransmission (DAR), and the Quick Acknowledgement (QA) scheme. The Freeze Counter scheme is an adaptive error recovery mechanism in 802.11, which can perform different actions according to the reasons for frame losses. With the differentiation functionality, the non-collision error frames could be rapidly retransmitted without the binary exponential backoff procedure. Next, Dynamically Adaptive Retransmission scheme is an enhanced feedback scheme in 802.11, in which the CTS frames carry additional information concerning the previous data delivery without violating the 802.11 MAC layer semantics. Thirdly, we propose a Quick Acknowledgement (QA) scheme as a replacement for positive acknowledgement in IEEE 802.11. QA is an adaptation of an ATM-based protocol, the Service Specific Connection Oriented Protocol (SSCOP), for use as a link layer protocol in wireless LANs. By using similar concepts as selective ACK and negative ACK, the proposed protocol solves the inefficiency problem of positive ACK in 802.11, and therefore it performs better than 802.11 MAC.

In the second part, we propose a lightweight statistical authentication protocol for wireless networks. With more and more applications on wireless networks, new concerns are raised when it comes to security issues. Authentication service particularly becomes one of the basic but necessary security measures for wireless applications. However, traditional authentication protocols for wired networks do not work well in a wireless environment due to unique characteristics, such as error-prone wireless transmission medium, node mobility, and power conservation constraints of wireless devices. To meet this target, we propose a lightweight statistical authentication protocol for wireless networks, namely *Shepherd*. To solve the inherent out-of-sync problem with Shepherd protocol, we develop three synchronization schemes with their statistical methods. In Shepherd, the legitimacy of a mobile node is determined by continuously checking a series of random authentication bits where each bit in this stream is piggybacked by a packet. Such an authentication bit stream is generated by both mobile node and access point using the same random number generator under the same shared seed as a key. The complete evaluation and analysis of all proposed approaches have been discussed. We also show that the proposed approaches are practical for implementation in 802.11 to improve the security and performance of wireless LANs.

CHAPTER 1. INTRODUCTION

1.1 IEEE 802.11

Although the original concept of wireless LANs has existed since late 1970s , the WLAN technology started catching people's eyes in late 1990s. Today, it has become a ubiquitous networking technology. The recent explosive growth of this technology can be attributed to many factors, for example, technological advances in error correcting codes, modulation techniques, processing power on network interfaces, availability of unlicensed radio spectrum, and the need for wireless connectivity and mobility.

In WLANs, the medium access control (MAC) protocol is the main element that manages congestion and error situations that may frequently occur in a lossy wireless link. In this dissertation, we focus on the efficiency of the IEEE 802.11 MAC protocol.

1.2 Dissertation Overview

In this dissertation, we propose approaches to achieve a secure and efficient wireless LAN. There are three approaches to enhance the IEEE 802.11 MAC protocol and one for the wireless security, i.e. the Freeze Counter scheme (FC) , the Dynamically Adaptive Retransmission (DAR), the Quick Acknowledgement (QA) scheme, and the Shepherd protocol.

In Chapter 2, we first give background knowledge of 802.11 MAC protocol. Then, we point out three problems causing the inefficiency in 802.11. Finally, we briefly present our solutions to these problems.

In Chapter 3, we first introduce the redundant backoff (RB) problem existing in IEEE 802.11. The main reason is the error recovery mechanism in 802.11 deems all error cases as collisions and involves binary exponential backoff to avoid collisions. However, in case of errors due to attenuation, fading, or interfering, binary exponential backoff will not help but cause extra frame delay. For the RB problem, we propose the Freeze Counter (FC) scheme, an adaptive error recovery mechanism, which can efficiently retransmit lost frames by effectively differentiating the collisions from other types of wireless errors.

In Chapter 4, we propose a dynamic adaptive retransmission (DAR) scheme to deal with redundant retransmission (RR) problem. In IEEE 802.11, a positive acknowledgement informs sender of successful arrivals of data frames. However unacknowledged frames could result from either unsuccessful transmissions of data frames or positive ACK frame losses. The sender will simply retransmit any unacknowledged data frame, which is actually redundant in case of positive ACK frame losses. The idea of DAR is to clearly differentiate the reasons for frame loss by using modified CTS frames containing additional information on transmission status of unacknowledged frames. Based on that information, sender is able to dynamically determine whether to retransmit or not.

In Chapter 5, we first explain why positive acknowledgement in IEEE 802.11 is inefficient. IEEE 802.11 provides fast recovery from frame losses using a rapid link level positive acknowledgment scheme. However, the adoption of positive acknowledgment causes frequent ACK timeout at high bit-error rate and leads to inefficient frame transmission. To improve efficiency of the acknowledgments mechanism in IEEE 802.11, we propose a novel link layer protocol for wireless LANs. The proposed protocol is an adaptation of an ATM-based protocol, the Service Specific Connection Oriented Protocol (SSCOP), for use as a link layer protocol in wireless LANs. The protocol uses much less bandwidth on the return path and hence enhances the performance of data frame transmission.

In the wireless security part , we propose a lightweight authentication protocol in Chapter 6. With the increasing performance and dropping price of wireless networking equipment, wireless networking has revolutionized the way people work and play. Wi-Fi hot spots popping up all over the country provide a convenient means of internet connectivity. For the ISPs of hot spots, authentication and accounting have been recognized as two most crucial concerns. For authentication, IETF PANA[1] WG, is working on a transport protocol for authenticating IP hosts for

[1] PANA stands for Protocol for Carrying Authentication for Network Access

network access. However, PANA does not provide access control and per-packet authentication, which are desirable in accounting and access control. Instead of using high-overhead crypto-based mechanisms, such as IPSec or 802.11i, we propose a lightweight statistical authentication protocol, namely *Shepherd*[2]. Our analytical results show that Shepherd performs well in terms of computational and communication cost, synchronization efficiency, and protocol operation secrecy. Finally, we conclude this proposal in Section 7.

[2] The access point (AP) in a wireless network authenticates the mobile nodes as a Shepherd discriminates among similar sheep according to their characteristics.

CHAPTER 2. BACKGROUND WORK AND THE PROBLEM

2.1 MAC Protocol in IEEE 802.11

IEEE 802.11b is a standard for Medium Access Control (MAC) and Physical Layer (PHY) specifications for wireless LANs, promoted by the Institute of Electrical and Electronics Engineers. With the increasing importance of Wireless technologies in the LAN environment and the IEEE 802.11 is the most mature technology to date. In this section, we will only describe some components in the 802.11 MAC protocol, which will be used in latter chapters. The details of 802.11 MAC can be found in [38] [74].

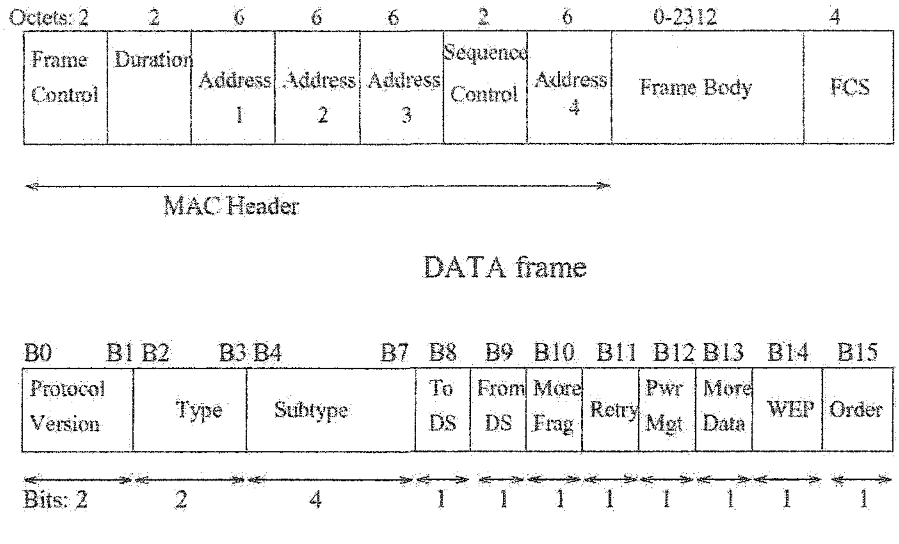
2.1.1 MAC Frame Format in IEEE 802.11

Three types of frames are defined in the IEEE 802.11 standard [38]. They are management frame, control frame, and data frame. The general format of an 802.11 MAC frame is represented in Fig.2.1. The type and subtype values in the frame control field of a frame determine the type of the frame. There are some reserved values in the field, not defined in the current standard.

2.2 Target Problems in 802.11 MAC

2.2.1 Redundant Backoff Problem

Previous works found that the 802.11 standard protocol performs inefficiently, and that an appropriate modification on error recovery mechanism can help the IEEE 802.11 protocol achieve to its optimal behavior. One potential flaw in the 802.11 error recovery mechanism is that 802.11 deems all error cases as collisions and involves binary exponential backoff to avoid collisions. In reality, there are many reasons leading to high error rate over wireless links, such as attenuation, fading, interfering active radiation sources, or collision with another transmission. Nevertheless,



DATA frame

Frame Control Field

Figure 2.1 802.11 MAC frame format and control field

it is difficult for a station to know the real reason for frame losses, and to differentiate wireless errors in the 802.11 MAC layer because no cross-layer mechanism or information exchange between PHY and MAC layer. Accordingly, at most, a station can estimate the knowledge and use it to perform the tuning. Obviously, the more accurately a station can estimate the knowledge, the more efficiently a station can perform the tuning. It appears that effectively differentiating wireless errors can reduce the times of redundant backoff, and therefore help to improve the performance in 802.11.

We look at a simple example to explain this problem. Let only two mobile hosts exist in a wireless network and one sends data flow to the other through a lossy wireless link. In other words, not all errors that occur are due to collisions. Unfortunately, whenever a error occurs, the sender will recover the error by binary exponential backoff, that is, to double the contention window (CW), because all errors are deemed as collisions in 802.11. Obviously, unnecessarily increasing the CW to avoid collisions degrades throughput performance. If the sender can be aware that the errors are due to other reasons, such as fading or interference, other error recovery mechanisms, such as keeping CW unchanged or faster retransmission, are appropriate.

2.2.2 Redundant Retransmission Problem

Unlike the Ethernet IEEE 802.3 Standard, which uses CSMA/CD to manipulate link layer frames, the IEEE 802.11 standard uses CSMA/CA to avoid transmission collision, and uses positive acknowledgement to inform the sender of successful delivery of data frames. To address the hidden node problem in wireless networks, the IEEE 802.11 standard has two special control frames, Request To Send (RTS) and Clear To Send (CTS) frames. When the sender fails to receive the ACK frame from the receiver upon expiration of the timer, which is deemed an unsuccessful delivery in the current 802.11 standard, the sender simply retransmits the data frame. But limitations exist. Though the positive ACK scheme is helpful in confirming the successful delivery of data frames, it may invoke unnecessary retransmissions. Particularly, in case of the ACK frame loss after a successful data frame delivery, the sender is unable to differentiate it from unsuccessful data delivery and will simply invoke the retransmission scheme. Thus the receiver will get redundant retransmitted frames, which compromises the transmission efficiency. Hence, the goal of our proposed scheme is to improve the efficiency of link layer retransmission by avoiding this redundancy.

Currently, two types of retransmission are applied for recovery of lost packets in lossy networks. Retransmission mechanisms exist in both the TCP layer and the link layer. TCP retransmission is a part of TCP congestion control mechanisms. When three duplicate ACKs are received (Fast Retransmit), or timeout occurs (Slow Start), the sender retransmits the corresponding TCP packet. On the other hand, when the link layer timer to receive an ACK[1] expires, a link layer retransmission will be triggered. Compared with TCP retransmission, link layer retransmission adapts quickly to link characteristics due to shorter timeout periods. Moreover, since the length of a frame is much shorter than that of a TCP packet, retransmission in the link layer costs less than that in TCP. In the last five years many researchers have been focusing on improving TCP retransmissions to solve wireless TCP problems [10][61][60]. Balakrishnan (1995) proposed the snoop TCP scheme, a TCP-aware link layer protocol using link layer retransmission from a base station [11]. Extensions of Link Layer retransmission are also used

[1] This ACK is an acknowledgement frame in link layer.

in research on QoS over wireless LANs [25]. To optimize the retransmission scheme in the link layer to achieve high transmission efficiency in higher layers is an important issue. However, no research has been done on link layer retransmission to improve the efficiency of the basic frame exchange protocol. In Chapter 3, we proposed an enhanced link layer retransmission scheme based on the 802.11 standard to make transmission more effective.

2.2.3 Inefficient Acknowledgement Problem

Due to the high loss rate experienced over wireless links as well as the presence of hidden terminals, the IEEE 802.11 standard uses a positive acknowledgement scheme. In the IEEE 802.11 protocol [38], the reception of data frames requires the receiving host to respond with an acknowledgment, generally an ACK frame, if the received frame is correct. Lack of reception of an expected ACK frame indicates to the source host that an error has occurred. This technique is known as positive acknowledgment. The main advantage of positive acknowledgement is high reliability since the sender can quickly detect the occurrence of any transmission error.

Fig.2.2 shows an example of positive acknowledgement. The receiver returns an acknowledgment frame, ACK, to the transmitter, immediately upon the successful completion of data reception. When the data frame is lost, the transmitter waits for the ACK frame for a period of ACK_Timeout, and then retransmits the lost data frame. Although the positive acknowledgment scheme is reliable and simple, it leads to inefficient frame transmission. Since each data frame requires one ACK, the large traffic overhead of ACK transmission wastes the scarce bandwidth of wireless networks. However, at a low error rate, most of the frame transmissions are correct and the positive acknowledgment scheme is inefficient. In this case, if the negative acknowledgement scheme is used, the receiver only requests the retransmission of the lost frames. Thus, the amount of ACK traffic can be reduced significantly. To solve the inefficiency problem of positive acknowledgement, this section proposes an idea of an adaptation of the Service Specific Connection Oriented Protocol (SSCOP), for use as a link layer protocol in wireless LANs.

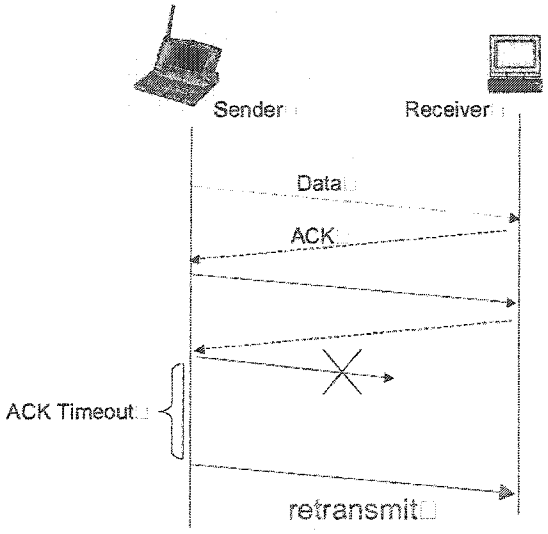


Figure 2.2 Positive acknowledgement scheme

2.3 Proposed Solutions

2.3.1 FC: Freeze Counter Scheme

There are many reasons leading to high error rate over wireless links, such as attenuation, fading, interfering active radiation sources, or collision with another transmission. Unfortunately, the error recovery mechanism in 802.11 deems all error cases as collisions and involves binary exponential backoff to avoid collisions. However, in the case of errors due to attenuation, fading, or interfering, binary exponential backoff cannot help but cause extra frame delay.

We propose a Freeze Counter (FC) scheme, an adaptive error recovery mechanism, to efficiently retransmit lost frames by differentiating the collisions from other types of wireless errors[90]. The performance of the IEEE 802.11 protocol, with and without the FC mechanism, is investigated through simulation. Simulation results show that differentiating wireless errors can be used to prevent unnecessary delay and improve throughput performance. It also indicates that our mechanism is very effective, robust, and has traffic differentiation potentialities.

2.3.2 DAR: Dynamically Adaptive Retransmission

In the IEEE 802.11 WLAN standard, a positive acknowledgement informs the sender of successful arrivals of data frames. However unacknowledged frames could result from either unsuccessful delivery of data frames or positive ACK frame losses. Therefore the sender simply retransmits the unacknowledged data frame, which may cause redundant retransmission in case of positive ACK frame losses. In Chapter 4, we propose an enhanced retransmission scheme that we call Dynamically Adaptive Retransmission (DAR), which uses modified RTS and CTS frames containing additional information on transmission status of unacknowledged frames[92]. Based on that information, the sender is able to dynamically determine whether to retransmit or not. Experiments and analysis show that our proposed scheme efficiently decreases redundant retransmission by clearly differentiating the reasons for frame loss.

2.3.3 QA: Quick Acknowledgement Scheme

The IEEE 802.11 standard provides fast recovery from frame losses using a rapid link level positive acknowledgment scheme. However, the adoption of positive acknowledgment leads to inefficient frame transmission. Therefore we propose a novel link layer protocol for wireless LANs[94]. The proposed protocol is an adaptation of an ATM-based protocol, the Service Specific Connection Oriented Protocol (SSCOP), for use as a link layer protocol in wireless LANs. We evaluate and compare the performance of the protocol with IEEE 802.11. The results show that the proposed protocol has a much better performance in an error-prone wireless environment, even when the bit error rate is severely degraded.

2.3.4 Shepherd

Since traditional authentication protocols for wired networks do not work well in a wireless environment, in Chapter 6, we propose a lightweight statistical authentication protocol, namely *Shepherd*[95]. In Shepherd, the legitimacy of a mobile node is determined by continuously checking a series of random authentication bits where each bit in this stream is piggybacked by a packet. Such an authentication bit stream is generated by both mobile node and access point using the same random number generator under the same shared seed as a key. We analyze this protocol under three synchronization schemes. Our analytical results show that this protocol performs well in terms of computational and communication cost, synchronization efficiency, and protocol operation secrecy. We also show that this new protocol is practical for implementation in wireless LANs.

CHAPTER 3. FC: FREEZE COUNTER SCHEME

3.1 Introduction

The explosive growth in the number of mobile device users and Internet services has been accompanied by the increasing number of wireless technologies. Wireless transmissions are subject to interference from outside sources, absorption, scattering, fading, and interference. This can result in very high error rates. Moreover, since conditions change over time (due to mobility or intermittent interference source), the error environment will also change. Such a variable, high error environment can bring problems for Medium Access Control (MAC)-layer protocols and higher-layer applications [34].

One big obstacle to compromise the good performance is non-negligible bit-error rates (BER)[55]. To make matters worse, error rates can be highly variable due to changes in the wireless environments. The networking community has explored a broad spectrum of solutions to deal with wireless error environments. They range from link layer solutions [34][24] to transport protocol [55][10].

Previous work have showed that the standard protocol can be very inefficient and that an appropriate tuning of its backoff algorithm can make the IEEE 802.11 protocol close to its optimal behavior. To perform this tuning, a station must have exact knowledge of the network contention level, such as the reasons for frame losses or the number of active nodes in the network. Unfortunately, this information is not obtainable because there is no cross-layer mechanism or information exchange between PHY and MAC layer. Accordingly, at most, a station can estimate the knowledge and use it to perform the tuning. Obviously, the more accurately a station can estimate the knowledge, the more efficiently a station can perform the tuning. We present a distributed estimation mechanism, called Freeze Counter (FC) scheme, for contention control in IEEE 802.11 Wireless LANs. The scheme measures the network contention level by using a simple estimate, the Freeze Counter, which can be easily obtained by exploiting information that is already available in the standard protocol. The FC scheme is an adaptive error recovery mechanism. That is, based on the estimated knowledge accuracy, FC can efficiently retransmit lost frames by differentiating the collisions from other types of wireless errors. Since our scheme extends from the DCF of 802.11, we will sketch CSMA/CA in the next section, and then go into the proposed scheme.

3.2 CSMA/CA

The CSMA/CA is a contention-based multiple access technology that requires each station to sense the medium to be idle for a period of time before sending each frame. The period of time is called inter-frame space (IFS) whose length is related to the frame priority. The level of frame priorities are classified as Short IFS (SIFS), PCF IFS (PIFS), DCF IFS (DIFS) and Extended IFS (EIFS), which correspond to, for example, ACK frames, PCF control frames, data frames, and retransmission frames, respectively. More details about the frame priority can be referred to [38]. In 802.11, the backoff procedure is used for collision avoidance, where each station waits for a backoff time (a random time interval) before its frame transmission.

3.3 Freeze Counter Scheme

In this section we first introduce the idea of differentiating between collision and other types of errors over WLANs, and then discuss the design of the proposed solution, the Freeze Counter (FC) scheme.

3.3.1 Main Idea

The main idea of the FC scheme is to use wireless traffic information collected by a mobile host in the backoff procedure to effectively differentiate wireless errors. Before sending each frame, a mobile host waits for the IFS and a backoff time. The station will decrease its backoff time counter by one if the medium is sensed idle for a slot-time and freeze the backoff time counter when the medium is busy. In other words, many freezes may happen in a backoff procedure. At a higher traffic load, the occurrences of freezes can be observed more frequently. When the backoff time is decreased to zero, the station transmits its frame immediately. If another host sends at the same time, a collision occurs. At a higher traffic load, the probability of collision is higher [67]. Hence conclusively the freeze counter (FC) could act as an indicator of probability of collisions.

3.3.2 Freeze Counter

Current 802.11 cannot differentiate collisions from various types of wireless errors and uses binary exponential backoff for all error types, which unnecessarily increases CW. Our scheme differentiates wireless errors according to the frame's freeze counter, which is calculated by the mobile host in the backoff procedure before sending each frame. Whenever an error occurs, the freeze counter is used to estimate probability of collision and to help differentiate wireless errors. Specifically, when FC is larger than *FCThresholds*, the error is estimated to be due to a collision, and binary exponential backoff is triggered. Otherwise, most likely the error is due to a fading or interference and the sender keeps CW constant. The procedure of the FC scheme is presented in Fig.3.1

3.3.3 An Example of the FC Scheme

An example of multiple mobile hosts is given to illustrate the calculated FC value in the backoff procedure. As shown in Fig.3.2, the backoff timer of station B freezes three times due to the transmission of station C, D, and E in B's backoff procedure. Thus, the freeze counter of the station B is 3. The values of FC of station A to E are (0,3,0,1,1).

3.4 Experiment and Analysis

3.4.1 Simulation Environment and Parameters

We used Network Simulator (NS-2) [48] to simulate a wireless network that consists of multiple sender-receiver pairs connected over a lossy link with bandwidth 10Mbps. Five experiments

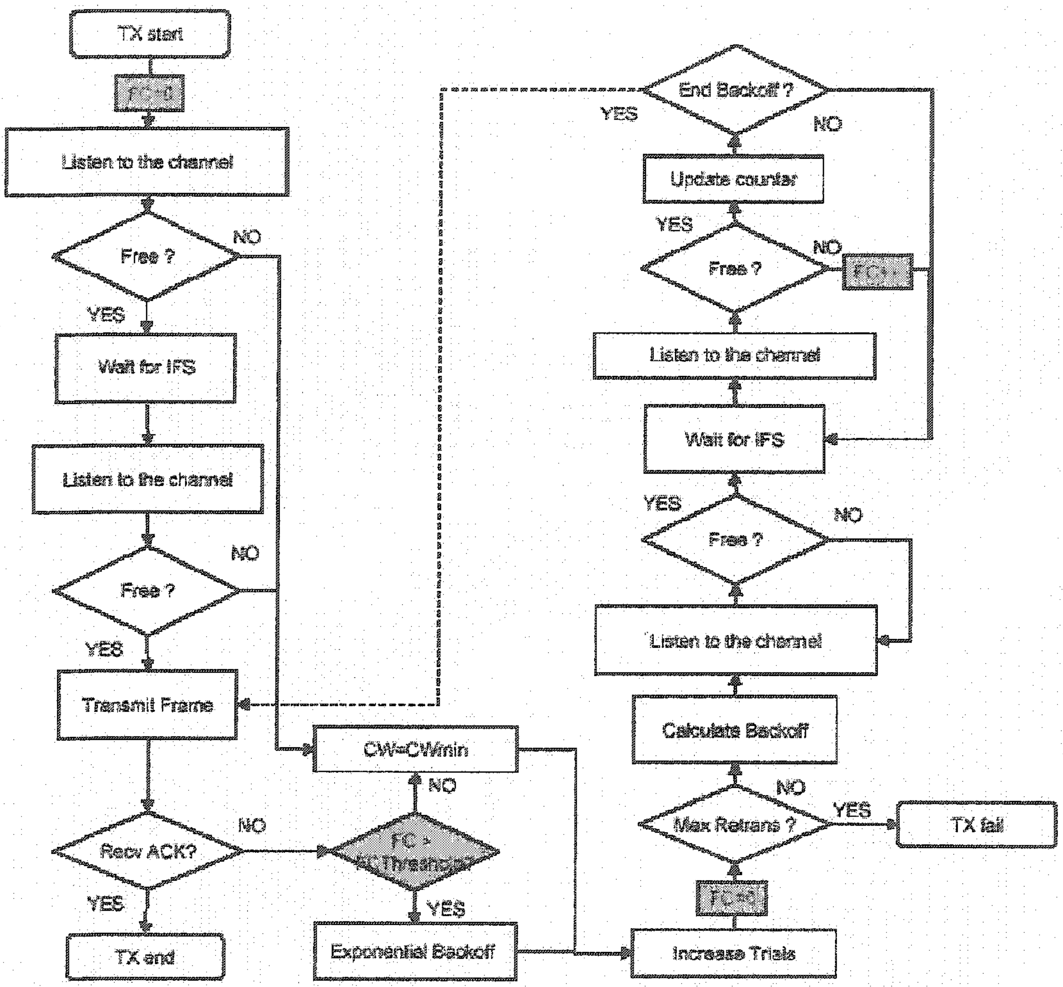


Figure 3.1 Procedure of Freeze Counter scheme

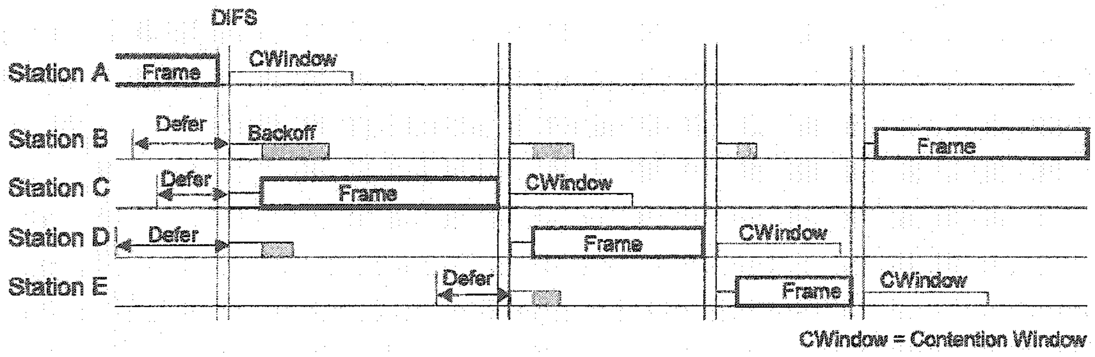


Figure 3.2 An example of 5 stations using the FC scheme

were performed to measure the performance of data transfer over wireless link with the FC scheme and the IEEE 802.11 standard. The FC scheme had been implemented using C++ in the NS-2 package. Specifically, mac-802_11.cc and mac-802_11.h , the two files involved in the 802.11 package in NS-2, were altered to favor the binary exponential backoff mechanism, and the operations of freeze counter were introduced.

In order to measure the performance of the protocols under controlled conditions, we generated errors on the lossy link using a two-state error model, including both error-free and error states[68]. In particular, each state has a random variable determining the length of each state. We investigated the performance of these protocols across a range of frame loss rates from 0.1% to 10%. At a high error rate, there were several occasions when multiple frames were lost in close succession or when both data and the first retransmission data frame were lost.

All the other parameters in the simulation models, listed in the Table 3.1, are referenced from [67].

3.5 Enhancements to the IEEE 802.11 Standard

3.5.1 Throughput Performance

In experiment 1, we examined the flaws of the current 802.11 standard with a special evaluation case. In this case, only two mobile nodes existed in the wireless network and one node

Table 3.1 Parameters used throughout all simulations parameter value

CW_{min}	31
CW_{max}	1023
Frame loss rate	variable: 0 to 0.1
Frame size	512 Bytes
SIFS	$10\mu s$
DIFS	$90\mu s$
Slot time	$20\mu s$
Number of mobile nodes	variable: 6 or 20
Number of flows	variable: 3 or 10
Flow rate	800kbps or 1200kbps
Medium capacity	10Mbpse
$FCThresholds$	variable: 3,6,9
RTS Threshold	300

sent one UDP flow with CBR[1] equal to 1200kbs to the other. Thus, no collision would occur in this scenario. The results of simulations are presented in Fig.3.3, showing the FC scheme achieved better throughput performance than 802.11. The reason of the improvement was that CW was fixed at CW_{min} whenever errors occurred. Accordingly, at a higher frame error rate, the improvement was even more significant, as shown in Fig.3.3. Because more error frames were misinterpreted by 802.11 as collisions and they were handled correctly in the FC scheme.

In experiment 2, a common case was used and the traffic pattern was closer to real network behavior. In this experiment, 6 mobile nodes existed in the wireless network. 3 mobile hosts sent 3 UDP flows at CBR equal to 800kbs to the other 3. In Fig.3.4, the FC scheme still has better throughput performance than 802.11 with increasing error rate. Fig.3.5 shows the improvement of the FC scheme increases as the error rate rase. For example, when the frame error rate is 5%, the improvement is about 2.5%.

In experiment 3, we chose a larger number of mobile hosts than that in experiment 2 and results were compared. Similarly, the FC scheme had better throughput performance than 802.11 with increasing error rate, as shown in Fig.3.6. Fig.3.7 shows that the improvement of

[1] CBR stands for constant bit rate.

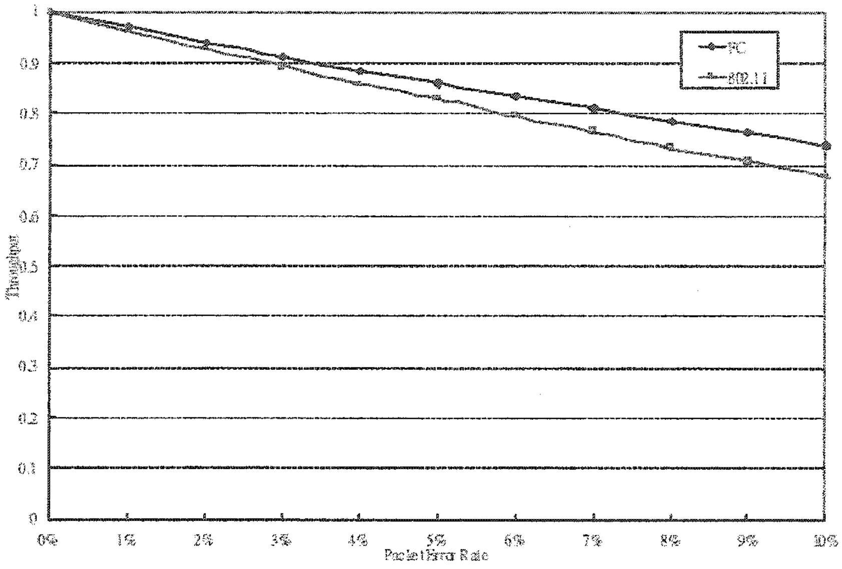


Figure 3.3 Throughput versus frame error rate for 2 stations

the FC scheme increases as error rate increased. For example, at a frame error rate of 5%, the improvement is about 2.3%.

These results suggested that the FC scheme always had a better throughput performance than 802.11, regardless of the number of mobile nodes existed. Furthermore, the improvement of the FC scheme was even higher at higher error rates because of the increased ability of the FC scheme to differentiate non-collision wireless errors.

In experiment 4, we explored the effect on different *FCThreshold* values. We tested 3, 6, and 9 as *FCThresholds*in the environment of experiment 2. In Fig.3.8, the differences between three cases were indistinct, that is, the influence of *FCThresholds* value was trivial in an environment of a small number of mobile nodes.

In experiment 5, a larger number of mobile hosts than that in experiment 4 was chosen and results were compared. In Fig.3.9, when the error rate was lower than 2%, the differences between the three cases were very small. When the error rate was larger than 2%, the curve of $FCThreshold = 9$ dropped faster indicating a lower throughput performance than the other 2 cases. When the error rate was larger than 5%, the curve of $FCThreshold = 6$ dropped even faster indicating a much lower throughput than the case of $FCThreshold = 3$. In summary, at

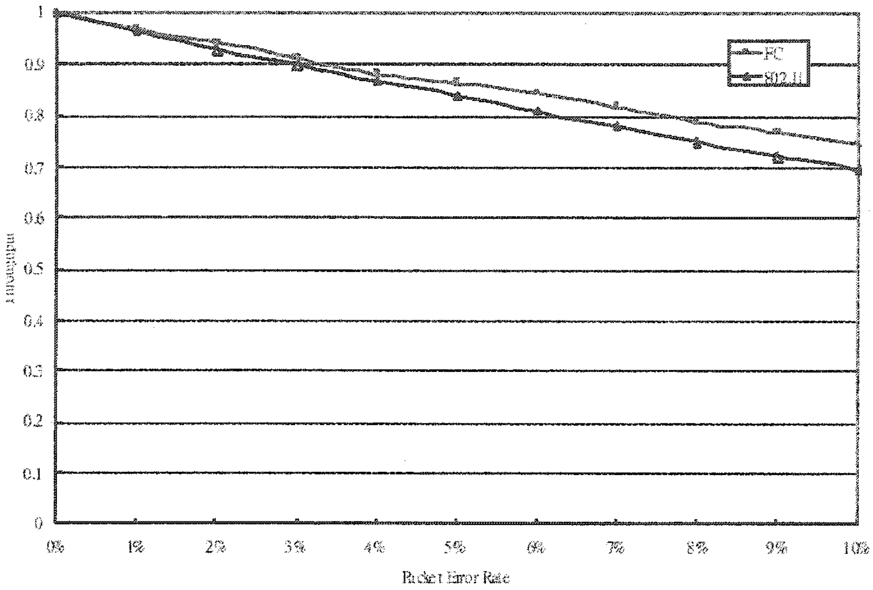


Figure 3.4 Throughput versus frame error rate for 6 stations

a low error rate, the differences between the three cases were small. While at a high error rate, the smallest *FCThresholds* had best throughput performance.

3.6 Summary

In this chapter, we proposed an adaptive error recovery mechanism, which can perform different actions according to the reasons for frame losses. With the differentiation function, the non-collision error frames could be rapidly retransmitted without the binary exponential backoff procedure in the current IEEE 802.11 MAC. The simulation results showed that the FC scheme could achieve a stable performance, regardless of the traffic load. In the future, the concepts of differentiation of wireless errors may be applied to improve the Quality of service (QoS) over wireless LAN.

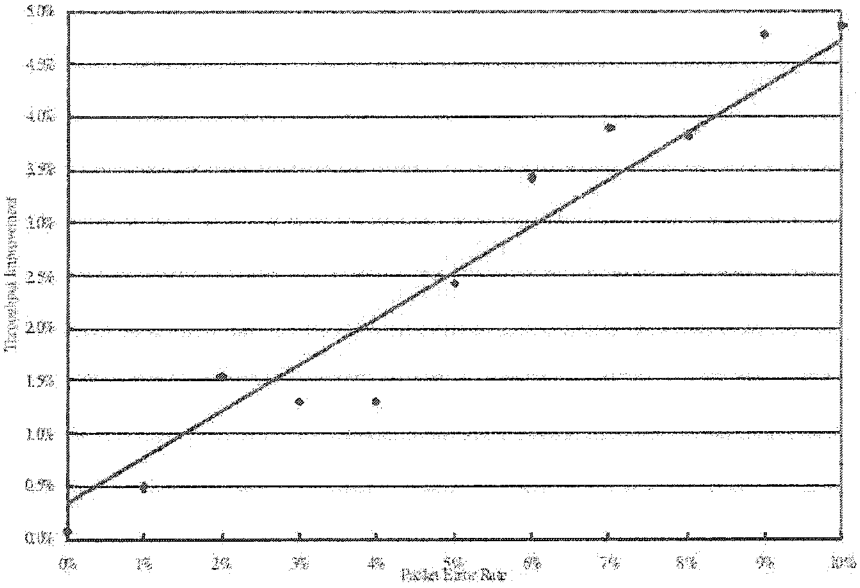


Figure 3.5 Throughput improvement of FC versus frame error rate for 6 stations

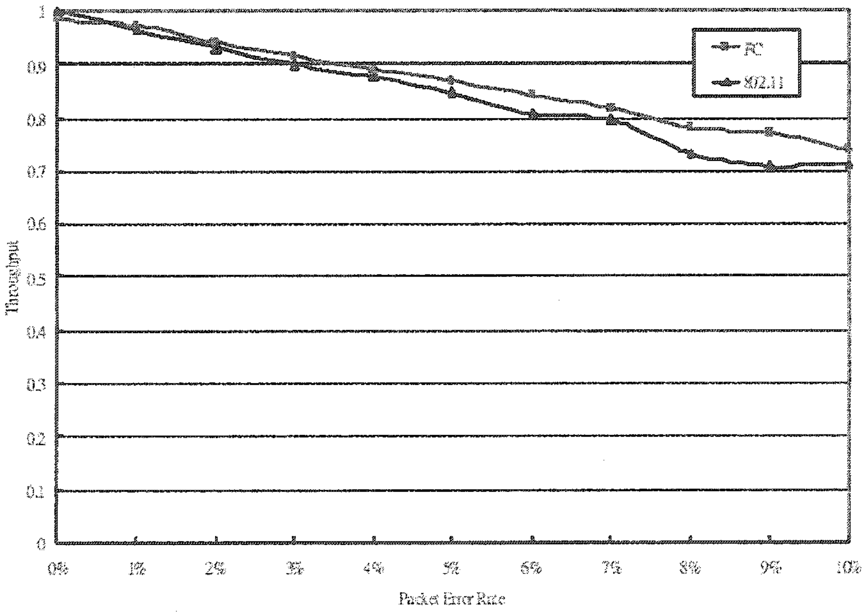


Figure 3.6 Throughput versus frame error rate for 20 stations

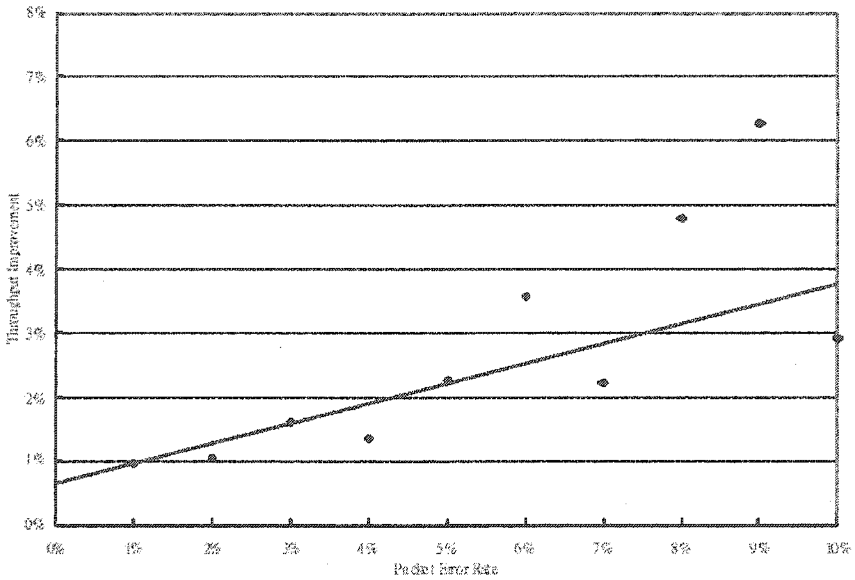


Figure 3.7 Throughput improvement of FC versus frame error rate for 20 stations

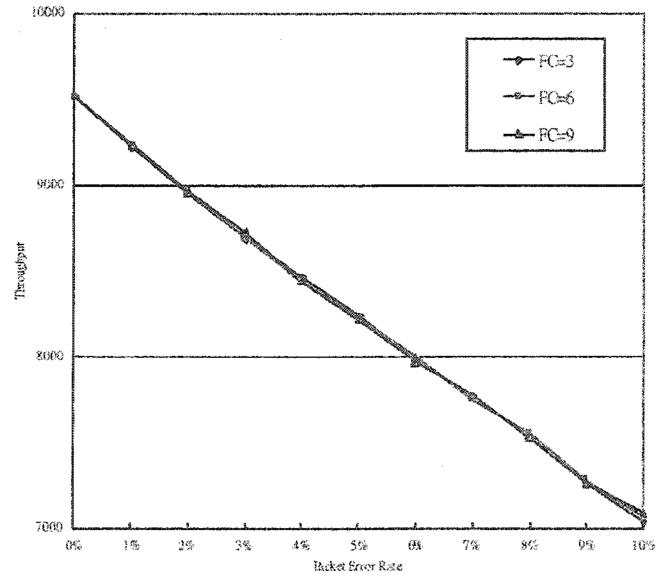


Figure 3.8 Throughput versus frame error rate for 6 stations

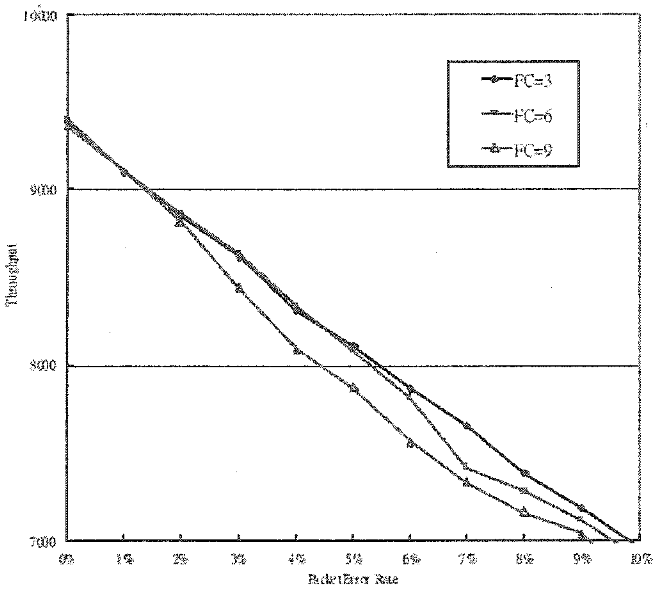


Figure 3.9 Throughput versus frame error rate for 20 stations

CHAPTER 4. DAR: DYNAMICALLY ADAPTIVE RETRANSMISSION

4.1 Introduction

Wireless local area networks (WLANs) are gaining wider and wider popularity in various fields. As a standard for WLAN, 802.11 was initiated by IEEE in 1997 to provide simple and robust features for wireless connection [38].

In 802.11, when the sender fails to receive the ACK frame from the receiver upon expiration of the timer, which is deemed an unsuccessful delivery in the current 802.11 standard, the sender simply retransmits the data frame. But limitations exist. Though the positive ACK scheme is helpful in confirming the successful delivery of data frames, in case of the ACK frame loss after a successful data frame delivery the sender is unable to differentiate it from unsuccessful data delivery and will simply invoke the retransmission scheme. Thus the receiver will get redundant retransmitted frames, which degrades the transmission efficiency. Hence, the goal of our proposed scheme is to improve the efficiency of link layer retransmission by avoiding this redundancy.

4.2 Newly Defined Frame Format in IEEE 802.11

Three types of frames are defined in the IEEE 802.11 standard [38], i.e. management frame, control frame, and data frame. The general format of an 802.11 MAC frame is represented in Fig.2.1, in which the type and subtype values in the frame control field of a frame determine the type of the frame. There are some reserved values in the field, not defined in the current standard. We have defined four new frames using some of the reserved subtype values (shown in Table 4.1). Their functions will be explained in the following section. Other fields in the above frames will be filled according to the current IEEE 802.11 standard.

Table 4.1 New frame types and subtypes

Frame	Type	Subtype
Data(Authentication bit=0)	10	1000
Data(Authentication bit=1)	10	1001
$ACK_{success}$	01	0001
$ACK_{failure}$	01	0010

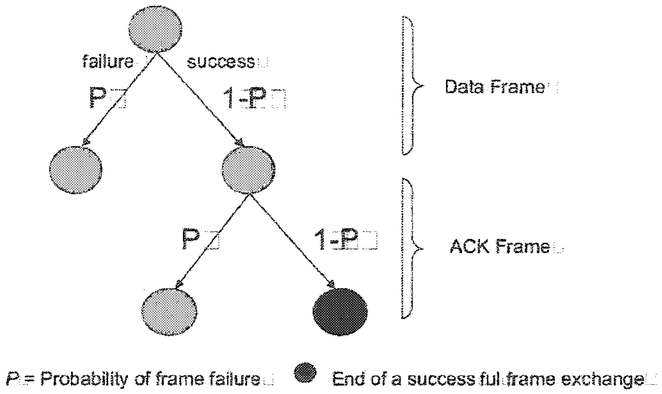

failure
success
P
1-P
Data Frame
P
1-P
ACK Frame
P = Probability of frame failure
● End of a success ful frame exchange

Figure 4.1 Scenarios of two-way frame exchange protocol

To facilitate understanding of our scheme, we use a simple model to demonstrate scenarios for each enhancement. As shown in Fig.4.1, each node represents a transmission state and each directed edge represents a state transition. A value is assigned to show the probability of the transition. The initial state is at the top in Fig.4.1. If the directed edge goes southeast, it stands for a successful frame delivery. If the directed edge goes southwest, it indicates a frame delivery failure.

Before we introduce our enhanced scheme, the conventional two-way frame exchange protocol is studied as follows (Fig.4.1). To simplify our analysis, we suppose the probability of frame errors is a fixed value P, regardless of the frame type. Let $F(e)$ be the probability of an event *e*. We have the following:

$$\begin{aligned} &F(Successful\ frame\ exchange) \\ &\qquad = F(Succ.\ data\ delivery) \times F(Succ.\ ACK\ delivery) \\ &\qquad = (1-P)(1-P) \\ &\qquad = (1-P)^2 \end{aligned}$$

The probability of a successful frame exchange in the 802.11 standard is represented as line 2 in Fig.4.2 where the X axis is probability of frame loss and the Y axis is the probability of a successful frame exchange. Line 1 in Fig.4.2 is an ideal target which means the probability of a successful frame exchange = 1 - (the probability of the frame loss). And our objective in proposing an enhanced scheme is to find a curve closely approaching line 1 between the two lines, represented as line 3 in Fig.4.2. In this section, two basic enhancements are introduced, the improved two-way and four-way frame exchange protocols. Then the proposed DAR scheme, which is derived from those two enhancements, is described in detail.

4.2.1 Improved Two-Way Frame Exchange Protocol

The two-way frame exchange protocol in IEEE 802.11 includes a pair consisting of a data frame from the sender to the receiver and a corresponding positive ACK frame from the receiver to the sender confirming a successful data frame delivery. Lack of reception of an expected ACK frame indicates to the sender that an error has occurred in the frame exchange. However, the receiver may have received the data frame correctly, and the error may have occurred in the reception of the ACK frame. To the initiator of the frame exchange, this condition is indistinguishable from that in which an error occurs in the initial frame. The sender may then simply retransmit the previous frame, which is redundant to the receiver.

In order to improve the conventional two-way frame exchange protocol, the sender needs additional information to determine whether a retransmission is necessary. The protocol for both the sender and the receiver are illustrated in Fig.4.3 and Fig.4.4 as modifications to the current IEEE 802.11 standard.

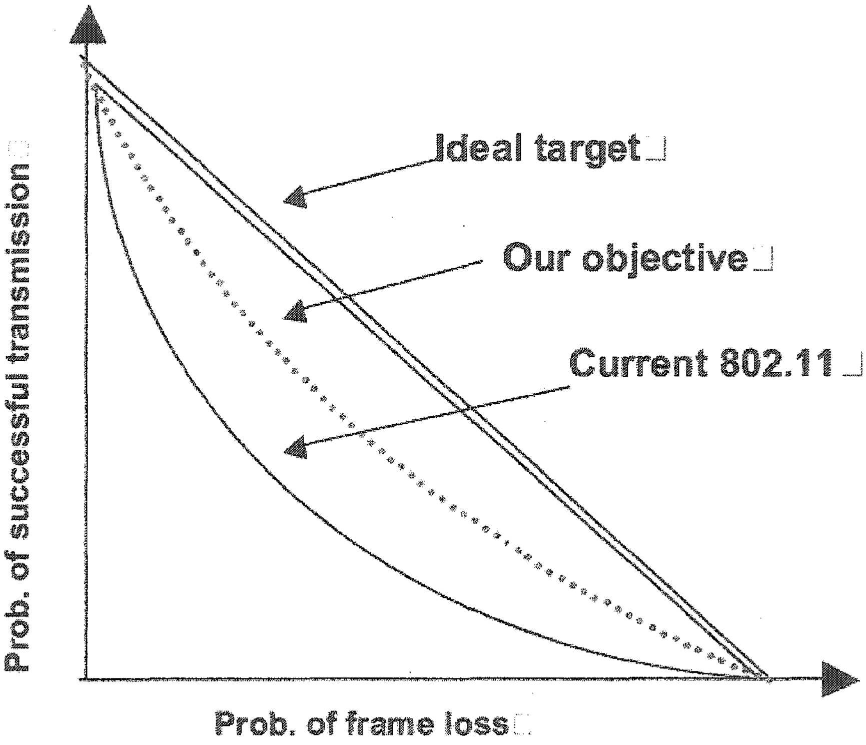


Figure 4.2 Probability of successful frame exchange

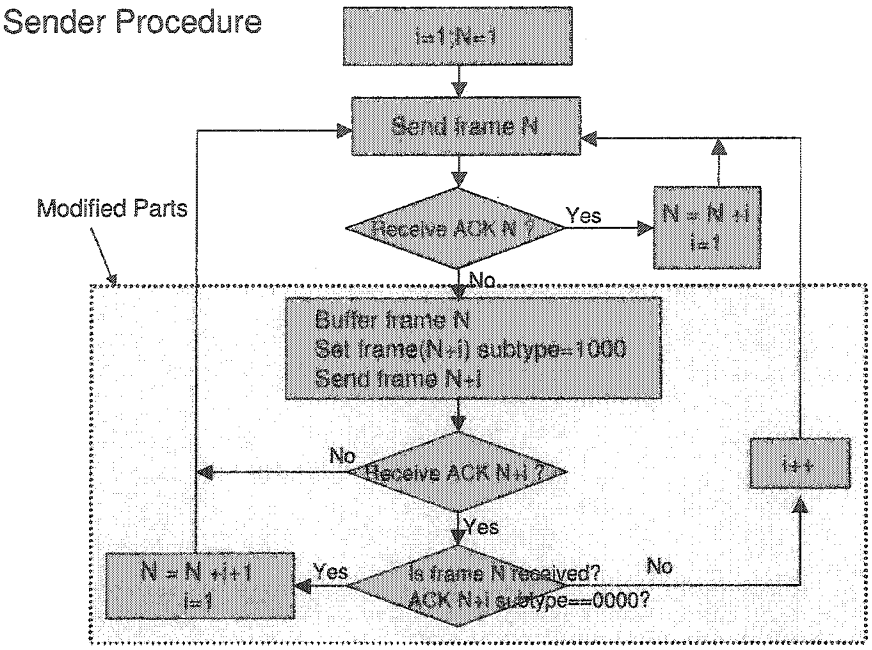


Figure 4.3 Improved two-way frame exchange protocol at the sender

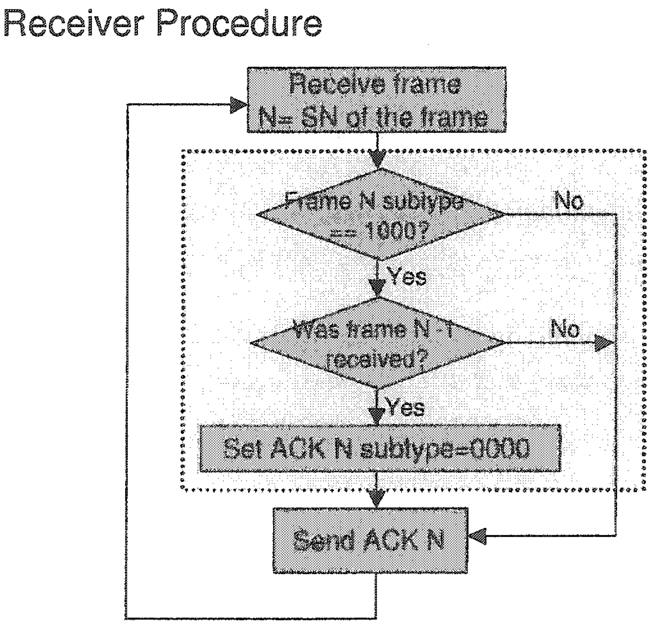


Figure 4.4 Improved two-way frame exchange protocol at the receiver

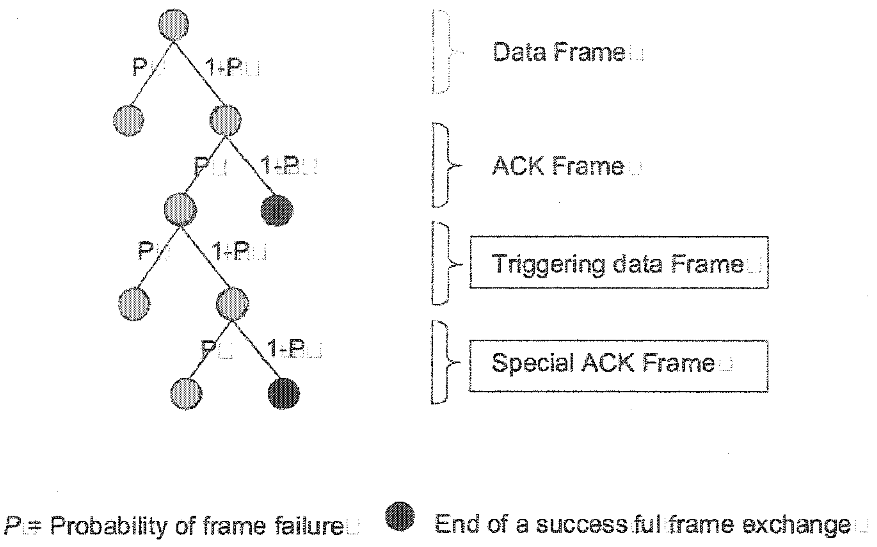


Figure 4.5 Scenarios of the improved two-way frame exchange protocol

After the sender sends a data frame, call it frame N, it buffers the frame in case it does not receive the corresponding ACK frame. The sender then sends the next data frame with subtype = 1000, called a triggering data frame, which triggers an inquiry from the sender to the receiver. The receiver will respond to the triggering data frame with a special ACK frame whose subtype is 0000 when the previous data has been successfully received. Otherwise a regular ACK frame will be sent back to the sender so that the sender is able to determine the previous data frame was lost and retransmission is necessary. It is obvious as shown in Fig.4.5 that the probability of a successful frame exchange improves as follows:

$$\begin{aligned} F(Successfulframeexchange) &= (1-P)^2 + (1-P)P(1-P)^2 \\ &= (1-P)^2 + P(1-P)^3 \; > \; (1-P)^2 \end{aligned}$$

4.2.2 Improved Four-Way Frame Exchange Protocol

The four-way frame exchange protocol aims at eliminating the hidden node problem by claiming the occupancy of wireless mediums before real transmission. Two types of small control

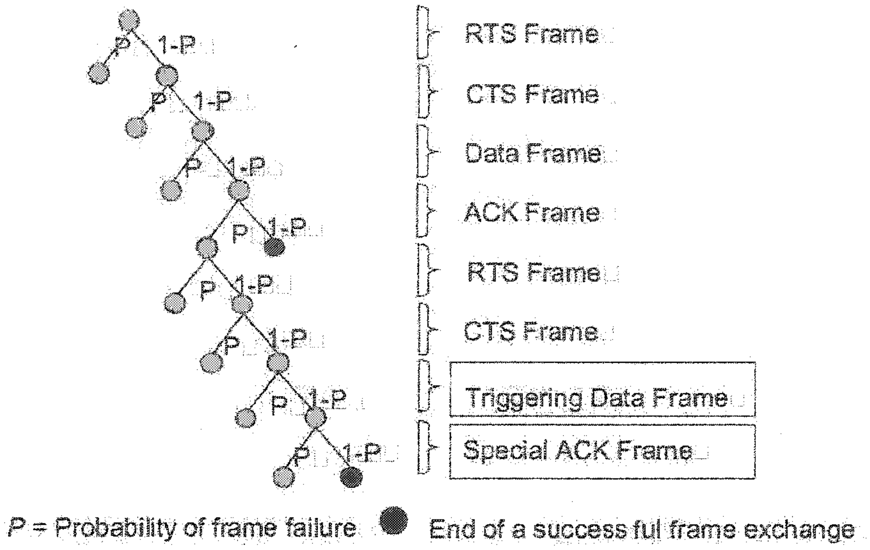


Figure 4.6 Scenarios of the improved four-way frame exchange protocol

frames RTS and CTS are exchanged between the sender and the receiver so that other parties in the wireless neighboring regions hearing the two frames can hold their traffic for a period of time to avoid collision.

Much like the improved two-way frame exchange protocol, the improved four-way protocol uses a special ACK frame to piggyback the transmit information to the sender after a triggering data frame. Fig.4.6 shows the scenarios of the improved four-way frame exchange protocol with RTS and CTS frames.

4.3 Dynamically Adaptive Retransmission (DAR) Scheme

DAR is proposed based on the above two improvements. We are not using the specially defined data frame as in the improved two-way frame exchange protocol, but a specially defined RTS instead with subtype set to 0001, called a triggering RTS, to inquire to the receiver if the previous data frame has successfully arrived. Therefore the special RTS/CTS frame exchange is triggered dynamically when the corresponding ACK is not received. In other words, we use the existing RTS/CTS frame exchange to piggyback the transmission information to the sender. In addition, the sender does not have to buffer frames in this scheme because it will

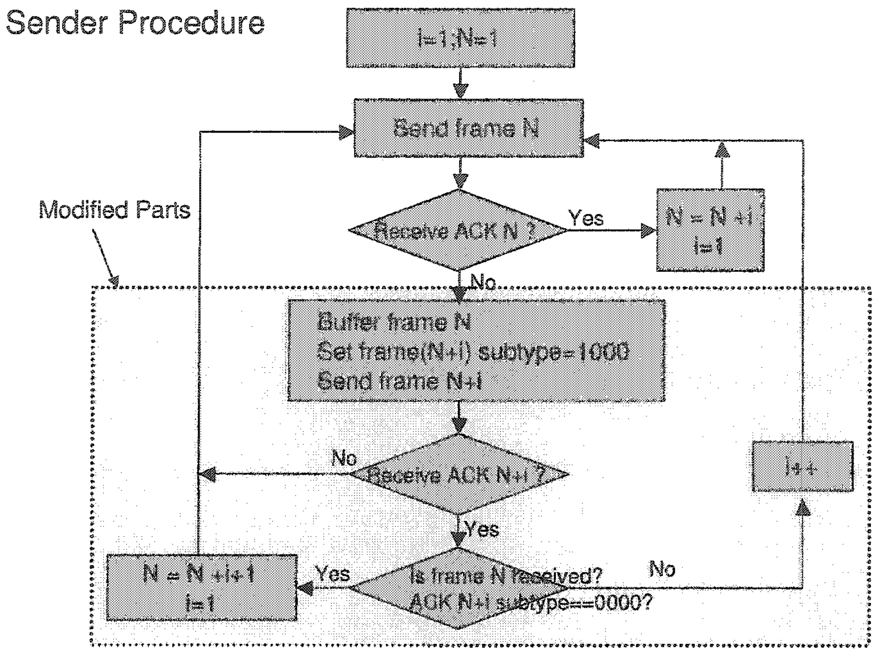


Figure 4.7 DAR scheme at the sender

be capable of determining which frame to send before transmission. The sender procedure can then be simplified as shown in Fig.4.7. The frame exchange initiator sends a special RTS frame whose subtype is 0001 if it is unable to receive a positive ACK frame before the timeout. Retransmission is not invoked immediately at this time. Upon receipt of a regular CTS frame, the sender knows that the previous data frame did not arrive at the receiver. Retransmission becomes necessary in this case. Otherwise, the sender just ignores the case of a lost ACK frame if it receives a special CTS frame whose subtype is 0010. If the last data frame is followed by an ACK loss, the sender will still initiate a triggering RTS inquiring whether the last data frame has been successfully delivered. In this RTS frame the duration field will be filled in accordance with the expected special CTS only. Fig.4.8 illustrates the DAR scheme at the receiver. Note that the 802.11 MAC layer semantics are not violated in DAR because the frame exchange process is not intercepted and the frame exchange sequence remains the same, which means it is still atomic. Fig.4.9 show the scenarios of DAR.

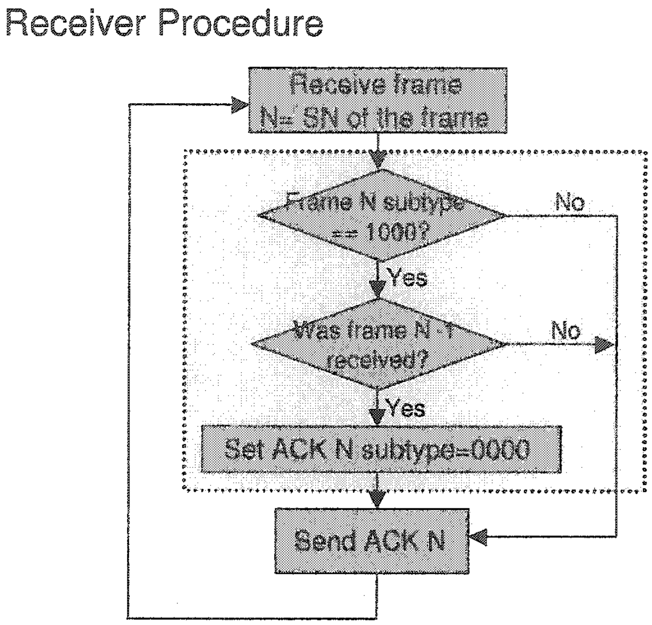


Figure 4.8 DAR scheme at the receiver

4.4 Theoretical Analysis

4.4.1 Analysis of the Improved Two-Way Frame Exchange Protocol

The key point of our improved two-way frame exchange protocol is two specially defined types of frames containing additional feedback information. Fig.4.10 shows the performance improvement (represented as the probability of successful frame exchange on the Y axis) with respect to bit error rate (represented as BER on the X axis) Obviously the probability of successful frame exchange in the enhanced scheme is higher than that in the current IEEE 802.11 standard. Performance will be improved as a result. A key concept in the analysis is the differentiation ratio, defined to measure the performance of DAR. We define the differentiation ratio as the ratio of successfully delivered frames with lost ACKs that can be differentiated by the sender using the enhanced scheme over all failed frames detected by the conventional retransmission scheme. It is obvious that the differentiation ratio in the conventional two-way frame exchange protocol is always 0. Let p represent BER., and len_d and len_a represent the lengths of the data and ACK frames. We calculate the differentiation ratio $Diff.$, in the improved two-way frame

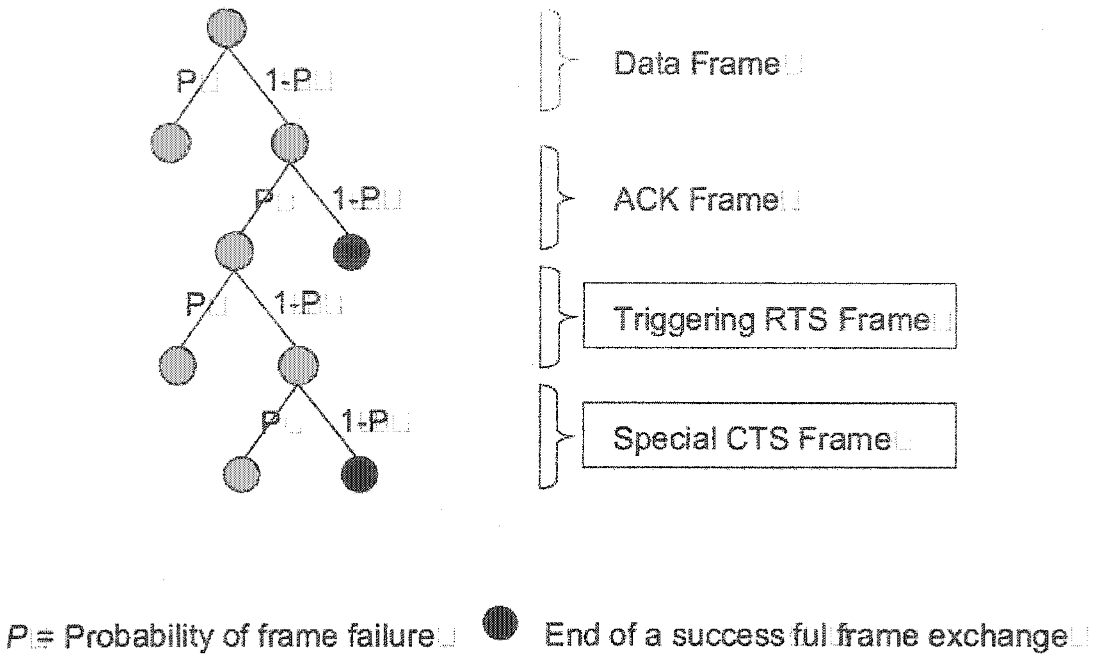


Figure 4.9 Scenarios of the DAR scheme

exchange protocol as follows:

$$\begin{aligned} Diff. &= \frac{number\ of\ successfully\ delivered\ data\ frames\ with\ lost\ ACK}{number\ of\ failed\ frames} \\ &= \frac{[(1-p)*len_d]*[p*len_a]*[(1-p)*len_d]*[(1-p)*len_a]}{[(1-p)*len_d]*[p*len_a]} \\ &= [(1-p)*len_d]*[(1-p)*len_a] \end{aligned}$$

Fig.4.11 shows the differentiation ratio in the improved two-way frame exchange protocol with respect to BER. When the bit error rate is relatively low, the differentiation ratio is high, which means many failure cases can be differentiated by the improved protocol as ACK loss cases without invoking retransmission. This gives a desirable result.

4.4.2 Analysis of Duration of Frame Exchange

IEEE 802.11 and the DAR frame sequences are illustrated in Fig.4.12. In the current 802.11 standard, the transmission initiator just retransmits the data frame without receiving an ACK (the top case). The DAR scheme intelligently deals with unacknowledged data frame by retrans-

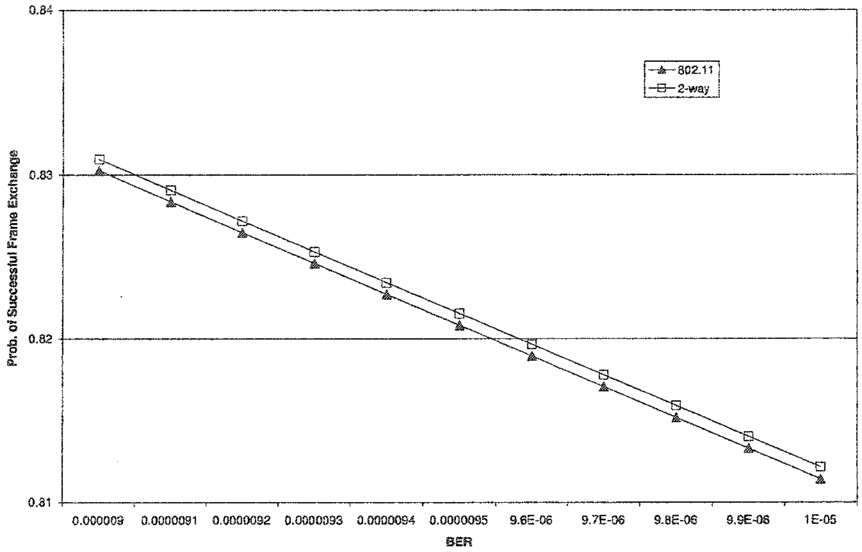


Figure 4.10 Performance in the improved two-way frame exchange protocol

mitting only what are not successfully delivered (the middle case). Any data frames followed by ACK losses will be diagnosed, then ignored (the bottom case). Note that the more cases of successful data delivery followed by ACK losses, the less time needed and the greater the improvement would be. Let l_1 represent the time savings in the bottom case, and l_2 the time over-expenditure in the middle case. We define the *Cost of Difference* (CD) as follows:

$$CD = l_1 \times P_1 - l_2 \times (1 - P_1)$$

where P_1 is the probability of the occurrence of the bottom case. A larger CD value indicates a more favorable improvement. We use *goodput* to measure the performance of both DAR and the 802.11 standard. The concept of goodput of the link layer is taken from TCP and defined as the bandwidth delivered to the receiver through the link excluding duplicate frames. Thus, the goodput G_l of a link l during a time interval t corresponds to the number of bytes B of link l forwarded to the upper layer during the interval t [11].

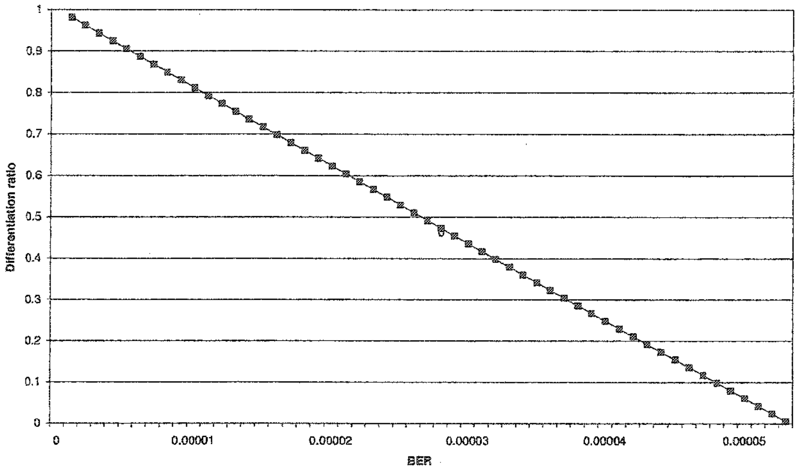


Figure 4.11 Differentiation ratio in the improved two-way frame exchange protocol

4.5 Experiments

4.5.1 Experimental Methodologies

We developed a simulator in C and performed several simulations to determine the performance and efficiency of the proposed DAR scheme. The MAC layer basically follows the IEEE 802.11 standard [38]. The DAR protocol is implemented as a set of modifications to the frame exchange protocol in the MAC layer. Our experimental testbed consists of two mobile hosts, which are interconnected using a shared-medium wireless LAN with a raw signaling bandwidth of 2 Mbps. This is because we attempt to ensure that losses are due only to wireless errors, not congestion. This also allows us to focus on the effectiveness of the mechanisms for handling such losses. The simple testbed topology represents typical scenarios for wireless links and mobile hosts, such as cellular wireless networks. In addition, our experiments focus on MAC frame exchange between the mobile hosts.

In order to measure the performance of the protocols under controlled conditions, we generate errors on the lossy link using a uniformly distributed bit-error model. Each run in the experiment consists of a 10 MByte transfer from the sender to the receiver across the wireless link. We chose

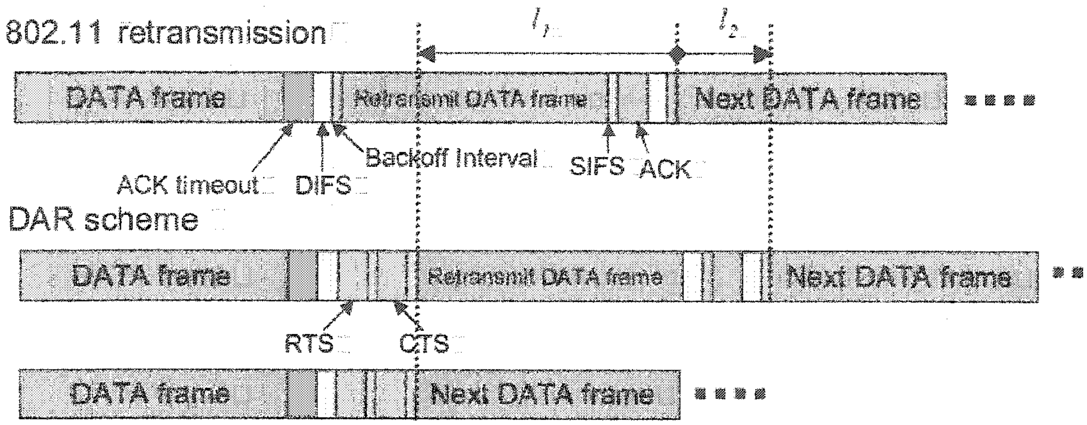


Figure 4.12 Frame sequences in 802.11 and DAR scheme

Table 4.2 Frame parameters in the experiments

Frame	Size (Byte)	Transfer Time (μs)
Data	500	4292
ACK	14	120
RTS	20	144
CTS	14	120

this rather long transfer size in order to limit the impact of transient behavior. During each run, we measure the goodput as normalized between 0 and 1. The other parameters in the simulation models, listed in the Table 4.2 and 4.3, are referenced from [76]

4.5.2 Experiment Results

Fig.4.13 shows the goodputs in 802.11 vs. DAR with respect to BER. DAR achieves only slightly higher goodput than the 802.11 standard. This is discussed in section 4.6. To demon-

Table 4.3 Interframe space in the experiments

Interframe space	Duration (μs)
SIFS	10
DIFS	110
ACK Timeout	120

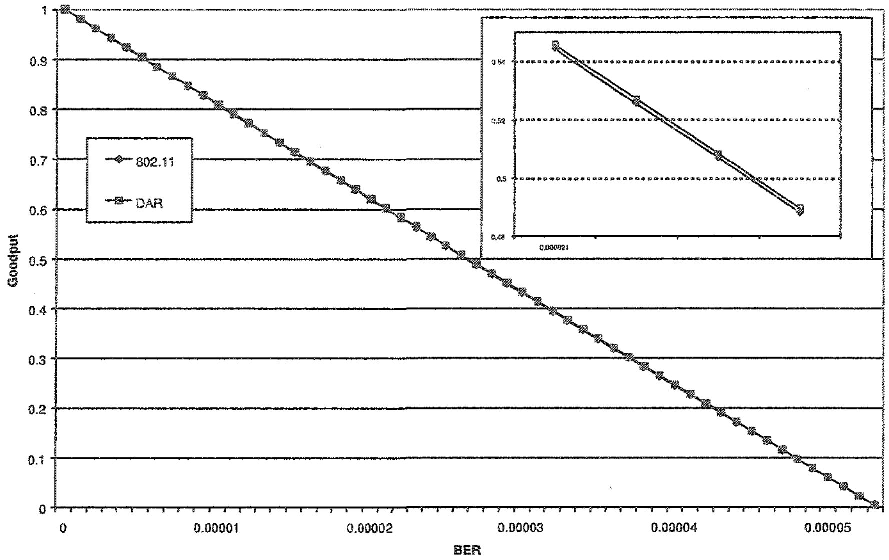


Figure 4.13 Goodput in DAR vs. 802.11 with respect to BER

strate the benefit of our scheme we calculated the goodput value using the ACK loss rate as shown in Fig.4.14. The Data frame loss rate, RTS loss rate and CTS loss rate are fixed to be 0.1, 0.0001 and 0.0001 respectively. It can be seen in Fig.4.14 that the goodputs degrade much more slowly in DAR than 802.11 with increasing ACK loss rate. The reason is that DAR is capable of avoiding redundant retransmission due to ACK losses.

Similar to the analysis in section 4.4, the differentiation ratio in the DAR scheme is analyzed as shown in Fig.4.15. With increasing BER, the differentiation ratio remains high, which means that a high percentage of failure cases can be differentiated as lost ACK cases and retransmission is not necessary to achieve high transmission efficiency.

4.6 Further Discussions

4.6.1 Performance Enhancement

The experiment results in Fig.4.13 show only slightly higher goodput achieved by DAR than 802.11. A major reason is that the goodput is influenced by many factors, such as the frequencies of frame losses and triggering DAR, and the value of *Cost of Difference* (CD).

In a higher error rate situation, more frame losses occur. But the DAR failure rate increases

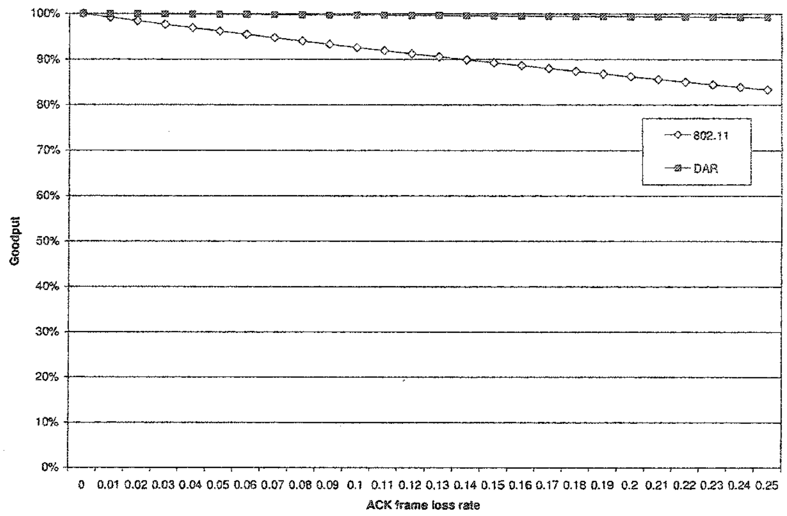


Figure 4.14 Goodput in DAR vs. 802.11 with respect to ACK loss rate

due to more losses of RTS and CTS frames. Thus considering the overall impacts of these factors, the result does not indicate a significant improvement.

Another issue in real transmission is the length of data frames. Longer data frames may incur more data frame losses, and lower the probability of successful data delivery followed by an ACK loss. However, longer data frame increases the value of CD. Thus the combining influences of the above factors make the performance of DAR scheme insignificantly different from IEEE 802.11.

4.6.2 Buffer Size

To recover from the frame loss, a data buffer is needed at the sender for the unacknowledged frame. It is obvious that more buffers may handle more complex cases such as consecutive ACK or CTS losses. However, it might be impractical to allocate a huge amount of buffer for each transmission due to limitations on memory resources. Moreover, the probability of the above event can be low. Experiments to explore the amount of buffer needed for each transmission therefore are necessary.

Theoretically the number of buffers determines the number of consecutive response losses that can be handled, because the unacknowledged data frames can be buffered before the sender

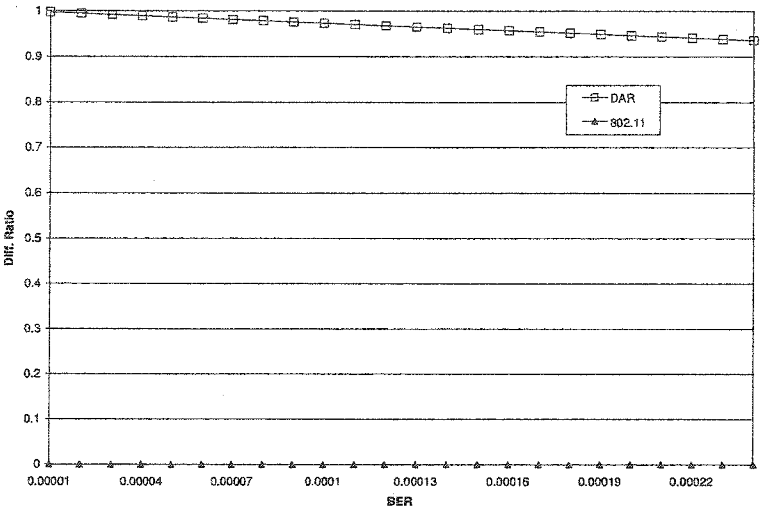


Figure 4.15 Differentiation ratio in DAR vs. 802.11

receives either affirmative or negative confirmation from the receiver.

Fig.4.16 shows the probability of consecutive response losses in various BER situations. The X axis represents the number of consecutive response losses including ACK and CTS frame losses. The Y axis represents the probability of these occurrences. Three lines have been drawn based on three different bit error rates, 0.001, 0.01 and 0.1. It can be seen that the more consecutive lost responses considered, the lower the probability. The lower the bit error rate, the more quickly the possibility degrades. Considering practical situations where the BER is low, it is unnecessary to cope with more than two consecutively lost responses, as proposed in our DAR scheme.

4.7 Summary

The current IEEE 802.11 standard confuses the sender when a positive ACK is lost during its way back. The sender will take it as an unsuccessful delivery and simply retransmit the data frame. An enhanced DAR scheme is introduced in this chapter, proposing a new feedback scheme, in which the CTS frames carry additional information concerning the previous data delivery without violating the 802.11 MAC layer semantics. Our method proves to be efficient

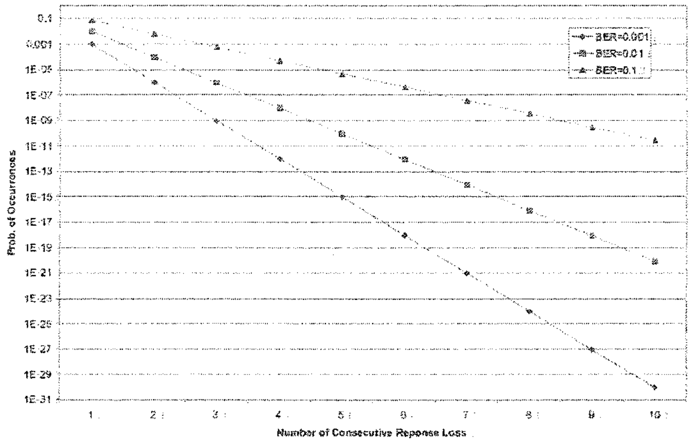


Figure 4.16 Probability of consecutive response losses in various BERs

in handling such error conditions as stated in the chapter. Experiments and analysis show that the DAR scheme efficiently decreases redundant retransmission by clearly differentiating ACK frame losses.

CHAPTER 5. QA: QUICK ACKNOWLEDGEMENT SCHEME

An SSCOP-based Link Layer Protocol for Wireless LANs

The IEEE 802.11 standard provides a fast recovery from frame losses using a rapid positive acknowledgment scheme at the link layer. However, the adoption of positive acknowledgment leads to inefficient frame transmission. Therefore, we propose a novel link layer protocol for wireless LANs adapted from an ATM-based protocol, called the Service Specific Connection Oriented Protocol (SSCOP). The protocol uses much less bandwidth on the return path and enhances the performance of data frame transmission. We evaluated and compare the performance of the protocol with IEEE 802.11. The results show that the proposed protocol has a much better performance in an error-prone wireless environment, even when the bit error rate is severely degraded.

5.1 Introduction

Wireless communication technology has gained widespread importance in recent years. With more and more wireless devices around, the requirement of high speed and reliable transmission over wireless links is growing. Due to the high loss rate experienced over wireless links as well as the presence of hidden terminals, the IEEE 802.11 standard uses a positive acknowledgement scheme.

In the IEEE 802.11 protocol [38], the reception of data frames requires the receiving host to respond with an acknowledgment, generally an ACK frame, if the received frame is correct. Missing of an expected ACK frame indicates to the source host that an error has occurred. This technique is known as positive acknowledgment. The main advantage of positive acknowledgement is high reliability since the sender can quickly detect the occurrence of any transmission error. The inefficiency problem in positive ACK has been proposed in Chapter 2.

5.2 Related Works

Several studies have been done to improve the throughput performance of the IEEE 802.11 MAC protocol [24][65][51][92]. A jamming-based retransmission mechanism that is compatible with the 802.11 standard is proposed in [24] and it could reduce the packet delay of real-time traffic. In [65], a reliable MAC protocol is proposed to reduce the number of control handshake messages. Since fewer control messages in frame exchanging, the protocol is efficient in transmission and power. In [51], the throughput performance of IEEE 802.11 wireless LANs has been evaluated in relation to overhead. Furthermore, sources of overhead are gap time, preamble, header fields for the PHY (physical) and the MAC (medium access control) layer, ACK (acknowledgement) frames, the TCP (transmission control protocol). In [92], the authors propose a scheme to prevent redundant retransmission in case of positive ACK frame losses.

There are other studies conducted to improve the acknowledgement scheme in the transport layer [61] [44]. However, no study has been done on improving the positive acknowledgement scheme of IEEE 802.11. In this chapter, we propose an enhanced link layer acknowledgement scheme, which is heavily based on a protocol that has already been implemented in ATM networks, called the Service Specific Connection Oriented Protocol (SSCOP) [42]. When originally conceived, SSCOP was intended to provide both a reliable link layer for ATM signaling and a reliable transport layer for user data over ATM networks. Several new transport protocols have been proposed based on SSCOP (e.g. Satellite Transport Protocol [45]). However, no link layer protocol is proposed based on it. Although SSCOP targets large delay-bandwidth product networks, it still performs quite well over wireless links with appropriate modifications. In addition, SSCOP relies on in-sequence data delivery in the lower protocol layers, which is also an important characteristic in the wireless link layer.

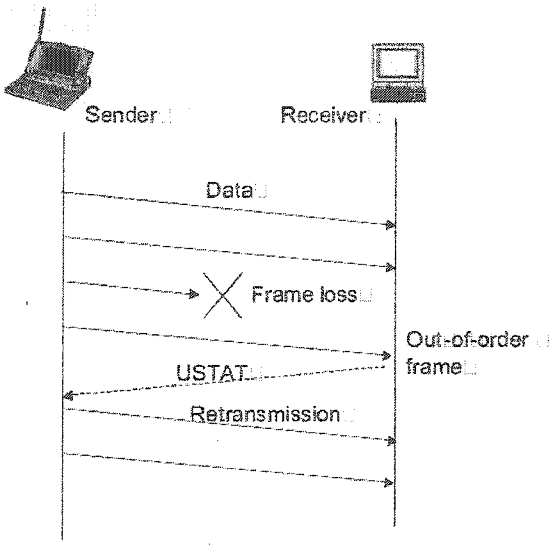


Figure 5.1 Example of USTAT operation

5.3 Proposed Protocol

In this section, two simple examples are given to show the basic operations of the proposed protocol. Then, we describe the detailed modification and additions to make SSCOP work in wireless LANs.

5.3.1 Basic Operations of the Proposed Protocol

There are two possible scenarios in the protocol and we illustrate them in Fig.5.1 and Fig.5.2. Fig.5.1 shows an example of the proposed protocol. Unlike IEEE 802.11, the proposed protocol does not use positive ACK frame to acknowledge the reception of data frames. A receiver can detect a frame loss by checking the sequence number in the frame header, defined in the IEEE 802.11 standard. If the sequence number is out-of-order, there could be one or more frame loss before this frame arrives because there is only one link between the transmitter and the receiver, and each frame is transmitted sequentially. When a receiver detects a frame loss, the receiver sends an *Unsolicited Status* (USTAT) control frame to the transmitter. Similar to the idea of negative acknowledgement (NACK) technique in the transport layer, the proposed protocol uses

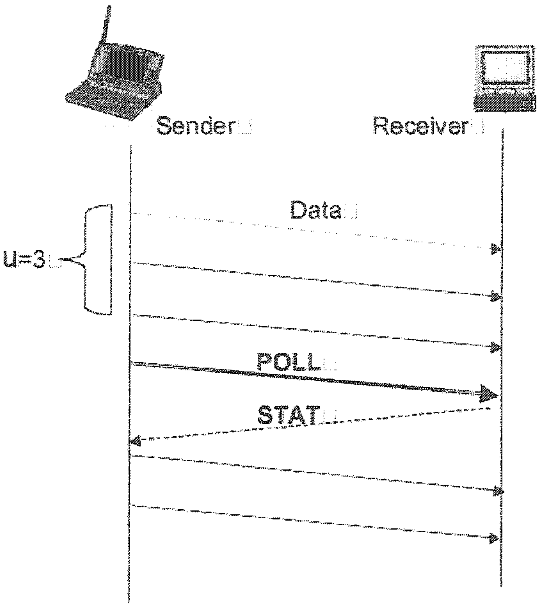


Figure 5.2 Example of POLL/STAT operation

USTAT frame to inform the transmitter about any frame loss. When the transmitter receives a USTAT frame from the receiver it retransmits the lost frame. Note that the USTAT frame is sent after the receiver has waited for only a SIFS (Short Inter frame Space) interval, therefore the receiver does not contend for the wireless medium with other hosts.

One important difference between IEEE 802.11 and the proposed protocol is the elimination of ACK_Timeout. A transmitter, after sending one data frame, does not wait for the ACK from the receiver. Instead, the transmitter goes into the next frame exchange stage; it sends the RTS frame for the next data frame. Meanwhile, the receiver receives the data frame and does not reply with the ACK frame. Thus, ACK_Timeout becomes unnecessary in the proposed protocol.

Fig.5.2 shows the other scenario of the proposed protocol. After a transmitter sends out a specified number of data frames without acknowledgement, say μ, a POLL frame is sent out to the receiver. When the receiver receives a POLL frame from the transmitter, the receiver will report the status of the last μ frames to the transmitter with a Status (STAT) frame. In the new protocol, a transmitter sends frames to the receiver, storing the frames for potential retransmission until the receiver has acknowledged them by STAT frame. The STAT message is similar to the TCP Selective Acknowledgment (SACK) protocol [61], except that the STAT message reports the entire state of the receiver buffer (rather than the most recent three gaps as in SACK), and the receiver does not contain information about previously acknowledged data (which is permitted in TCP SACK). In the case of Fig.5.2, the receiver reports to the transmitter the successful reception of the last 3 frames with a STAT message. After receiving the STAT frame from the receiver, the transmitter flushes its buffer, removes the old frames, adjusts the μ value for sending new frames, and then continues to send subsequent frames.

5.3.2 Timeout Mechanisms

Two new timeout mechanisms are brought in the protocol, *POLL_Timeout* and *data_timeout*, used to avoid useless transmission from the transmitter to the receiver when the link is broken. Link breakage is common in wireless networks due to host mobility and interference. In this case, the receiver cannot receive any frame from the transmitter and the transmitter cannot receive any STAT/USTAT frame, either. If no timeout exists, transmitter and receiver do not know about the link breakage and it may cause higher layer timeout, e.g. TCP timeout.

1. POLL_Timeout: After sending μ data frames and one POLL frame, the transmitter waits for the STAT frame from the receiver. The transmitter retransmits the POLL frame, after the POOL_Timeout.

2. Data_Timeout: The receiver waits for the data frame for a period of Data_Timeout. If it does not receive the data within that period, it sends out a STAT frame to the transmitter.

These link layer timers are intended to trigger retransmission in advance of the higher layer timeouts.

5.3.3 Determination of μ Value

μ is an important parameter for the transmitter. It needs to be adjusted based on the STAT report from the receiver. A high μ value means a POLL frame is transmitted after a large number of frames. There are three effects of a high μ value:

1. POLL/STAT overhead is small,
2. the buffer requirement at the transmitter is high,
3. the response to any link break is slow

In contrast, a small μ value causes a high POLL/STAT overhead, but a low buffer requirement at the transmitter and quick detection of link breaks. We can see that the protocol degrades to to IEEE 802.11 when $\mu = 1$. The adjustment of this parameter is a tradeoff between the response time and the POLL/STAT overhead. We have devised a simple adjustment scheme to take both the detection time and the overhead into consideration. μ can take two values: STAT_Max and 1. When the successful frame transmission rate is equal to or greater than STAT_Threshold, μ is set to STAT_Max. When the successful frame transmission rate is lower than STAT_Threshold, then μ is 1. The idea behind the adjustment scheme is that when the link becomes prone to errors, multiple frame losses will cause timeout at a higher layer. Thus, the response to the frame loss is important when frame loss rate is high.

5.3.4 Buffer Management

The use of selective retransmission requires the receiver to allocate a retransmission buffer at both the sender and the receiver. At the sender side, all the sending frames should be saved in the retransmission buffer until the STAT arrival. At the receiver side, when an out-of-order frame arrives, this and the subsequent frames will be buffered until the lost frame is received by the receiver. As shown in Fig.5.3, after data frames 3-7 are sent out, these frames are buffered at the transmitter. After receiving the STAT frame, the transmitter will empty the buffer. The receiver detects an out-of-order frame when receiving data frame 11, and the receiver buffers this frame. Upon the arrival of the frame 9 at the receiver, the receiver will release this buffer.

5.3.5 Modified NAV Value

Since the ACK frame is embedded in the frame exchange of IEEE 802.11, eliminating the ACK frame will change the calculations of NAV value. In the proposed protocol, all the NAV

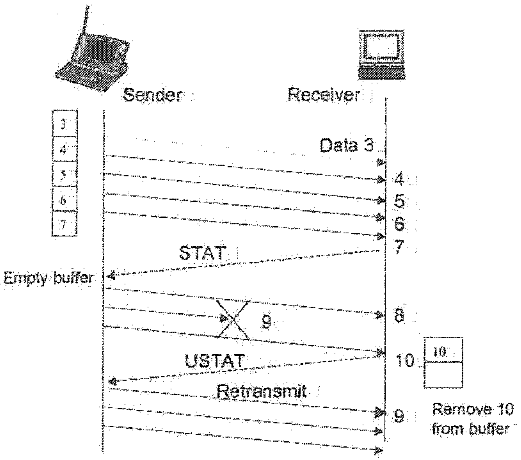


Figure 5.3 An example of buffer management in the proposed scheme

values do not include the transmission of ACK. For example, the NAV value in a RTS frame includes the transmission duration of RTS/CTS/DATA frame. Note that after one data frame transmission, hosts intending to send will still contend for the wireless medium with others. In other words, the contention for the wireless medium among all the hosts is still the same.

5.3.6 Newly Defined MAC Frame Format

Three new types of frame are introduced in the proposed protocol, namely, *STAT* (status) frame, *USTAT* (unsolicited STAT) frame, and *POLL* frame. The goal of the USTAT frame is to quickly inform the transmitter of any frame loss, and the goal of the STAT frame is to report the transmission status to the transmitter.

To minimize the modification made to the current IEEE 802.11 standard, we utilize the reserved type and subtype fields in frame control field to define the new frames as shown in the Fig.2.1. For a POLL frame, we embed the poll information into a data frame. As shown in table5.1, a POLL frame is a data frame with the type=10 and the subtype=1000. Since a STAT frame needs to carry information about the frames in the buffer, the STAT frame could be varying in length. We identify a special type of data frame (i.e. type=10 and subtype=1001) to carry the statistical information about frame transmissions in the payload. USTAT frame is

Table 5.1 Adaptation of IEEE 802.11 MAC frame format

Frame	Type	Subtype
POLL	10	1000
STAT	10	1001
USTAT	01	0010

defined as a special type of ACK frame with type=01 and subtype=0010. Hence, all the three new frame structures are made compatible with IEEE 802.11.

5.3.7 Discussion

In the proposed protocol, the receiver notifies the transmitter of lost frame accurately, so the transmitter can retransmit lost frames more efficiently than in 802.11. One advantage of the proposed protocol is the reduction of the acknowledgement traffic. Fig.5.4 compares the overhead before and after the removal of ACK frame for each data frame transmissions. The reduction also means shorter transmission time and lower power consumption for each frame exchange.

Another advantage of the proposed protocol is the elimination of frequent ACK timeouts from 802.11 at a high error rate. As shown in Fig.5.5, the transmitter in 802.11 has to wait for ACK_timeout after one data frame loss. While in the proposed protocol, the transmitter can retransmit immediately after receiving the USTAT. Obviously, this reduction presents shorter transmission time and lower power consumption for each frame exchange.

5.4 Simulation Results

The simulations were performed in NS-2 [48]. The positive acknowledgement mechanism of IEEE 802.11 was modified in the proposed protocol. Nodes were static (no mobility) in our simulations. A free space channel model was used in the simulations model. The channel data rate was 2Mbps. In the simulation, we consider a grid topology with N flows and $2 \times N$ nodes, where N ranged from 1 to 10. All the nodes were within the range of other nodes in the network.

We compared the proposed protocol with IEEE 802.11. We were interested in comparing the

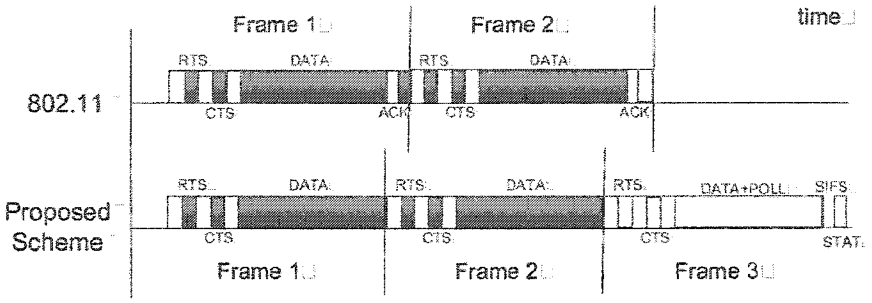


Figure 5.4 Comparison of 802.11 and the proposed scheme

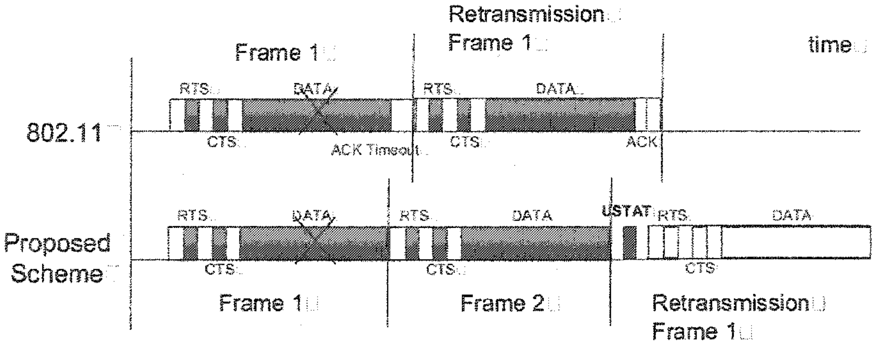


Figure 5.5 Comparison of 802.11 and the proposed scheme during the occurrence of frame loss

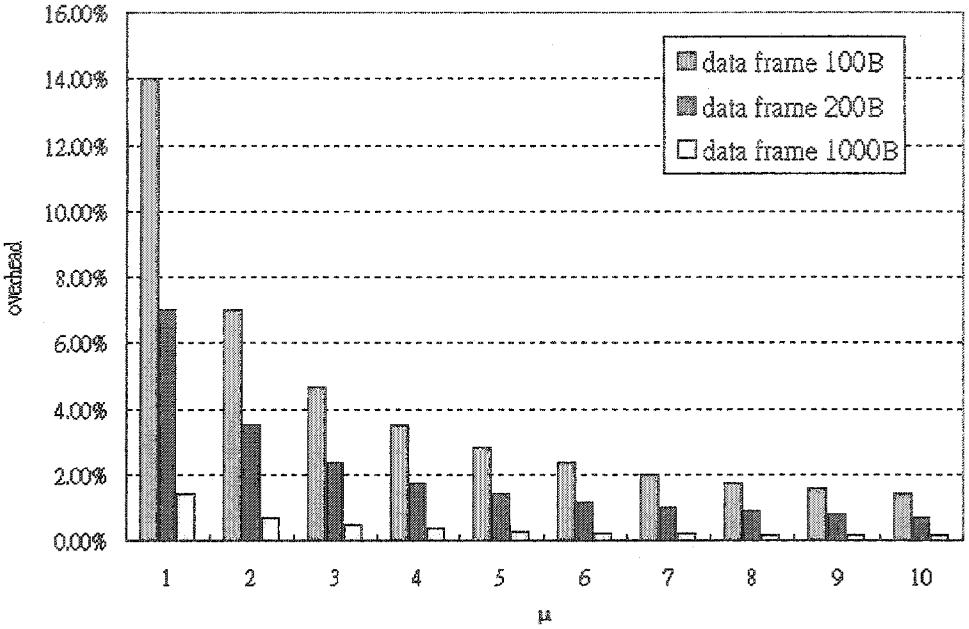


Figure 5.6 The POLL/STAT overhead with increasing μ value

overhead incurred as well as the performance of both protocol in the presence of errors. Fig.5.6 shows the varying POLL/STAT overhead at different μ values. The overhead is defined as the POLL/STAT transmission time over the total transmission time. Thus, a smaller frame length must have a higher POLL/STAT overhead. Note that the case where μ=1 showed exactly the same result as IEEE 802.11. Fig.5.6 shows a high μ value led to low POLL/STAT overhead.

The second simulation is to compare the throughputs in IEEE 802.11 and the proposed protocol with increasing number of flows. Fig.5.7 shows the result at frame loss rate of 0. It is clear that the proposed protocol always performs better than IEEE 802.11.

Fig.5.8 shows the result at $framelossrate = 10\%$. With increasing of number of flows, the proposed protocol gets more and more improvement over 802.11. This is because the proposed protocol can retransmit lost frame more efficiently than IEEE 802.11 by using STAT/USTAT and removing unnecessary ACK traffic.

Fig.5.9 shows the result with frame loss rate as high as 20%. It is obvious that, compared with Fig.5.6, higher frame loss rate causes the throughput to drop. The difference between IEEE 802.11 and the proposed protocol becomes larger when the number of flows is 3 and above. We

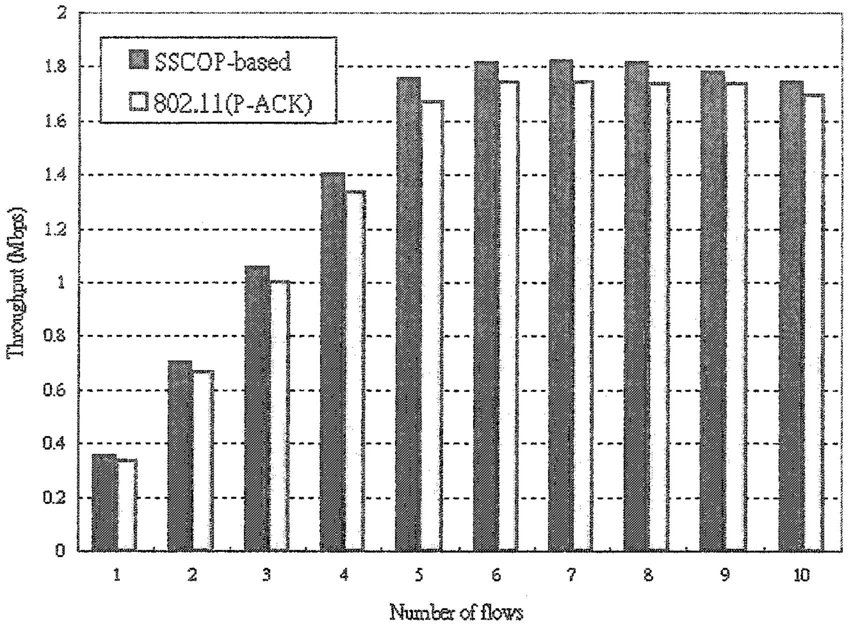


Figure 5.7 Total throughput with increase number of flows at frame loss rate=0

find that the proposed protocol always performs better than IEEE 802.11 and it is even more obvious at high error rate.

5.5 Summary

An SSCOP-based link layer acknowledgement protocol has been designed as a replacement for positive acknowledgement in IEEE 802.11. Although the SSCOP was originally intended to provide end-to-end error recovery for user data and link protection for ATM signaling, the concept of SSCOP can also be applied to the link layer with appropriate modifications. By using both concepts of SACK and NACK, the proposed protocol solves the inefficiency problem of positive ACK in IEEE 802.11. Because of the elimination of ACK timeout and the precise acknowledgement, the protocol provides much better performance than IEEE 802.11. The simulation results show that the performance improvement of the proposed protocol increases with increasing bit error rate.

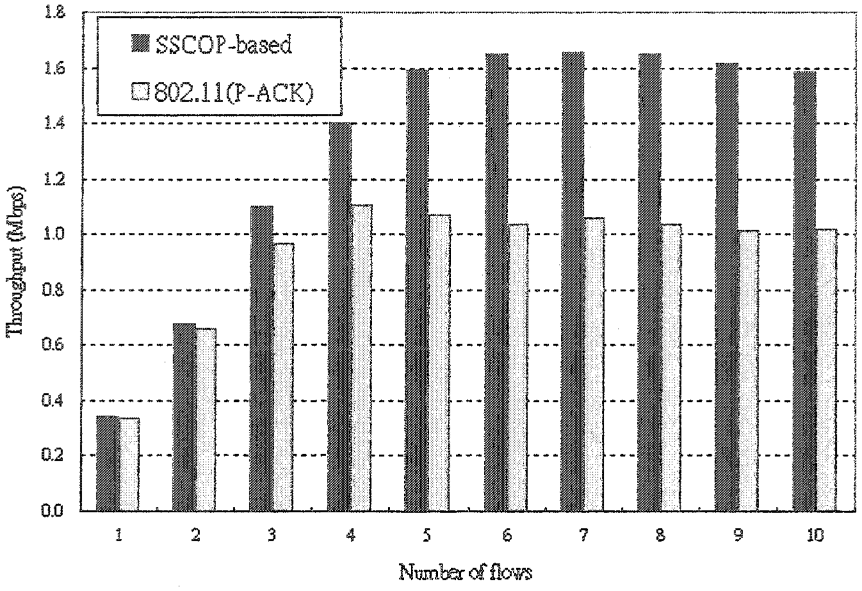


Figure 5.8 Total throughput with increase number of flows at frame loss rate=0.1

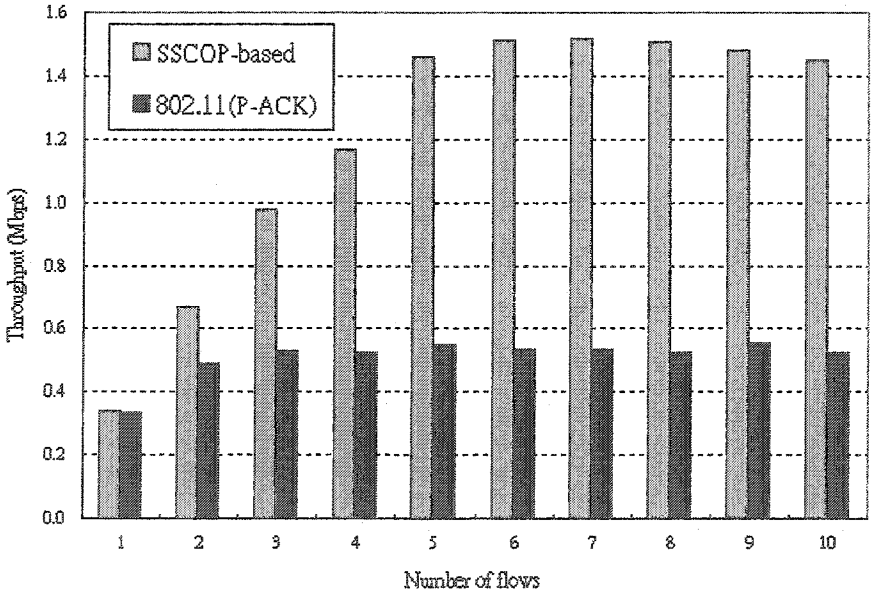


Figure 5.9 Total throughput with increase number of flows at frame loss rate=0.2

CHAPTER 6. SHEPHERD: A LIGHTWEIGHT STATISTICAL AUTHENTICATION PROTOCOL FOR ACCESS CONTROL IN WIRELESS LANS

6.1 Authentication on Wired Networks

Wireless networks have come into wide use in recent years. With more and more applications on wireless networks, the security over wireless networks is becoming a significant issue. The lack of security in the wireless environment has delayed many initiatives in wireless applications, such as e-commerce on wireless devices.

Authentication is one of the basic and necessary security services required by wireless applications. In order to provide security services for applications in the wireless environment, two types of authentication services are necessary [32] : *user authentication*, which provides the systems proof that a user is who they claim to be, and *data authentication*, which consists of two sub-services: *data integrity* and *data origin authentication*. For data integrity, the receiver can be convinced that data was not changed in transit. For data origin authentication, the receiver is assured that data did come from the stated sender [8].

Authentication has several forms in the wired networks. The most common one is username and password. Additional forms of authentication are provided as tokens or digital certificates. In the wireless environment, however, the traditional wired authentication cannot work effectively for the following reasons:

1. Error-prone wireless medium: Unlike wired networks, where error rate is low enough to ignore, the wireless medium is so error-prone that error recovery mechanisms, such as retransmission, or forward error code, are necessary in the wireless world. Furthermore, in an error-prone wireless network, it is difficult to identify whether an attacker or wireless

medium causes frame losses. That is, the characteristics of an error-prone wireless network provide shelters for attackers from detections. To handle errors from wireless mediums for security services is a challenging issue.

2. Mobility: Since most hosts in wireless networks are mobile nodes, the mobility issue has to be taken into great consideration. During a data transmission in a wireless network, different routes and intermediate nodes may be chosen due to mobility. This implies that a sender may authenticate many times to different nodes during a data transmission, which is impossible in traditional wired networks.

3. Computation and communication cost: Traditional security services in wired networks do not consider the power issue. However, most wireless devices, such as personal digital assistants (PDA) and cellular phones, rely on batteries as the source of power, so the power consumption needs to be considered. In general, computation and communication consume most of the power. An ideal wireless protocol requires the least amount of computation and communication, so that it potentially minimizes the power consumption and extends the life of the devices.

6.2 Visitor Networks

With the increasing performance and dropping price of wireless networking equipment over the past few years, wireless local area network (WLAN) has grown significantly. There are more and more locations providing access service to the Internet through WLAN, such as cafés, airport lounges, or campus. Generally, we can call these locations 802.11 hot spots, or a representation of *visitor networks*. Visitor networks, defined as LANs that are most often deployed in public space, enable the public network access on an ad hoc basis [57].

For ISPs deploying visitor networks, the most two important issues are authentication and accounting. In particular, before providing the connecting service to Internet, the ISPs need to validate the users, grant permission to them, and charge them according to their usage. For these emerging requirements, an IETF Working Group, Protocol for Carrying Authentication for Network Access (PANA)[41], is working on a transport protocol to support various types of authentication methods, dynamic service provider selection, and roaming clients. PANA is a network layer messaging protocol for authenticating IP hosts for network access [36]. In essence, PANA does not aim to replace the link layer authentication, but can complement and coexist with the link layer authentication mechanism. Furthermore, PANA does not provide access control and per-packet authentication[70]. Thus, a link layer protocol, potentially under PANA, is needed to efficiently control packets to access the network, i.e. per-packet authentication and access control[99].

Traditional authentication protocols for wired networks do not work well in a wireless environment due to the unique characteristics of wireless networks, such as error-prone wireless transmission medium, node mobility, and power conservation constraints.

For example, in the network layer, IPSec provides the IP security features [40], which is an expensive crypto-based mechanism for wireless hosts. In link layer, the current IEEE 802.11i require AES cryptograph operations, introducing overhead for most power-limited wireless devices [99][71]. In an infrastructure-mode wireless local area network, the access point (AP) is responsible for authenticating a number of mobile nodes communicating with the AP. Current authentication mechanism in 802.11 standard is the Wired Equivalent Privacy(WEP)[38], whose flaws have been pointed out in [20].

In this chapter, we propose a lightweight statistical authentication protocol, called Shepherd. The connotation of authentication is like a Shepherd to discriminate among similar sheep according to the limited information of their characteristics. Based on that, Shepherd determines the authenticity of a station as a probability value. The limited information for authentication results from a small amount of transmission and error-prone wireless networks. To design Shepherd for wireless networks, we consider some unique characteristics, e.g error-prone medium, node mobility, and the power conservation constraints. Shepherd provides a *per-frame authentication* at link layer for wireless networks. The major goal of the protocol is to determine the authenticity of a mobile node in an error-prone wireless environment and to provide a basis for access control. When the system detects an illegal node, some countermeasures against it can be triggered. The main challenge of designing this protocol is to effectively tell the authentication bit errors resulting from the wireless errors apart from those coming from attackers. We

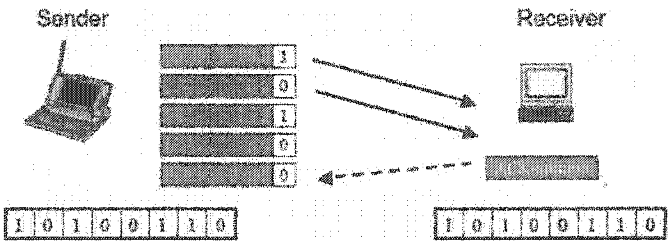


Figure 6.1 A simple scenario of the lightweight authentication protocol

study this protocol under three synchronization schemes. Through our analysis, we show that this lightweight authentication protocol performs well in terms of computational and communication cost, synchronization efficiency, and protocol operation secrecy. We will show that this lightweight statistical authentication protocol is practical for implementation in 802.11 WLAN.

6.3 Proposed Authentication Protocol: Shepherd

Unlike traditional challenge-response authentication protocols, the proposed protocol determines the legitimacy of a station by continuously checking a series of packets transmitted by the station. As shown in Fig.6.1, in the beginning, both the sender and the receiver create a random bit stream called the authentication stream as well as a pointer pointing to the first bit of the stream. Since the sender and receiver have the same seed value and stream generator, the constructed authentication streams are the same. The sender sends each frame with one additional bit and the bit value is equal to the value of the authentication bit pointer. When the receiver receives a frame successfully, the receiver checks the bit value of the frame with its pointer value. After checking a number of bits, the receiver can use the checking results as a measure of the sending station being an attacker.

We assume the sender and receiver pointers are synchronized initially and the bit error rate (BER) in a wireless network is known. The frame loss rate due to wireless errors can be derived by a given bit error rate and frame length. In the three synchronization schemes, since the sequence number of each frame is easily modified in a wireless network, the sequence number is not faithful to authentication protocols, so we assume the sequence number is unknown and not used by Shepherd.

In an error-prone wireless network, frames are frequently lost due to wireless error. The frame losses cause sender's and receiver's pointers to be unsynchronized in the protocol, that is, the *non-synchronization problem*. Thus, we develop three synchronization schemes to solve this problem.

The objective of the three synchronization schemes is to synchronize sender's and receiver's pointers. Among three synchronization schemes, the main difference is in the synchronization and the sequence of pointer movements. For each scheme, we present each scheme operation followed by an example and its formal algorithm.

6.3.1 Scheme 1: Sender's Pointer Jumps Forward (*SPF)*

Initially, the sender's pointer, P_s, and the receiver's pointer, P_r, are synchronized, that is, $P_s = P_r$. Moreover, the bit value that P_s points to, $Bit[P_s]$, equal to the bit value that P_r points to, $Bit[P_r]$, that is, $Bit[P_s] = Bit[P_r]$. The sender sends each frame with a bit value, $Bit_{frame} = Bit[P_s]$. After sending a frame and before receiving an acknowledgement, the sender keeps P_s the same. When receiving a frame, the receiver checks Bit_{frame} with $Bit[P_r]$. If $Bit_{frame} = Bit[P_r]$, P_r moves forward a step, that is $P_r = P_r + 1$, and the receiver replies the sender with an $ACK_{success}$ frame. If $Bit_{frame} \neq Bit[P_r]$, P_r still moves forward a step but the receiver replies the sender with an $ACK_{failure}$ frame. If the receiver does not receive a frame successfully due to the interference, P_r does not move. Then, the sender may trigger a synchronization process according to the received acknowledgement. When the sender receives an $ACK_{success}$ frame, it means that two bit values match and the sender does not need a synchronization. As normal, the sender moves P_s forward a step, that is $P_s = P_s + 1$. At this time, P_s and P_r are in synchronization again, $P_s = P_r$, and ready for the next frame exchange. In contrast, when receiving an $ACK_{failure}$ frame, the sender initiates a synchronization action—sender moves P_s to the next opposite bit (**NOB**) plus one. The NOB refers to the closest bit with opposite value of current one. For example, consider the case of the bit stream 00001100. The pointer is at the first bit, the NOB is at 5 and synchronization will move the pointer to the opposite bit plus one (from 1 to 6).

An example of scheme 1 is shown in the Fig.6.2. We define the non-synchronization index

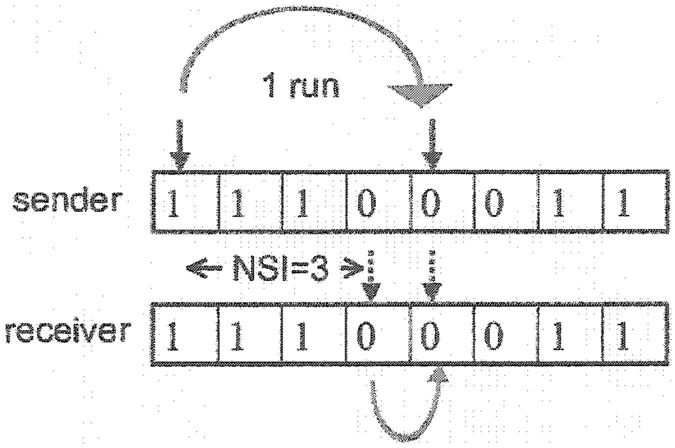


Figure 6.2 An example of the synchronization for scheme 1

(**NSI**) to be the distance between the P_s and P_r. Initially, $P_s = P_r = 1$. After three successive ACK frame losses, $P_s = 1$, $P_r = 4$, and $NSI = 3$.When the fourth $ACK_{failure}$ frame reaches to the sender, P_s moves to the $NOB + 1$, and both P_s and P_r are synchronized at 5. In scheme 1, the synchronization is initiated at the sender side and the Sender's Pointer jumps Forward, so we call scheme 1 **SPF**. Some observations and properties discussed in [95]. However, it has a drawback on the sender awareness. In scheme 1, the sender is aware of the results of matching bit. Illegitimate senders may attack the system by using this information. To hide the result information from the sender, we have to shift the synchronization to the receiver side. Thus, we develop scheme 2 for this drawback.

Algorithm 1: Sender's Pointer Jumps Forward (SPF)

```
Receiver receives a data frame
if $Bit_{frame} = Bit[P_r]$ then
    $P_r++$
    reply sender with $ACK_{success}$
else
    $P_r++$
    reply sender with $ACK_{failure}$

Sender receives an ACK frame
if receives $ACK_{success}$ then
    $P_s++$
else
    $P_s = NOB + 1$
```

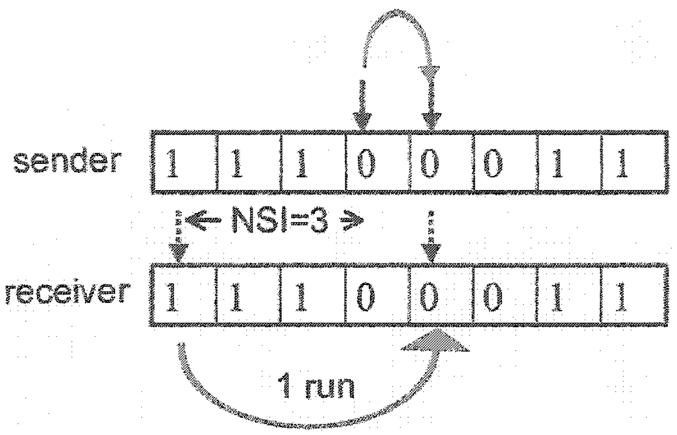


Figure 6.3 An example of the synchronization for scheme 2

6.3.2 Scheme 2: Receiver's Pointer Jumps Forward (*RPF*)

Initially, similar to scheme 1, $P_s = P_r$ and $Bit[P_s] = Bit[P_r]$. The sender sends each frame with a bit value, $Bit_{frame} = Bit[P_s]$. Just after sending a frame, the sender moves P_s forward a step, $P_s = P_s + 1$. When receiving a frame, the receiver checks Bit_{frame} with $Bit[P_r]$. If $Bit_{frame} = Bit[P_r]$, P_r moves forward a step, that is $P_r = P_r + 1$, and the receiver replies the sender with an ACK. If $Bit_{frame} \neq Bit[P_r]$, the receiver initiates the synchronization— moves P_r to the $NOB + 1$ and replies the sender with an ACK. If the receiver does not receive a frame successfully due to the interference, P_r does not move. Then, the sender keeps P_s the same when receiving the ACK, since it moved immediately after sending. If the sender does not receive ACK, P_s does not move.

An example of scheme 2 is given in the Fig.6.3. Initially, $P_s = P_r = 1$. After three successive DATA frame losses, $P_s = 4$, $P_r = 1$, and $NSI = 3$.When the fourth DATA frame reaches to the receiver, P_r moves to the $NOB + 1$, and both P_s and P_r are synchronized at 5. In scheme 2, the synchronization is initiated at the receiver side and the Receiver's Pointer jumps Forward, so we call scheme 2 **RPF**. Obviously, scheme 2 removes the drawback of sender awareness by shifting the duty of synchronization from the sender to the receiver. However, scheme 2 has an inherent drawback. In the above example, we observe that the out-of-sync event is caused by the *DATA frame loss.* In scheme 1, however, the out-of-sync event is caused by the *ACK frame loss.* It is apparent that the DATA frame is more easily lost than the ACK frame at the same

BER due to the different frame length. That is, there are more out-of-sync events in scheme 2 than in scheme 1. For this concern, we develop the scheme 3. Scheme 3 prevents the sender awareness and makes out-of-sync events caused by ACK frame loss.

Algorithm 2: Receiver's Pointer Jumps Forward (RPF)

```
*Sender sends a data frame*
$P_s + +$
*Receiver receives a data frame*
**if** $Bit_{frame} = Bit[P_r]$ **then**
    $P_r + +$
    reply sender with ACK
**else**
    $P_r = NOB + 1$
    reply sender with ACK
```

6.3.3 Scheme 3 : Receiver's Pointer Jumps Backward (*RPB*)

Initially, $P_s = P_r$ and $Bit[P_s] = Bit[P_r]$. The sender sends each frame with a bit value, $Bit_{frame} = Bit[P_s]$. Like scheme 1, after sending a frame and before receiving an ACK, the sender keep P_s the same. When receiving a frame, the receiver checks Bit_{frame} with $Bit[P_r]$. If $Bit_{frame} = Bit[P_r]$, P_r moves forward a step, that is $P_r = P_r + 1$, and the receiver replies the sender with an ACK . If $Bit_{frame} \neq Bit[P_r]$, the receiver initiates the synchronization— moves P_r *backward* to the closest opposite bit plus one and replies the sender with an ACK. Then, the sender moves P_s forward a step when receiving the ACK. If the sender does not receive ACK, P_s does not move.

An example of scheme 3 is given in the Fig.6.4. Initially, $P_s = P_r = 1$. After three successive ACK frame losses, $P_s = 1$, $P_r = 4$, and $NSI = 3$.When the fourth DATA frame reaches to the receiver, P_r moves backward to the closest opposite bit plus one, and both P_s and P_r are synchronized at 2. In scheme 3, the synchronization is initiated at the receiver side and the Receiver's Pointer jumps Backward, so we call scheme 3 **RPB**. As we anticipate, scheme 3 successfully makes out-of-sync event caused by ACK frame loss and avoid the sender awareness.

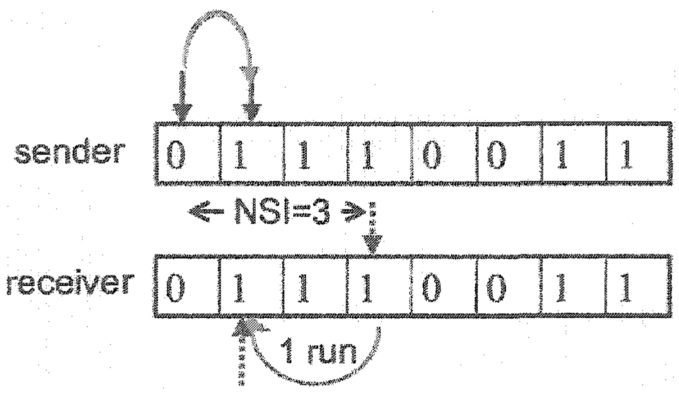


Figure 6.4 An example of the synchronization for scheme 3

Algorithm 3: Receiver's Pointer Jumps Backward (RPB)

```
*Receiver receives a data frame*
**if** $Bit_{frame} = Bit[P_r]$ **then**
    $P_r ++$
    reply sender with ACK
**else**
    $P_r = NOB_{back} + 1$
    reply sender with ACK
*Sender receives an ACK frame*
$P_s ++$
```

6.3.4 Discussion

We apply the following five aspects to compare the three proposed schemes. Table 6.1 displays the comparison results.

1. *Act first*: In the frame exchange, it tells which host's pointer acts first.

2. *Sender awareness*: Whether the sender knows the checking results. In scheme 1 and 3, the sender runs the synchronization when receiving $ACK_{failure}$, so the sender is aware of the checking result. Since the checking results may be used for malicious hosts, an ideal scheme should keep the sender unaware of the checking results.

3. *Reason for non-synchronization*: Specifies which type of frame loss causes non-synchronization. In schemes 1 and 3, the reason for non-synchronization is the loss of ACK frame. In scheme 2, data frame loss causes non-synchronization. At a fixed wireless bit error rate, the larger

Table 6.1 Comparison of three proposed schemes

Scheme	1	2	3
Name	SPF	RPF	RPB
Act first	Receiver	Sender	Receiver
Sender awareness	Yes	No	No
Reason for non-sync	ACK	Data	ACK
Jump direction	Forward	Forward	Backward(back)

frame has the higher frame loss rate[58]. So, the data frame loss rate is higher than the ACK frame loss rate at the sameBER (Bit Error Rate). To minimize the occurrence of non-synchronization, the protocol, whose non-synchronization is caused by ACK loss, is better than the protocol, whose non-synchronization is caused by data frame loss.

4. *Jump direction*: The three schemes are classified into two categories according to jump directions: forward or backward. In schemes 1 and 2, the pointer jumps forward in synchronization. In scheme 3, the pointer jumps backward in synchronization.

6.4 Numerical Analysis

To validate an analysis of the proposed theorems, we use Mathematica software [98] to generate the numerical analysis results. We study the impacts of different w,s, and BER on $Pr(H = legal|w, s)$. In the following analysis, $G = 10$.

6.4.1 BER

Fig.6.10 shows the $Pr(H = legal|w, s)$ of scheme 1 in the range of s from 0 to 10, when $BER = 10^{-4}, 5 \cdot 10^{-5}$,and 10^{-5} and $w = 50$. When $s < 5$, three flat curves are very close to 1. The curve of largest BER, i.e. 10^{-4}, drops at s=5 and approaches to 0 at $s = 6$. Similarly, the other two curves drop at 7 and 8. The curve dropping at small s means the $Pr(H = legal|w, s)$ is more sensitive, since the receiver requires a small number of synchronization runs to identify the sender as illegal. As expected, the results show higher BER requires larger value of s to make $Pr(H = legal|w, s)$ close to 0. That is, at higherBER, receiver requires more run of

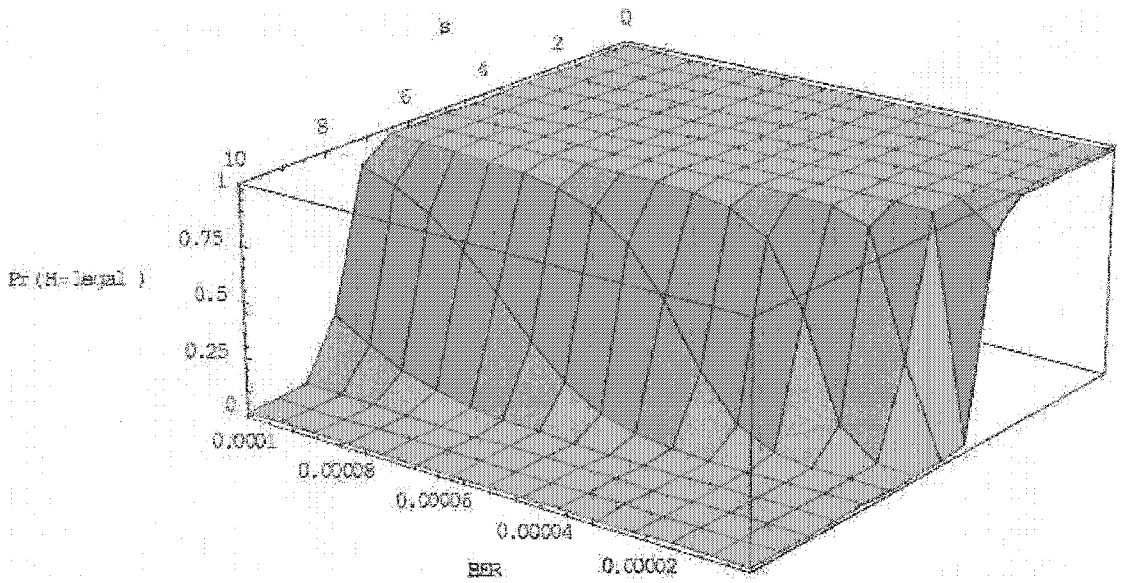


Figure 6.5 $Pr(H = legal|w, s)$ in scheme 1 with different s andBER

synchronization to identify the node as illegitimate one. Thus, the impact of high BER is to decrease the sensitivity of the protocol. Due to constraints of space, we only show the analysis results of scheme 1 and scheme 2 and 3 conform with the results.

6.4.2 Synchronization Runs

Fig.6.5 shows the probability of host H being legal when s is in a range from 0 to 10 and $w = 50$. For example, when $r = 2 \cdot 10^{-5}$ and $s > 6$, $Pr(H = legal|w, s)$ is lower than 1%. When $s < 3$, the probability is almost 100%. When $r = 10^{-4}$ and $s > 8$, $Pr(H = legal|w, s)$ is lower than 1%. When $s < 5$, the probability is almost 100%. These numerical results are reasonable, because more run of sync runs are required to judge the authenticity of a host at a higher frame loss rate.

6.4.3 Checked Frames

We discuss the impact of the number of checked frames, w, as follows. Apparently, checking more frames in authentication take longer time, but we want to see whether it is worthwhile. Fig.6.6 shows the $Pr(H = legal|w, s)$ of scheme 1 in the range of w from 10 to 80 and the range

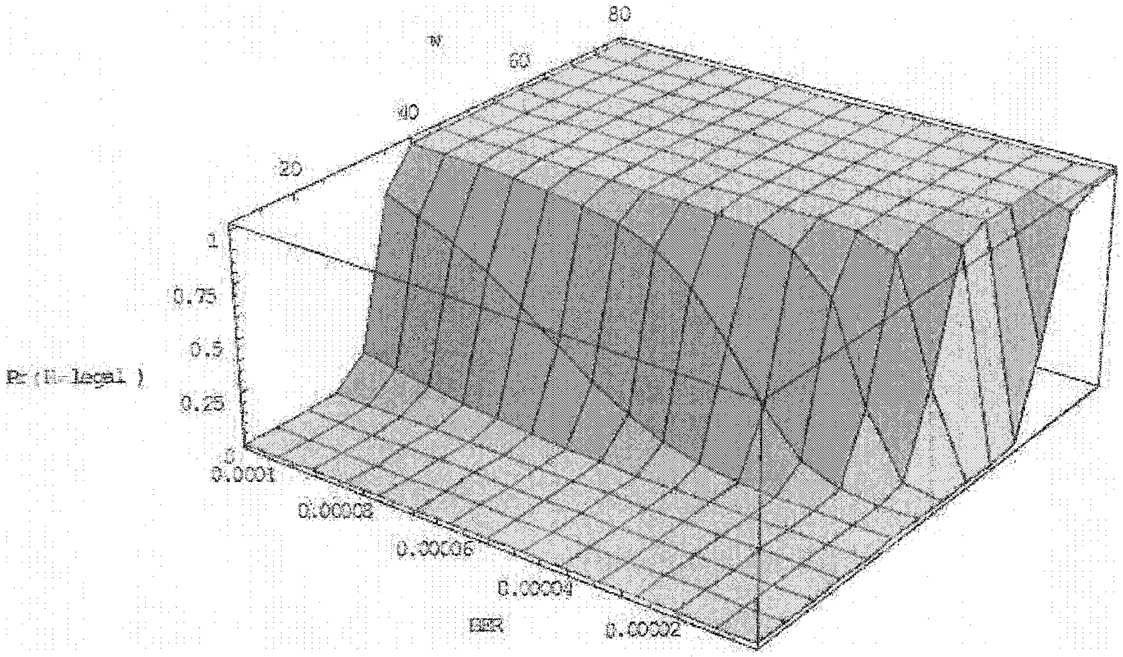


Figure 6.6 $Pr(H = legal|w, s)$ in scheme 1 with different w andBER

of BER from 10^{-4} to 10^{-5}, when $s = 5$. $Pr(H = legal|w, s)$ increases with increasing w, because a large w causes smaller ABER, when s is fixed, which leading to higher $Pr(H = legal|w, s)$. Moreover, $Pr(H = legal|w, s)$ increases with a increasingBER, which means more mismatches can be due to wireless error.

6.4.4 Schemes Comparison

In all above analysis, we present only the $Pr(H = legal|w, s)$ of scheme 1. Fig.6.7 shows the $Pr(H = legal|w, s)$ for threes schemes, when $w = 15$ and $BER = 10^{-4}$. The curves of scheme 1 and 3 are very close and drop more sharply than that of scheme 2. This means $Pr(H = legal|w, s)$ in scheme 2 does not change quickly with increasing s. Thus, it is more difficult for scheme 2 to tell the node from legal nodes than scheme 1 and 3.

6.5 Statistical Method for Authenticity of a Mobile Node

This section discusses the process of the sender's legitimacy judgment by the receiver. All symbols used in the chapter are listed in Table6.2.

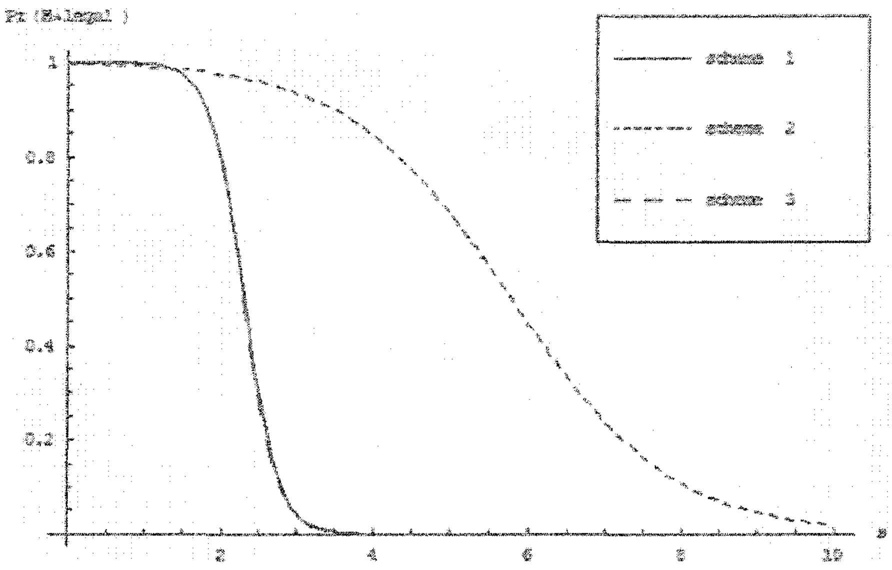


Figure 6.7 $Pr(H = legal|w, s)$ in three schemes with different s

6.5.1 Assumptions

We made two assumptions in our analysis. The first assumption is that the system is in synchronization whenever we apply the statistical methods. In reality, it is impossible to guarantee synchronization at any time of the process. For this assumption, we do a check whenever applying statistical methods. If there is no authentication bit error (ABE) in the last n received frames, we have the probability of synchronization equal to $(1 - 2^{-n})$.

When the probability of synchronization is larger than or equal to a threshold, we assume the system is synchronized after the last received frame, and apply the statistical methods. When the probability is lower than a threshold, i.e. there are a large number of ABEs in w, the statistical method can not be used. We define the authentication bit error rate $\delta = \frac{s}{w}$, that is, the number of ABE within w received frames, s, over w. There is a theoretical limitation of the statistical method: authentication bit error rate due to the wireless errors must be lower than 0.5. The reason is that when δ is greater than 0.5, it becomes impossible to tell ABEs due to the wireless errors apart from those due to attackers.

The second assumption is that no frame loss happens in the process of synchronization. In other words, in the case of $NSI = n$ due to continuous n frame losses, no frame loss happens

Table 6.2 Notations

Notation	Meaning
δ	Average Authentication Bit Error Rate ($ABER$)
ABE	Authentication Bit Error
NSI	Non-Synchronization Index, the distance between the sender and receiver pointers.
L_{data}	Length of Data Frame
L_{ACK}	Length of ACK Frame
BER	Bit error rate
r	Frame loss rate
w	Authentication window size
s	Number of ABEs in w
s_i	Number of ABEs, caused by frame loss segment, with $NSI = i$ in w
b_i	Number of segments of frame loss with $NSI= i$ in w
h_{ji}	Number of ABEs, caused by the $j'th$ frame loss segment, with $NSI= i$
G	Maximum length of a frame loss segment.

before the system is synchronized, i.e. $NSI = 0$. This assumption is to simplify the analysis of statistical methods.

6.5.2 SPF Scheme

In scheme 1, we use a statistical method to determine the authenticity of a station. The main objective of this statistical method is to determine whether the sending station is an attacker or not, according to the information at the receiver. This method is able to determine the authenticity of a station as a probability value. It appears that the number of synchronization runs is a measure of the sending station being an attacker. In scheme 1, there can be non-synchronization in the protocol due to frame loss in the wireless medium.

Theorem 1 *For a sending mobile station H, assume that* a priori *probability of station H to be an attacker is 50%, that is, $Pr(H = illegal) = 50\%$ and $Pr(H = legal) = 50\%$, the probability of this mobile station H being a legitimate one when the number of synchronizations* *is s,*$Pr(H = legal|w, s)$, *is given by*

$$Pr(H = legal|w, s) = \frac{\delta^s(1-\delta)^{w-s}}{2^{-w} + \delta^s(1-\delta)^{w-s}} \tag{6.1}$$

, *where* δ *is the average authentication bit error rate and calculated as*

$$\delta = \sum_{i=1}^{G}[(L_{ACK} \times BER)^i \times \frac{i+1}{2}] \tag{6.2}$$

To prove Theorem 1, we will use the following four lemmas. Consider the case where the sender is a legal station. The only factor that increases the synchronizations is the frame loss rate.

Lemma 1 *If the system is not synchronized and the* NSI *value is* U, *then one or more, up to* U, *runs of synchronization are required.*

Proof: At each synchronization run, both the sender's and the receiver's pointers advance. As specified in Lemma 1, the sender pointer is at least one greater than the receiver pointer, since the sender jumps its pointer to opposite bit plus one and the opposite bit is one or more bits ahead. Thus it is obvious that at least one synchronization run makes the sender jump $U + 1$ bits. For example, the bit stream is `111111000` and the sender is at the first bit and the receiver is at the seventh bit, only one synchronization run is needed to reach synchronization.

In the worst case, the NSI value decreases by only one after a synchronization run. Thus, at most U runs of synchronization are needed when $NSI = U$. For example, as shown in Fig.6.8, if the bit stream is `1010011` and the NSI value is 3 with the sender pointer at first bit and the receiver pointer at the fourth bit, after one run of synchronization, the sender jumps to the third bit and the receiver jumps to the fifth bit. After the second synchronization, the sender jumps to the fifth bit and the receiver to the sixth bit. After the third synchronization, the sender and the receiver finally jump to the same place, the seventh bit, and are synchronized. Thus, we need three runs of synchronization when the NSI value is three. ■

The following conclusion is obtained from the lemma. After one synchronization run, the minimum decrease of the NSI value is one and the maximum is U, i.e. the new $NSI = 0$.

Lemma 2 *Consider checking an authentication bit stream. In the case of no continuous* ACK *loss, when the sender and the receiver are in a synchronization state, the sum of the lost frame,* m, *is equal to the number of runs of the synchronization algorithm,* s, *i.e.,* $s = m$.

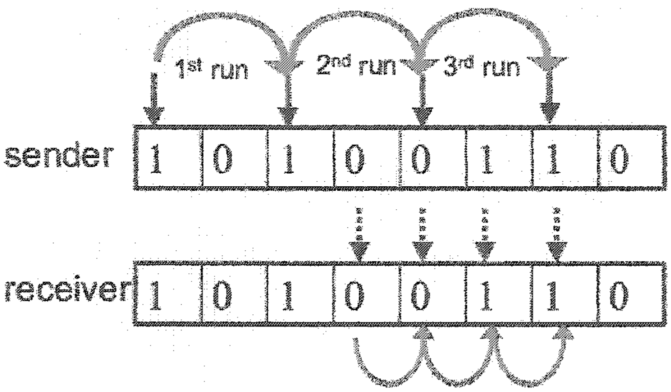


Figure 6.8 An example of Lemma 1 ($NSI = 3, s = 3$)

Proof: If there is no continuous ACK loss and the system is synchronized at the last authentication bit, it is obvious that an ACK loss causes the NSI value to increase by one. To achieve synchronization, i.e. to make $NSI = 0$, one synchronization run is required. Then both sender and receiver return to synchronization state again. Thus, the sum of lost ACK frame with receiving w frame is equal to the runs of the synchronization algorithm. ■

Lemma 3 *Consider a series of continuous ACK losses with the length n. When the sender and the receiver are in a synchronization state, the average number, $E[s]$, of runs of the synchronization algorithm for the series of continuous ACK losses is equal to $(n+1)/2$, that is,*

$$E[s] = \frac{n+1}{2} \tag{6.3}$$

Proof: We use Mathematical Induction to prove this lemma as follows.

1. When $n = 1$, it is true , that is, $E[h_{j1}] = 1$, because of lemma 2.

2. Assume equation 6.3 holds for $n = k$, that is,

$$E[h_{jk}] = (k+1)/2. \tag{6.4}$$

3. When $n = k+1$, we divide this $(k+1)$ continuous frame loss segment into two parts, that is, the previous k continuous frame loss segments and the latest added-on frame loss.

$$h_{j(n+1)} = h_{jn} + m_{j(n+1)} \tag{6.5}$$

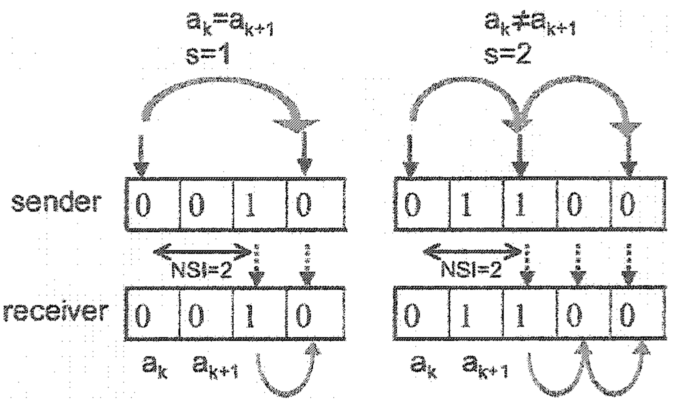


Figure 6.9 Two examples in Lemma 3 (left: $NSI = 2, s = 1$; right: $NSI = 2, s = 2$)

where $m_{j(n+1)}$ is the number of ABEs caused by this added-on frame loss.

The latest added-on frame loss may change the total number of ABEs, $h_{j(k+1)}$. In lemma 1, we have proven that at most n ABEs are required for n continuous frame loss. We can extend lemma 1 to that one added-on frame loss can lead to either none or one more ABEs.

Either zero of one ABE caused by the added-on frame loss is determined by the pattern of authentication bits between sender's and receiver's pointers. Let a_k be the bit, which is pointed by sender and let a_{k+1} be the bit next to a_k. We observe that, when a_k is equal to a_{k+1} this latest added-on frame loss will not cause one additional ABE. On the other hand, when a_k is not equal to a_{k+1} this latest added-on frame loss will cause one additional ABE.

$$m_{j(n+1)} = \begin{cases} 0 & , a_k = a_{k+1} \\ 1 & , a_k \neq a_{k+1} \end{cases} \tag{6.6}$$

For example, in the Fig.6.9, a_k is the first bit and a_{k+1} is the second bit of the bit stream. In the case of $a_k = a_{k+1}$ (left figure), after one synchronization run, that is, $s = 1$, system reaches synchronization. In the case of $a_k \neq a_{k+1}$, two synchronization runs are required to reach synchronization.

Since the authenticate bit is generated randomly, the probabilities of equality and inequality are 50%. We have $Pr(a_k = a_{k+1}) = 0.5$ and $Pr(a_k \neq a_{k+1}) = 0.5$. Thus, the expected value of $m_{j(n+1)}$ is:

$$\begin{aligned} E[m_{j(n+1)}] &= Pr(a_k = a_{k+1}) \times 0 + \\ &\quad Pr(a_k \neq a_{k+1}) \times 1 \qquad (6.7) \\ &= 0.5 \qquad (6.8) \end{aligned}$$

Then, we have

$$\begin{aligned} E[h_{j(n+1)}] &= E[h_{jn} + m_{j(n+1)}] \qquad (6.9) \\ &= E[h_{jn}] + E[m_{j(n+1)}] \qquad (6.10) \\ &= E[h_{jn}] + 0.5 \qquad (6.11) \end{aligned}$$

According to equation (6.4) , $E[h_{jk}] = (k+1)/2$, we have

$$\begin{aligned} E[h_{j(n+1)}] &= \frac{k+1}{2} + \frac{1}{2} \qquad (6.12) \\ &= \frac{(k+1)+1}{2} \qquad (6.13) \end{aligned}$$

Hence, in accordance with Mathematical Induction, equation (6.3) is proved.

■

Lemma 4 *When the receiver successfully receives w data frames, the expected value of segments of frame loss with $NSI = i$ in w is:*

$$E[b_i] = w \times r^i(1-r) \tag{6.14}$$

The proof of the lemma can be found in 6.10.

Lemma 5 *Consider checking an authentication bit stream. Let the frame loss rate due to the wireless errors be r. In case of continuous ACK losses, when the sender and the receiver are in a synchronization state, the average authentication bit error rate due to wireless error, δ , can be derived as follows:*

$$\delta = \sum_{i=1}^{G}(r^i \times \frac{1+i}{2}), \tag{6.15}$$

where G is the maximum length of a frame loss segment.

The proof of above lemmas can be found in 6.10.

Proof of Theorem 1: According to Bayes' Theorem, we have

$$Pr(H = illegal|w, s) = \tag{6.16}$$
$$\frac{Pr(w,s|H=illegal) \times Pr(H=illegal)}{Pr(w,s|H=illegal)Pr(H=illegal)+Pr(w,s|H=legal)Pr(H=legal)}$$

First let us assume that the sender is an attacker, that is, it does not know the authentication stream. In this case, the probability of s ABEs in w when H is illegal

$$Pr(w, s > 0|H = illegal) = \begin{pmatrix} w \\ s \end{pmatrix} \times 2^{-w} \tag{6.17}$$

This is because the attacker does not know the authentication bit stream, and it does not matter how the attacker takes action to generate the next bit, either randomly choosing zero/one or moving the next opposite bit +1. So Formula (6.17) is reasonable. According to the five lemmas, we can calculate δ from equation (6.2), and then it is easy to know the probability of the number of synchronization runs, s, in w,

$$Pr(w, s|H = legal) = \begin{pmatrix} w \\ s \end{pmatrix} \times \delta^s(1-\delta)^{w-s} \tag{6.18}$$

Combine (6.16), (6.17), and (6.18), and we can derive (1) easily.
Since $Pr(H = illegal|w, s) = 1 - Pr(H = legal|w, s)$, we can derive the probability of H being an attacker when the number of synchronizations being s is given by

$$Pr(H = illegal|w, s) = \frac{2^{-w}}{2^{-w} + \delta^s(1-\delta)^{w-s}} \tag{6.19}$$

Hence, Theorem 1 is proved.

6.5.3 RPF Scheme

Although the jump behaviors of scheme 1 are quite different from scheme 2, their statistical methods are similar. We observe that the jump behavior in scheme 2 is the case of scheme 1, where sender and receiver switch their roles. One main difference between analysis of scheme 1 and 2 is the reason for non-synchronizations. As we mentioned in Section 6.3, data frame loss causes non-synchronization in scheme 2, instead of ACK loss in scheme 1. Thus, some modifications are added in the analysis for scheme 2. We have the following theorem for scheme 2.

Theorem 2 *For a sending mobile station H, assume that* a priori *probability of station H to be an attacker is 50%, that is, Pr(H = illegal) = 50% and Pr(H = legal) = 50%, the probability of this mobile station H being a legitimate one when the number of synchronizations is s, Pr(H = legal|w, s) , is given by*

$$Pr(H = legal|w, s) = \frac{\delta^s(1-\delta)^{w-s}}{2^{-w} + \delta^s(1-\delta)^{w-s}}, \tag{6.20}$$

where δ is the average authentication bit error rate and calculated as

$$\delta = \sum_{i=1}^{G}\{(L_{data} \times BER)^i[1-(L_{data} \times BER)]\frac{i+1}{2}\} \tag{6.21}$$

In scheme 2 and 3, when receivers detect ABE, one run of synchronization is triggered at the receiver side. Thus, ABE number is the same as sync and Lemma 4 cannot be applied in scheme 2 and 3. We develop Lemma 6 for scheme 2 and 3.

Lemma 6 *Consider checking an authentication bit stream. Let the frame loss rate due to the wireless errors be r. In case of continuous ACK loss, when the sender and the receiver are in synchronization , the average authentication bit error rate due to wireless error, say δ , can be derived as follows:*

$$\delta = \sum_{i=1}^{G} r^i(1-r) \times \frac{i+1}{2}, \tag{6.22}$$

where G is the maximum length of a frame loss segment.

The proof of the lemma is given in 6.10. Since lemma 6 holds in scheme 2, the proof of Theorem 2 is similar to that of Theorem 1.

6.5.4 RPB Scheme

Although the jump direction in scheme 3 are opposite to that in scheme 2 [1], their statistical methods are the same except for the frame loss rate. In particular, since ACK loss causes non-synchronization in scheme 3, r represents ACK frame loss rate, instead of data frame loss rate

[1] Scheme 2 is forward and scheme 3 is backward

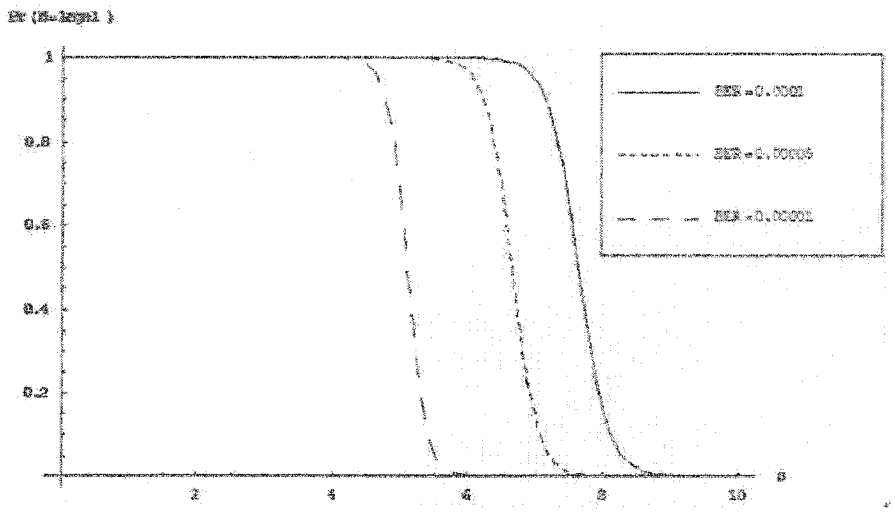


Figure 6.10 $Pr(H = legal|w, s)$ in scheme 1 with different s

in scheme 2. We observe that the lemma 3 in scheme 1 also holds both in scheme 2 and 3. Thus, scheme 3's statistical method is similar to scheme 2's. We have the following theorem for scheme 3.

Theorem 3 *For a sending mobile station H, assume that* a priori *probability of station H to be an attacker is 50%, that is, $Pr(H = illegal) = 50\%$ and $Pr(H = legal) = 50\%$, the probability of this mobile station H being a legitimate one when the number of synchronizations is s, $Pr(H = legal|w, s)$, is given by*

$$Pr(H = legal|w, s) = \frac{\delta^s(1-\delta)^{w-s}}{2^{-w} + \delta^s(1-\delta)^{w-s}} \tag{6.23}$$

where δ is the average authentication bit error rate and calculated as

$$\delta = \sum_{i=1}^{G}\{(L_{ACK} \times BER)^i[1 - (L_{ACK} \times BER)]\frac{i+1}{2}\} \tag{6.24}$$

Since lemma 6 holds in scheme 3, the proof of Theorem 3 is similar to that of Theorem 1.

6.6 Simulation Results

To evaluate the three schemes under more realistic cases, we developed a C-based simulator to simulate a legitimate host's synchronization behavior of the three schemes in an error-prone wireless network. We compared the performances of the three schemes at different error rates. A desirable synchronization scheme can often keep the system in synchronization or cause the least number of authentication bit errors even when the wireless error rate is high. Thus, to measure the effectiveness of the synchronization scheme, we use two metrics: *synchronization rate*, R_{sync} ,and *authentication bit error rate*, δ.

Synchronization rate, R_{sync}, is defined as follows: in the last w frames successfully received by the receiver, the number of frames which are received when the system is in synchronization [2]. Notice that, in reality, it is impossible for the sender or receiver to know whether the current status is in synchronization or not. The sender or receiver only knows the results of checking authentication bits. If the bits are matched, the system may still be in non-synchronization. Thus, we can only have synchronization rate through simulation, though it is an accurate metric to evaluate the synchronization scheme.

On the other hand, authentication bit error rate, δ, is the information that can be observed at the receiver. Authentication bit error rate is defined as follows: in the last w frames successfully received by the receiver, the number of frames, whose authentication bit is mismatched with the receiver's. Since when sender's and receiver's bits are not matched, the system must be in non-synchronization, we have $\delta \geq (1 - R_{sync})$. This inequality can be used to roughly validate our simulation results.

In each scenario, involving different wireless error parameters and random number generator seeds, the length of the bit stream is 10^9 and the window size is 50. To see the impact of the data frame length, we use two different data frame lengths: 300 bytes and 1000 bytes[3]. In the scenario for long data frame, the data frame length is fixed to be 300 bytes. In the scenario for short data frame, the data frame length is fixed to 1000 bytes.

Fig.6.11 shows the authentication bit error rate for three schemes at different wireless bit error rates with a specific data frame length. Both curves of scheme 2 increased more rapidly than scheme 1 and 3. In scheme 2, the curve of 1000 bytes data frame length went up at a higher slope than that of 300 bytes and reached a maximum, 0.5, at $BER = 6.3 \cdot 10^{-5}$. The

[2] That is, sender's and receiver's pointers are at the same place, $P_s = P_r$

[3] In the IEEE 802.11 WLAN standard, the data frame length is range from 34 to 2346 bytes and ACK frame is 18 bytes.

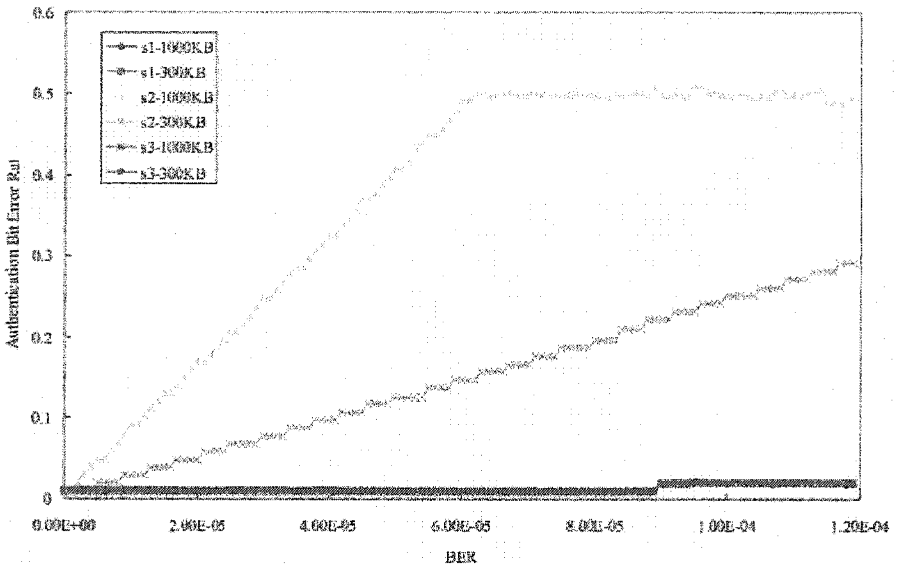


Figure 6.11 Authentication bit error rates for three schemes at different BER

other two curves rose at a slower rate. Notice that since a reasonable range of wireless bit error rate is from 10^{-5} to 10^{-9}, we can derive that the probability of ACK frame loss rate larger than 0.1 in reality is lower than 10^{-3}. To deeply investigate the three schemes and evaluate their performance, we did a simulation at a high ACK frame loss rate, which can make the non-synchronization problem worse, but does not frequently happen in a real wireless network.

Fig.6.12 shows the authentication bit error rate for three schemes at different ACK frame loss rates with a specific data frame length. Scheme 2 increased rapidly, but the other curves went up at similar slopes and reached a maximum as ACK frame loss rate is 0.48.

As we discussed before, the synchronization rate is a more accurate metric for evaluation. Fig.6.13 shows the synchronization rate for three schemes at different wireless bit error rates with a specific data frame length. Both curves of scheme 2 decreased more rapidly than others. In scheme 2, the curve of 1000 bytes data frame length went down at a higher slope than that of 300 bytes and reached a minimum, at$BER = 6.3 \cdot 10^{-5}$. The other three curves fell at a low rate.

Fig.6.14 shows the synchronization rate for three schemes at different ACK frame loss rates with a specific data frame length. Scheme 2 presented a sharp drop and the other curves went

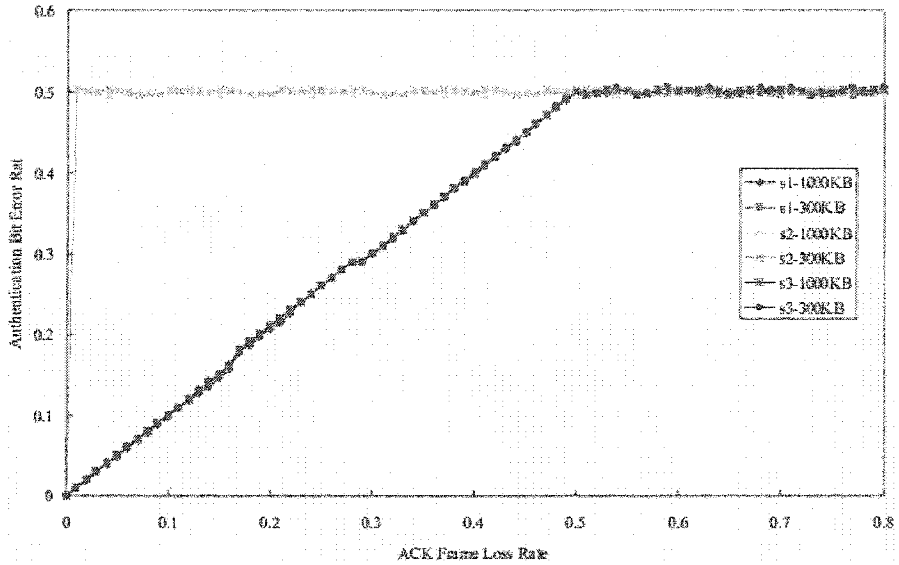


Figure 6.12 Authentication bit error rates for three schemes at different ACK frame loss rate

down gradually. Scheme 1 reached a minimum as ACK frame loss rate reached 0.49.

The simulation results indicate that scheme 1 and 3 are always able to synchronize more efficiently than scheme 2, and scheme 3 performs better than scheme 2 at a high ACK frame loss rate. The results agree well with our numerical analysis. For the data frame length, the results imply that a large data frame length appears to reduce the synchronization capability of scheme 2 because of a higher data frame loss rate. Data frame length does not impact the other schemes.

6.7 Implementation Considerations

We describe how to implement the three proposed schemes within the existing IEEE 802.11 protocol [38]. The extra bit needed for authentication using the new protocol is taken from the existing frame structure of IEEE 802.11. This means the proposed scheme does not modify the frame structure and is compatible with legacy devices which do not use the authentication scheme. As shown in Table 6.3 and Fig.2.1, two reserved types are used to represent the two possibilities of the authentication bit. In particular, the type 10 and subtype 1000 means the authentication bit is 1. The type 10 and subtype 1001 means the authentication bit is 0.

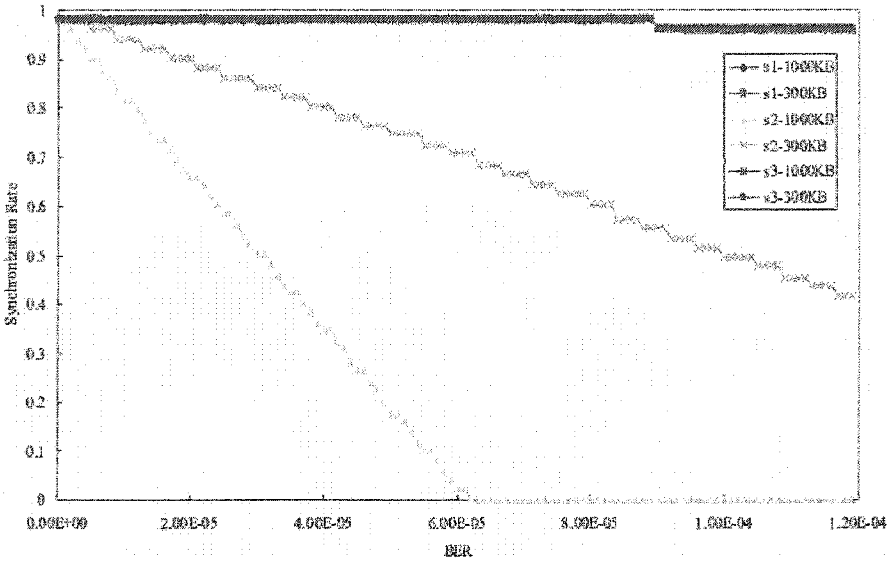


Figure 6.13 Synchronization rates for three schemes at different BER

Table 6.3 Adaptation of IEEE 802.11 MAC frame format

Frame	Type	Subtype
Data(Authentication bit=0)	10	1000
Data(Authentication bit=1)	10	1001
$ACK_{success}$	01	0001
$ACK_{failure}$	01	0010

Similarly, two reserved types in ACK frames are used to represent ACK-success and ACK-failure, which are used in schemes 1 and 3. The type 01 and Subtype 0001 means the frame is an ACK-success frame. The type 01 and Subtype 0010 means the frame is an ACK-failure frame.

6.8 Related Works

SOLA protocol was an authentication protocol of the first use of random bit [49]. SOLA was designed to solve the problem of redundancy, that is, when both the WEP and IPSec are used, each frame sent out from the mobile stations is encrypted twice for authentication. The authors of [49] also presented the non-synchronization problem and proposed a synchorization scheme

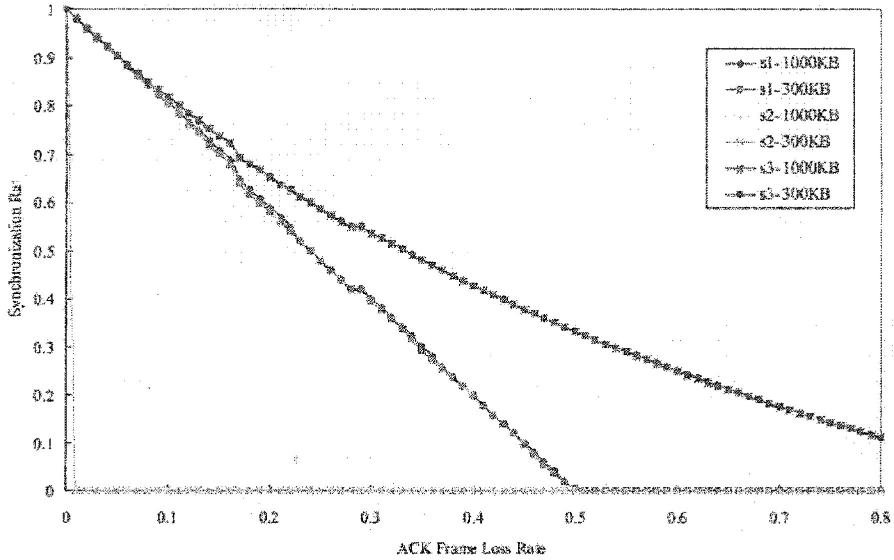


Figure 6.14 Synchronization rates for three schemes at different ACK frame loss rate

as a solution. But a problem exists in the synchronization algorithm of the work and hence it is unlikely to solve the problem. Hence, we proposed a workable synchronization scheme with a statistical method in [95]. To simplify the analysis of the statistical method, the assumption is made that no continuous frame loss occurs in wireless networks, which may not be real in some wireless scenarios. Here we remove this assumption.

An access control framework under PANA was developed in [99]. Data Packet Access Control (DPAC) introduces the possibility of using and negotiating a range of light-weight per-data-packet source authentication methods to control the data packets from mobile hosts. Based on the DPAC framework, authors implemented SOLA and used secure random bits to control the network access. In [104], authors proposed an enhanced random-bit window-based authentication protocol in IP layer, called RBWA. Unlike SOLA in link layer, RBWA does not have a non-synchronization problem by utilizing the sequence number in each packet. Thus, it can achieve the synchronization even in the ACK-less IP layer. However, the sequence number is not faithful to authentication protocols, since the sequence number of each frame is easily modified in a wireless network.

6.9 Summary

In this chapter, we have discussed the design of a lightweight statistical authentication protocol, Shepherd. We have presented three synchronization schemes with their own statistical methods. The complete evaluation and analysis of the three schemes are also discussed. In our analysis, the third scheme, namely Receiver's Pointer Jumps Backward (RPB), is able to synchronize efficiently and hides most of the information from the sender. Through our analysis, we show that this lightweight authentication protocol performs well at a high wireless error rate. Hence we can conclude that this lightweight statistical authentication protocol is easy and practical for implementation in wireless networks.

6.10 Proof of Lemmas

Proof of lemma 4

One important characteristic in scheme 1 is that one ABE may or may not cause one run of synchronization because of possible ACK-failure frame loss. Thus, given the total number of ABEs, a receiver cannot have the accurate number of synchronization runs at a sender, N_{sync}. N_{sync} can be calculated as follows:

$$N_{sync} = N_{ABE} - N_{loss}. \tag{6.25}$$

Although receiver cannot have the accurate N_{sync}, receiver can calculate the average of ACK-failure frame loss by using the given wireless error rate.

$$E[N_{sync}] = N_{ABE} \times r, \tag{6.26}$$

where r is the ACK frame loss rate.

Then, since number of ABEs is known at a receiver, we can derive the average runs of synchronization at a sender, $E[N_{sync}]$ as:

$$\begin{aligned} E[N_{sync}] &= E[N_{ABE} - N_{loss}] && (6.27)\\ &= N_{ABE} - N_{ABE} \times r && (6.28)\\ &= N_{ABE} \times (1 - r) && (6.29) \end{aligned}$$

Proof: First, we construct an abstract bit stream at a receiver for saving the checking results for each successfully received data frame. Each bit in the bit stream represents a comparison result for one successful reception of a data frame. The bit value, denoted as b, is determined as:

$$b = \begin{cases} 0 & \text{, if two bits are matched;} \\ 1 & \text{, otherwise.} \end{cases} \tag{6.30}$$

After successfully receiving a data frame, the receiver saves the checking result in this bit stream and moves the pointer to next bit. Before the successful reception, some possible frame losses may happen, and those frame losses may cause the bit = 1. We analyze the possible frame losses segment before one successful reception and then extend to w receptions. Given the ACK frame loss rate r, the probability of the length of frame loss segment being 0 is $(1-r)$, i.e.$Pr(x_0) = (1-r)$. Similarly, we have $Pr(x_1) = r(1-r)$ and $Pr(x_2) = r^2(1-r)$. We can derive that $Pr(x_n) = r^n(1-r)$ and we can calculate the sum of all probabilities as:

$$\begin{aligned} \sum_{i=1}^{\infty} Pr(x_i) &= Pr(x_0) + Pr(x_1) + \ldots \quad (6.31) \\ &= (1-r)/(1-r) = 1 \quad (6.32) \end{aligned}$$

Thus, in the period of w successful receptions, the expected value of segments of frame loss with $NSI = i$ in w is:

$$E[b_i] = w \times r^i(1-r).$$

Hence, equation (6.14) is proved. ▩

Proof of lemma 5

Proof: Let the average number of ABEs received in the past w frame be $E[s]$. We have

$$\delta = \frac{E[s]}{w}. \tag{6.33}$$

In scheme 1, because the average runs of the synchronization algorithm in the received w frame are derived as, $E[N_{sync}] = E[s] \times (1-r)$, we have,

$$\delta = \frac{E[s]}{w} = \frac{E[N_{sync}]}{w \times (1-r)}. \tag{6.34}$$

Then, we classify all frame losses into G groups, based upon the length of continuous frame losses, which is also equal to the NSI value. Since the total synchronization runs in w is the sum of synchronization runs in each group, that is,

$$N_{sync} = \sum_{i=1}^{G} N_{sync_i}, \tag{6.35}$$

we have

$$E[N_{sync}] = \sum_{i=1}^{G} E[N_{sync_i}]. \tag{6.36}$$

Let h_{ji} be runs of synchronization, caused by the $j'th$ frame loss segment, with NSI= i. We have

$$N_{sync_i} = \sum_{j=1}^{b_i} h_{ji}. \tag{6.37}$$

Combine (6.36) and (6.37), and we can derive

$$\begin{aligned} E[N_{sync}] &= \sum_{i=1}^{G} E[N_{sync_i}] && (6.38)\\ &= \sum_{i=1}^{G} E[\sum_{j=1}^{b_i} h_{ji}] && (6.39)\\ &= \sum_{i=1}^{G}\sum_{j=1}^{b_i} E[h_{ji}]. && (6.40) \end{aligned}$$

Then, we will apply an equation proved in [13]. Let X_i and Y be random variables. If all X_i's are *i.i.d.*,

$$\sum_{i=1}^{Y} E[X_i] = E[X_i] \times E[Y]. \tag{6.41}$$

Apply equation (6.40) in (6.41), since all h_{ji} are i.i.d., therefore, we have

$$E[N_{sync}] = \sum_{i=1}^{G}\sum_{j=1}^{b_i} E[h_{ji}] = \sum_{i=1}^{G} E[b_i] \times E[h_{ji}]. \tag{6.42}$$

Combine (6.42), (6.3), and (6.14), and we have

$$E[N_{sync}] = \sum_{i=1}^{G} w \times r^i(1-r) \times \frac{i+1}{2}. \tag{6.43}$$

Combine (6.34) and (6.43), we have

$$\begin{aligned} \delta &= \frac{\sum_{i=1}^{G} w \times r^i(1-r) \times \frac{i+1}{2}}{w \times 1 - r} && (6.44)\\ &= \sum_{i=1}^{G}(r^i \times \frac{1+i}{2}). && (6.45) \end{aligned}$$

Hence, equation (6.15) is proved. ■

proof of lemma 6

Proof: Let the average runs of the synchronization algorithm in receiving past w frame be $E[s]$. We have $\delta = \frac{E[s]}{w}$
Then, we classify all frame losses into G groups, based upon the length of continuous frame losses, which is also equal to the NSI value. Since the total number of ABEs in w is the sum of ABEs in each group, that is, $s = \sum_{i=1}^{G} s_i$, we have

$$E[s] = \sum_{i=1}^{G} E[s_i]. \tag{6.46}$$

Total ABE in each group is the sum of ABE caused by individual segment. Let h_{ji} be number of ABE, caused by the j'th frame loss segment, with NSI= i. We have

$$s_i = \sum_{j=1}^{b_i} h_{ji}. \tag{6.47}$$

Combine (6.46) and (6.47), and we can derive

$$\begin{aligned} E[s] &= \sum_{i=1}^{G} E[s_i] && (6.48)\\ &= \sum_{i=1}^{G} E[\sum_{j=1}^{b_i} h_{ji}] && (6.49)\\ &= \sum_{i=1}^{G}\sum_{j=1}^{b_i} E[h_{ji}]. && (6.50) \end{aligned}$$

Then, we will apply an equation proved in [13] to equation (6.50). Let X_i and Y be random variables. If all X_i's are $i.i.d.$, $\sum_{i=1}^{Y} E[X_i] = E[X_i] \times E[Y]$

$$E[s] = \sum_{i=1}^{G}\sum_{j=1}^{b_i} E[h_{ji}] = \sum_{i=1}^{G} E[b_i] \times E[h_{ji}]. \tag{6.51}$$

Combine (6.51), (6.3), and (6.14), and we have

$$E[s] = \sum_{i=1}^{G} w \times r^i(1-r) \times \frac{i+1}{2} \tag{6.52}$$

$$\delta = \sum_{i=1}^{G} r^i(1-r) \times \frac{i+1}{2}. \tag{6.53}$$

Hence, equation (6.22) is proved. ■

CHAPTER 7. CONCLUSIONS

In this dissertation, we propose four approaches to achieve a secure and efficient wireless LAN. There are three approaches to enhance the IEEE 802.11 MAC protocol, and one for wireless security, i.e. the Freeze Counter scheme (FC) , the Dynamically Adaptive Retransmission (DAR), the Quick Acknowledgement (QA) scheme, and the Shepherd protocol.

7.1 FC: Freeze Counter Scheme

In the Chapter 3, we propose FC scheme, an adaptive error recovery mechanism. The FC scheme can perform different actions according to the reasons for frame losses. With the differentiation function, called Freeze Counter mechanism, the non-collision error frames could be rapidly retransmitted without the binary exponential backoff procedure in the current IEEE 802.11 MAC. The simulation results show that the FC scheme can achieve a stable performance regardless of the traffic load.

7.2 DAR: Dynamically Adaptive Retransmission

In the Chapter 4, we propose the Dynamically Adaptive Retransmission scheme. The current IEEE 802.11 standard confuses the sender when a positive ACK is lost during its way back. The sender will take it as an unsuccessful delivery and simply retransmit the data frame. DAR is a new feedback scheme, in which the CTS frames carry additional information concerning the previous data delivery without violating the 802.11 MAC layer semantics. Our method proves to be efficient in handling such error conditions as stated in the paper. Experiments and analysis show that the DAR scheme efficiently decreases redundant retransmission by clearly differentiating ACK frame losses.

7.3 QA: Quick Acknowledgement Scheme

In the Chapter 5, an SSCOP-based link layer acknowledgement protocol, namely QA scheme, has been designed as a replacement for positive acknowledgement in IEEE 802.11. Although the SSCOP was originally intended to provide end-to-end error recovery for user data and link protection for ATM signaling, the concept of SSCOP can also apply to the link layer with appropriate modifications. By using both concepts of SACK and NACK, the proposed protocol solves the inefficiency problem of positive ACK in IEEE 802.11. Because of the elimination of ACK timeout and the precise acknowledgement, the protocol provides much better performance than IEEE 802.11. The simulation results show that the performance improvement of the proposed protocol increases with increasing bit error rate.

7.4 Shepherd

In the Chapter 6, we design a lightweight statistical authentication protocol, called Shepherd. We present three synchronization schemes with their own statistical methods. The complete evaluation and analysis of the three schemes are also discussed. In our analysis, the third scheme, namely Receiver's Pointer Jumps Backward (RPB), is able to synchronize efficiently and hides most information from the sender. Through our analysis, we show the lightweight authentication protocol performs well at a high wireless error rate. Hence we can conclude that this lightweight statistical authentication protocol is easy and practical for implementation in wireless networks.

ACKNOWLEDGEMENTS

First, I would like to thank my advisor Prof. Doug Jacobson for his guidance. Next, I would like to thank Prof. Yong Guan, Prof. Manimaran Govindarasu, Prof. James Davis, and Prof. Lu Ruan for kindly being in my Ph.D. committee. I appreciate all the help that they have given me.

I would also like to thank Prof. Morris Chang for recruiting me into Iowa State University, and Prof. James Yu at Depaul University for helpful discussions on SSCOP. I would also like to thank Prof. Daniel Berleant, since I learned a lot when I was his teaching assistant for three semesters.

Additionally, I would also like to thank Jinghao Miao, my roommate and best friend, for taking care of me in my life.

Bibliography

[1] I. Aad and C. Castelluccia. Differentiation mechanisms for IEEE 802.11. *Proc. IEEE INFOCOM'01*, 2001.

[2] I. Aad and C. Castelluccia. Enhancing IEEE 802.11 performance in congested environments. *Annales des Telecommunications-Annals of Telecommunications*, 58(3-4):397–416, 2003.

[3] G. Anastasi and L. Lenzini. QoS provided by the IEEE 802.11 wireless LAN to advanced data applications: a simulation analysis. *Wireless Networks, ACM Journal*, vol.6:pp.99–108, 2000.

[4] Anon. WLAN solution supporting IEEE 802.11. *IEEE Communications Magazine*, 35(6):26–26, 1997.

[5] Anon. 802.11 wireless LANs encryption vulnerability. *Computers and Security*, 20(6):453–453, 2001.

[6] W. A. Arbaugh. Wireless security is different. *Computer*, 36(8):99–101, 2003.

[7] W. A. Arbaugh, N. Shankar, Y. C. J. Wan, and K. Zhang. Your 802.11 wireless network has no clothes. *IEEE Wireless Communications*, 9(6):44–51, 2002.

[8] P. Ashley, H. Hinton, and M. Vandenwauver. Wired versus wireless security: the Internet, WAP, and iMode for E-Commerce. *Proc. of ACSAC'01*, 2001.

[9] H. Balakrishnan and R. H. Katz. Explicit loss notification and wireless web performance. *Proc. of IEEE Global Telecommunications Conference (GLOBECOM'98), Mini Conference*, 1998.

[10] H. Balakrishnan, V. N. Padmanabhan, S. Seshan, and R. H. Katz. A comparison of mechanisms for improving TCP performance over wireless links. *IEEE/ ACM Trans. On Networking*, vol.5(no.6):pp.756–769, Dec. 1997.

[11] H. Balakrishnan, E. Amir S. Seshan, and R. H. Katz. Improving TCP/IP performance over lossy networks. *Proc. of the first ACM International Conference on Mobile Computing and Networking*, 1995.

[12] M. Benveniste. Summary of features proposed for the enhanced-DCF wireless MAC protocol. *IEEE Document, 802.11-01/003*, 2001.

[13] D. P. Bertsekas and J. N. Tsitsiklis. *Introduction to Probability.* Athena Scientific, 2002.

[14] G. Bianchi, L. Fratta, and M. Oliveri. Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless lans. volume 2, pages 392–396, 1996.

[15] C. W. Blanchard. Wireless security. *BT Technology Journal*, 19(3):67–75, 2001.

[16] U. Blumenthal, M. Marcovici, S. Mizikovsky, S. Patel, G. S. Sundaram, and M. Wong. Wireless network security architecture. *Bell Labs Technical Journal*, 7(2):19–36, 2002.

[17] L. Bononi, M. Conti, and L. Donatiello. A distributed mechanism for power saving in IEEE 802.11 wireless LANs. *Mobile Networks and Applications*, 6(3):211–222, 2001.

[18] L. Bononi, M. Conti, and E. Gregori. Design and performance evaluation of an asymptotically optimal backoff algorithm for IEEE 802.11 wireless LANs. pages 3049–3058, 2000.

[19] L. Bononi, M. Conti, and E. Gregori. Runtime optimization of IEEE 802.11 wireless LANs performance. *Parallel and Distributed Systems, IEEE Transactions on*, 15(1):66–80, 2004.

[20] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: the insecurity of 802.11. *Proc. of ACM MOBICOM'01*, 2001.

[21] F. Cali, M. Conti, and E. Gregori. IEEE 802.11 protocol: Design and performance evaluation of an adaptive backoff mechanism. *IEEE Journal on Selected Areas in Communications*, 18(9):1774–1786, 2000.

[22] A. Champness. Understanding IEEE 802.11. *Communications News*, 34(8):25–26, 1997.

[23] W.-T. Chen, J.-J. Dai, and S.-C. Lo. A MAC protocol with QoS guarantee for multiclass traffics in wireless LANs. *Proc. of the 13th International Conference on Wireless Communications*, 2001.

[24] W.-T. Chen, B.-B. Jian, and S.-C. Lo. An adaptive retransmission scheme with QoS support for the IEEE 802.11 MAC enhancement. *Proc. of IEEE VTC Spring'02, Vehicular Technology Conference*, 2002.

[25] C. F. Chiasserini and M. Meo. Improving TCP over wireless through adaptive link layer setting. *Proc. of IEEE Global Telecommunications Conference (GLOBECOM'01)*, 2001.

[26] H. R. Cho and S. C. Park. Modified backoff algorithm with station number adaptiveness for IEEE 802.11 wireless LANs. *IEICE Transactions on Communications*, E86B(12):3626–3629, 2003.

[27] S. Choi and K. G. Shin. A unifield wireless LAN architecture for real-time and non-real-time communication service. *IEEE/ACM Transaction on Networking*, 8(1), Feb. 2000.

[28] C. Coutras, S. Gupta, and N. B. Shroff. Scheduling of real-time traffic in IEEE 802.11 wireless LANs. *Wireless Networks*, 6(6):457–466, 2000.

[29] B. P. Crow, I. Widjaja, J. G. Kim, and P. T. Sakai. IEEE 802.11 wireless local area networks. *IEEE Communications Magazine*, 35(9):116–126, 1997.

[30] B. P. Crow, I. Widjaja, J. G. Kim, and P. T. Sakai. IEEE 802.11 wireless local networks. *IEEE Communications Magazine*, vol.35:pp.116–126, Sep. 1997.

[31] D. J. Deng and R. S. Chang. A priority scheme for IEEE 802.11 DCF access method. *IEICE Transactions on Communications*, E82B(1):96–102, 1999.

[32] D. Denning. *Information Warfare and Security.* Addison-Wesley Publishers, 1999.

[33] W. Ding and A. Jamalipour. A new explicit loss notification with acknowledgment for wireless TCP. *Proc. of 12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, 2001.

[34] D. A. Eckhardt and P. Steenkiste. Improving wireless LAN performance via adaptive local error control. *Proc. of IEEE ICNP*, 1998.

[35] K. Fall and S. Floyd. Simulation-based comparisons of Tahoe, Reno, and SACK TCP. *Computer Communication Review*, 1996.

[36] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, and A. Yegin. Protocol for carrying authentication for network access (PANA). *IETF Draft, http://www.ietf.org/html.charters/pana-charter.html*, access date: Mar. 15, 2004.

[37] C. Fullmer and J.J. Garcia-Luna-Aceves. Floor acquisition multiple access (FAMA) for packet radio networks. *Computer Communication Review*, vol.25:pp.47–59, Apr. 1995.

[38] IEEE 802.11 Working Group. IEEE standard 802.11. *LAN MAN Standards of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specification*, 1997.

[39] IEEE 802.11 Working Group. IEEE 802.11a. *IEEE Std 802.11a-1999 Supplement to IEEE standard for Information technology: High-speed Physical Layer in 5 GHZ Band*, 1999.

[40] IETF IPSec Working Group. IETF RFC of IPSec. *http://www.ietf.org/html.charters/ipsec-charter.html*, access date: Mar. 15, 2004.

[41] IETF PANA Working Group. IETF Draft of PANA. *http://www.ietf.org/html.charters/pana-charter.html*, access date: Mar. 15, 2004.

[42] ITU-T Working Group. B-ISDN signaling ATM adaptation layer- service specific connection oriented protocol (SSCOP). *ITU-T Recommendation Q.2110*, 1994.

[43] J.L. Hammond and P.J.P. O'Reilly. *Performance Analysis of Local Computer Networks.* Addison-Wesley, 1988.

[44] T. Henderson. Design principles and performance analysis of SSCOP: a new ATM adaptation layer protocol. *Computer Communication Review*, vol.25:pp.47–59, Apr. 1995.

[45] T. Henderson and R. Katz. Satellite transport protocol (STP): An SSCOP-based transport protocol for datagram satellite networks. *Proc. of 2nd Workshop on Satellite-Based Information Systems, WOSBIS '97*, 1997.

[46] T. C. Hou, C. M. Wu, and M. C. Chan. Performance evaluation of wireless multihop ad hoc networks using IEEE 802.11 DCF protocol. *IEICE Transactions on Communications*, E86B(10):3004–3012, 2003.

[47] IEEE 802.11–Task Group E. Draft of IEEE P802.11E. *http://www.ieee802.11.org/11/*, access date: Mar. 15, 2004.

[48] USC ISI. NS-2 simulator. *http://www.isi.edu/nsnam/ns/*, access date: Mar. 15, 2004.

[49] H. Johnson, A. Nilsson, J. Fu, S.F. Wu, A. Chen, and H. Huang. SOLA: A one-bit identity authentication protocol for access control in IEEE 802.11. *Proc. of IEEE GLOBECOM'02*, 2002.

[50] E.-S. Jung and N. Vaidya. An energy efficient MAC protocol for wireless LANs. *Proc. of INFOCOM'02*, 2002.

[51] A. Kamerman and G. Aben. Net throughput with IEEE 802.11 wireless LANs. *Proc. of IEEE WCNC'00, Wireless Communications and Networking Conference*, 2000.

[52] S. Kapp. 802.11: Leaving the wire behind. *IEEE Internet Computing*, 6(1):82–85, 2002.

[53] T. Kobayashi. TCP performance over IEEE 802.11 based multichannel MAC protocol for mobile ad hoc networks. *IEICE Transactions on Communications*, E86B(4):1307–1316, 2003.

[54] J. J. Kong, H. Y. Luo, K. X. Xu, D. L. Gu, M. Gerla, and S. W. Lu. Adaptive security for multilevel ad hoc networks. *Wireless Communications and Mobile Computing*, 2(5):533–547, 2002.

[55] R. Krishnan, M. Allman, C. Partridge, and J. Sterbenz. Explicit transport error notification (ETEN) for error-prone wireless and satellite networks–summary. *Proc. of Earth Science Technology Conference*, 2002.

[56] Chen Kwang-Cheng. Medium access control of wireless LANs for mobile computing. *Network, IEEE*, 8(5):50–63, 1994.

[57] D. Leifer. Visitor networks. *Internet Protocol Journal*, 2002.

[58] W. Liu and H. Song. Research and implementation of mobile adhoc network emulation system. *Proc. of IEEE ICDCSW '02*, 2002.

[59] S. C. Lo, G. Lee, and W. T. Chen. An efficient multipolling mechanism for IEEE 802.11 wireless LANs. *IEEE Transactions on Computers*, 52(6):764–778, 2003.

[60] M. Mathis and J. Mahdavi. Forward acknowledgement: refining TCP congestion control. *ACM SIGCOMM*, 1996.

[61] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow. TCP selective acknowledgement (SACK) options. *IETF RFC 2018*, 1996.

[62] S. K. Miller. Facing the challenge of wireless security. *Computer*, 34(7):16–18, 2001.

[63] A. Mishra, M. Shin, and W. Arbaugh. An empirical analysis of the IEEE 802.11 MAC layer handoff process. *Computer Communication Review*, 33(2):93–102, 2003.

[64] R. Molva and P. Michiardi. Security in ad hoc networks. *Personal Wireless Communications, Proceedings*, 2775:756–775, 2003.

[65] B.E. Mullins, N.J. Davis, and S.F. Midkiff. A wireless local area network protocol that improves throughput via adaptive control. *Proc. of IEEE ICC'97, International Conference on Communications*, 1997.

[66] M. Nakahara. Theoretical throughput/delay analysis for variable packet length in the 802.11 MAC protocol. *Information Networking*, 2662:284–294, 2003.

[67] M. Natkaniec and A. R. Pach. Analysis of backoff mechanism in IEEE 802.11 standard. *Proc. of ISCC'00, Symposium on Computers and Communications*, 2000.

[68] G.T. Nguyen, R.H. Katz, B. Noble, and M.A. Satyanarayanan. Trace-based approach for modelling wireless channel behavior. *Proc. of Winter Simulation Conference*, 1996.

[69] B. O'Hara and A. Petrick. *IEEE 802.11 handbook: A designer's companion.* IEEE Press, 1999.

[70] B. Patil and A. Yegin. Frequent asked questions of protcol for carrying authentication for network access (PANA) FAQ. *http://www.toshiba.com/tari/pana/pana-faq.txt*, access date: Mar. 15, 2004.

[71] B. Potter and B. Fleck. *802.11 Security.* O'Relly Publisher, 2003.

[72] D. J. Qiao, S. Y. Choi, A. Soomro, and K. G. Shin. Energy-efficient PCF operation of IEEE 802.11 a WLANs via transmit power control. *Computer Networks-the International Journal of Computer and Telecommunications Networking*, 42(1):39–54, 2003.

[73] C. Severance. IEEE 802.11: Wireless is coming home. *Computer*, 32(11):126–127, 1999.

[74] S. Sharma. Analysis of 802.11b MAC: A QoS, fairness, and performance perspective. *Department of Computer Science Stony Brook University*, 2003.

[75] S. T. Sheu and T. F. Sheu. A bandwidth allocation/sharing/extension protocol for multimedia over IEEE 802.11 ad hoc wireless lans. *IEEE Journal on Selected Areas in Communications*, 19(10):2065–2080, 2001.

[76] S.-T. Sheu, T.-F. Sheu, C.-C. Wu, and J.-Y. Luo. Design and implementation of a reservation-based MAC protocol for voice/data over IEEE 802.11 ad-hoc wireless networks. *Proc. of IEEE ICC'01, International Conference on Communications*, 2001.

[77] A. K. Singh. Deployment of public-key infrastructure in wireless data networks. *Proc. of LCN'01*, 2094:217–224, 2001.

[78] J. L. Sobrinho and A. S. Krishnakumar. Quality-of-service in ad hoc carrier sense multiple access wireless networks. *Selected Areas in Communications, IEEE Journal on*, 17(8):1353–1368, 1999.

[79] T. Suzuki and S. Tasaka. Performance evaluation of video transmission with the PCF of the IEEE 802.11 standard MAC protocol. *IEICE Transactions on Communications*, E83B(9):2068–2076, 2000.

[80] S. Tasaka. *Performance Analysis of Multiple Access Protocols.* MIT Press, 1986.

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

[82] O. Tickoo and B. Sikdar. On the impact of IEEE 802.11 MAC on traffic characteristics. *IEEE Journal on Selected Areas in Communications*, 21(2):189–203, 2003.

[83] Y. C. Tseng, C. S. Hsu, and T. Y. Hsieh. Power-saving protocols for IEEE 802.11-based multi-hop ad hoc networks. *Computer Networks-the International Journal of Computer and Telecommunications Networking*, 43(3):317–337, 2003.

[84] U. Varshney. The status and future of 802.11-based WLANs. *Computer*, 36(6):102–105, 2003.

[85] M. Veeraraghavan, N. Cocker, and T. Moors. Support of voice services in IEEE 802.11 Wireless LANs. *Proc. of INFOCOM'01*, 2001.

[86] A. Veres, A. T. Campbell, M. Barry, and Sun Li-Hsiang. Supporting service differentiation in wireless packet networks using distributed control. *Selected Areas in Communications, IEEE Journal on*, 19(10):2081–2093, 2001.

[87] S. Vincze. How secure personal mobility can be? *Proc. of Computational Science and Its Applications - ICCSA'03, Pt 1*, 2667:238–244, 2003.

[88] H. Wang, J. Cardo, and Y. Guan. Shepherd: A lightweight probabilistic authentication protocol for wireless networks. *Poster in International Symposium on Modern Computing (JVA03)*, 2003.

[89] H. Wang and M. Chang. Improving TCP performance in wired-cum-wireless environments. *Proc. of International Conference on Information and Communication Technologies (ISBN: 974-615-089-8)*, 2003.

[90] H. Wang and M. Chang. Improving wireless LAN performance via adaptive retransmission. *Proc. of International Conference on Information and Communication Technologies (ISBN: 974-615-089-8)*, 2003.

[91] H. Wang, J. Miao, and M. Chang. An enhanced link layer retransmission scheme for IEEE 802.11. *Proc. of International Computer Symposium (ICS'02)*, 2002.

[92] H. Wang, J. Miao, and M. Chang. Dynamically adaptive retransmission in IEEE 802.11. *Proc. of IEEE WCNC'03, Wireless Communications and Networking Conference*, 2003.

[93] H. Wang and A. Velayutham. An enhanced one-bit identity authentication protocol for access control in IEEE 802.11. *Proc. of IEEE MILCOM'03, Military Communications*, 2003.

[94] H. Wang and A. Velayutham. An SSCOP-based link layer protocol for wireless LANs. *Proc. of IEEE GLOBECOM'03*, 2003.

[95] H. Wang, A. Velayutham, and Y. Guan. A lightweight authentication protocol for acess control in IEEE 802.11. *Proc. of IEEE GLOBECOM'03*, 2003.

[96] J. Weinmiller, M. Schlger, A. Festag, and A. Wolisz. Performance study of access control in wireless LANs-IEEE 802.11 DFWMAC and ETSI RES 10 HIPERLAN. *Mobile Networks and Applications*, 2:pp. 55–67, 1997.

[97] J. Weinmiller, H. Woesner, J. P. Ebert, and A. Wolisz. Analyzing the RTS/CTS mechanism in the DFWMAC media access protocol for wireless LANs. *Proc. of IFIP TC6*, 1995.

[98] S. Wolfram. *The Mathematica Book.* Wolfram Research, 1999.

[99] S.F. Wu, F. Zhao, C. Shin, H. Johnson, R.C. Guo, T.J. Liu, K.P. Fan, and J. Fu. A framework for data packet access control (DPAC). *IETF Draft*, 2003.

[100] Y. Xiao. A simple and effective priority scheme for IEEE 802.11. *IEEE Communications Letters*, 7(2):70–72, 2003.

[101] Y. Xiao and J. Rosdahl. Throughput and delay limits of IEEE 802.11. *IEEE Communications Letters*, 6(8):355–357, 2002.

[102] S. G. Xu and T. Saadawi. Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks? *IEEE Communications Magazine*, 39(6):130–137, 2001.

[103] S. G. Xu and T. Saadawi. Revealing the problems with 802.11 medium access control protocol in multi-hop wireless ad hoc networks. *Computer Networks-the International Journal of Computer and Telecommunications Networking*, 38(4):531–548, 2002.

[104] F. Zhao, Y. Shin, S. F. Wu, H. Johnson, and A. Nilsson. RBWA: An efficient random-bit window-based authentication protocol. *Proc. of IEEE GLOBECOM'03*, 2003.