DEPARTMENT OF ELECTRONIC AND ELECTRICAL ENGINEERING

Random Access MAC Protocols and System Monitoring Methodology in Wireless Mesh Networks

Feiyi Huang

A thesis submitted on requirements for the degree of

Doctor of Philosophy

of

University of London.

Department of Electronic and Electrical Engineering

University College London

February, 2008

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

Statement of Originality

Unless otherwise stated in the text, the work presented in this thesis was carried out by the candidate. It has not been presented previously for any degree, nor is at presented under consideration by any other degree awarding body.

Candidate: Feiyi Huang

Research Supervisor: Dr. Yang Yang

Abstract of the thesis

As an extension of wireless Ad Hoc [1] and sensor [2] networks, wireless mesh networks (WMN) [3] have recently been developed as a key solution to provide high-quality multimedia services and applications, such as voice, data and video, over wireless personal area networks (WPAN) [4], wireless local area network (WLAN) [5] and wireless metropolitan area network (WMAN) [6]. A WMN usually has a hierarchical network infrastructure with backbone and access networks operated in both Ad Hoc and centralized modes with self-organization and self-configuration capabilities. Along with flexibilities, WMN brings several problems and requirements at the same time. In this thesis, problems and challenges such as packet collisions, interference and security issues are initialized discussed with existing solutions reviewed. After that, three innovative random access MAC protocols are proposed for wireless mesh access networks with comprehensive analysis and discussion followed. Moreover, in order to detect misbehaviors of wireless terminals and abnormal performance of applications, the network traffic flow concept in wired IP network is extended to WMN with "Meshflow" defined. Based on this new concept, a comprehensive framework is designed for wireless mesh backbone network to monitor users, routers, applications and services so as to achieve abnormal or intrusion detection, malicious user identification and traceback.

Acknowledgements

To Dr. Yang Yang for four years great supervision; To Dr. Liwen He for excellent guiding during the BT placement period; To Prof. Sheng Chen and Prof. Yang Hao for their great effort in reviewing the thesis and providing very useful refining suggestion; To Prof. Izzat Darwazeh and Dr. John Mitchell for useful discussion and research suggestion; To all colleagues Darren Shea, Bahman Kalantari-Sabet, Kai Li, Saad Sari and Jiayuan Chen.

Contents

List of Figures

List of Tables

List of Abbreviations

ACM	Association for Computing Machinery
ACK	Acknowledgement
ACL	Access Control List
AODV	Ad hoc On-demand Distance Vector
AP	Access Point
AWGN	Additive While Gaussian Noise
BPSK	Binary Phase Shift Keying
BS	Base Station
BT	British Telecommunication
CCA	Clear Channel Assessment
CC	Client to Client
CCK	Complimentary Code Keying
CDMA	Code Division Multiple Access
CR	Client to Router

CTS	Clear to Send
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CW	Contention Window
DBTMA	Dual Busy Tone Multiple Access
DCF	Distributed Coordination Function
DIFS	DCF Interval Frame Space
DoS	Denial of service
DDoS	Distributed Denial of Service
DSDV	Destination Sequenced Distance Vector
DSMA-D	Double Sense Multiple Access – Double Channel
DSMA-S	Double Sense Multiple Access – Single Channel
DSR	Dynamic Source Routing
DSSS	Direct Sequence Spread Spectrum
FDM	Frequency Division Multiplexing
FHSS	Frequency Hopping Spread Spectrum
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific and Medical
MAC	Medium Access Control

MANET	Mobile Ad Hoc Network
NAV	Network Allocation Vector
NIC	Network Interface Card
OFDM	Orthogonal Frequency Division Multiplexing
OLSR	Optimized Link State Routing
PCF	Point Coordination Function
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal digital assistant
PDF	probability density function
PN	Pseudo Noise
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RR	Router to Router
RSMA	Receiver Sense Multiple Access
RTS	Request to Send
SIFS	Short InterFrame Space
SINR	Signal to Interference plus Noise Ratio

TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
UDP	User Datagram Protocol
UNII	Universal Networking Information Infrastructure
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network

List of Symbols

λ	wavelength
$W_a(d)$	area mean power at the distance d
$W_l(d)$	local mean power at the distance d
$W(d_0)$	close-in power value at the distance d_0
W_t	transmission power level
w	instantaneous power level
n_0	the power of the additive Gaussian white noise
T_c	the minimum required SINR
I	lengths of idle period
I_s	lengths of idle period that guarantee a successful transmission
B_s	lengths of successful busy period
B_f	lengths of failed busy period
p_s	successful access probability
p_f	failed access probability

P_B	blocking probability
γ	RTS length of DSMA-S and RSMA
δ	DATA length of DSMA-S and RSMA
γ'	RTS length of DSMA-D
δ'	DATA length of DSMA-D
τ	time slot
r_{max}	maximum retransmission times
D	access delay
E	energy consumption
R	number of retransmission times
S	throughput

Chapter 1

Introduction

1.1 Thesis structure

Wireless mesh network [7; 8] consists of a group of self-organized client and router devices which construct a flexible network architecture. Both centralized and distributed access modes are utilized to manage the wireless access from a mesh client. This flexibility provides advantages as well as induces disadvantages.

Chapter 1 In this chapter, a brief introduction of the thesis is provided. It contains summaries of each chapter, major contributions and a list of publications.

Chapter 2

In Chapter 2, the infrastructure of wireless mesh access and backbone network are both introduced at the beginning. Router meshing interconnection constructs the wireless mesh backbone network. The network is able to be self-configured when new routers join in or existing routers leave the backbone network. In the access network, client meshing enables the client-to-client communication in a distributed manner without the support from the mesh router. It is a good supplementary access method for the conven-

tional centralized access method and makes the mesh access network become a hybrid architecture. As a result, the coverage range of the access network is enlarged because of packet relaying, and traffic load on the mesh router is released because of direct link among mesh clients. On the other hand, the hybrid infrastructure and distributed network architecture makes the collision avoidance very difficult to be achieved on the medium access control (MAC) layer. Furthermore, the open network structure and hybrid operation mode increase the possibility for malicious users or attackers to sneak in, disguise as legitimate users, compromise mesh routers or clients, misbehave with communication protocols and launch a variety of attacks against different wireless functionalities, services and applications.

Chapter 3

As a promising techology of wireless mesh network, IEEE 802.11a,b,g MAC and physical layer specification [18; 19; 20] is reviewed comprehensively in Chapter 3 in terms of radio technology, access mechanism and signal propagation characteristics. In particular, the "hidden terminal problem" and its solution: distributed coordination function (DCF) request to send - clear to send (RTS-CTS) handshake mechanism are emphasized and analyzed in details.

Chapter 4

In Chapter 4, a number of problems and challenges in wireless mesh network are reviewed and discussed, e.g. packet collision, energy conservation, interference aware transmission, etc. These problems are clearly illustrated and analyzed by a set of examples which also provides a general solution for each of the problems. A number of existing solutions that try to resolve these problems or satisfy these requirements are also discussed with open research

issues provided.

It is known that the collision avoidance capability is the basic requirement on MAC protocols. Thus, several collision avoidance MAC protocols, e.g. [32; 33; 34; 35; 40] are reviewed first. Second, as mesh clients always have constraints on energy supply, energy conservation, e.g. [51; 54] capability is also a common requirement that can be achieved by several different ways. Third, from the physical layer's perspective, packet level collision becomes the signal interference. The intended signal will be failed (collided), if the power ratio between this signal and the interference plus the background noise is smaller than the required threshold. By carefully adjust the packet transmission power, the interference can be efficiently controlled, e.g. [61]. And the transmission rate is also able to adapt with the reduced signal to interference plus noise ratio (SINR) and thus be maximized, e.g. [59]. Forth, in wireless mesh access networks, clients are enabled to flexibly choose their transmission route, as well as the corresponding transmission power level. The network topology will be affected accordingly. In order to reduce the transmission interference and energy consumption, and improve the throughput performance, the best route and topology should be selected according to the link propagation quality, link traffic load and transmission delay. Finally, in both wireless mesh backbone and access network, the open network structure makes it easy for malicious users or attackers to misbehave existing network protocols and functionalities, or even launch an attack, e.g. [71; 73; 74]. How to detect a misbehavior or attacking action in real-time and reduce the harm to the network as far as possible is a very challenging topic.

Chapter 5

In wireless mesh access network, wireless connections usually consist of

client-to-client (CC) and client-to-router (CR) links. For a CC communication, both the sender and the receiver are mesh clients. Each of them has limited resource on signal processing and wireless communication. To satisfy this constraint, a simple "double sense" mechanism is proposed specifically for CC communication in Chapter 5. Based on this mechanism, a random access MAC protocol, Double Sense Multiple Access - Double Channel (DSMA-D) is proposed to resolve or alleviate the packet collision problem summarized in Chapter 4. As indicated by the name, the protocol operates on two separated channels for control message and data payload transmission respectively. As a result, the control-data packet collision is avoided inherently. The "double sense" mechanism is implemented on the control channel at the sender side to avoid the data-data collision. After that, another random access MAC protocol is proposed based on this "double sense" mechanism on a single shared wireless channel, namely, Double Sense Multiple Access -Single Channel (DSMA-S). The data-data collision avoidance can still be achieved by the "double sense" mechanism while the control-data collision is avoided by a newly proposed "mandatory waiting" mechanism. Apart from the collision avoidance, the DSMA-S is able to improve the energy conservation capability by introducing a "mandatory clearance" mechanism to mandatory clear the channel when collision happens. A precise mathematic model is constructed to analyze the throughput, delay and blocking probability of DSMA-D and DSMA-S with simulation results verified. Comparison between the two protocols, as well as with another newly proposed protocol (RSMA) is conducted in chapter 6.

Chapter 6

According to the architecture of wireless mesh access network, CR com-

munication usually has a large amount of packet to transmit and very sensitive to packet collisions. The collision period analysis in Chapter 5 (Appendix A) illustrates that frequent collision among control packets will also severely affect the network performance. In Chapter 6, another innovative random access MAC protocol, Receiver Sense Multiple Access (RSMA), is proposed to resolve the packet collision as far as possible. With this protocol, both the control packet and the data packet transmission are partially or completely protected by busy tone signals. As a result, the data-data and control-data collisions are completely avoided and the control-control collision is also efficiently alleviated. A more precise performance analysis is conducted by taking the physical layer propagation model into account. DSMA-D, DSMA-S and RSMA are then compared among each other. These protocols are further compared with an existing random access protocol, Dual Busy Tone Multiple Access (DBTMA) [40], to illustrate the performance improvement.

Chapter 7

In Chapter 7, a network monitoring framework is constructed for the wireless mesh backbone network to monitor the network performance. The network traffic flow concept for conventional wired network is extended to the wireless mesh network with the "Meshflow" defined. A "Meshflow" record contains the general information of several packets that share the same characteristics, e.g. source and destination address, next hop address, transport protocol, etc. The "Meshflow" function generate "Meshflow" records continuously when network operates. These records are exported to a dedicated server at every time interval for further analysis. As "Meshflow" records can reflect the real-time network performance, e.g. who is generating packets, who is receiving packets, how many packets are being transmitted, etc., the network

can be monitored by simply generating and analyzing the "Meshflow" records. As a result, intrusion detection, terminal, application and service monitoring or even attacker/malicious user traceback can be achieved.

1.2 Contributions

In wireless mesh access network, both the centralized and decentralized (distributed) network architectures are used to supply wireless connections for mesh clients. A packet usually travels through a multi-hop wireless link before reaching its final destination, e.g. a mesh router or another mesh client. The hybrid multi-hop wireless link makes the collision avoidance and energy conservation very difficult to be achieved. The dynamic and open architecture makes the network more vulnerable to malicious usage and attacking.

1. We first of all discuss problems on physical, MAC and routing layer in both wireless mesh access and backbone network. A number of existing solutions that target at these problems are reviewed, analyzed and classified with open research issues summarized.

2. Two innovative MAC protocols are proposed to manage the access procedure of CC communications: DSMA-D (Double Sense Multiple Access – Double Channel) and DSMA-S (Double Sense Multiple Access – Single Channel). As DSMA-D suggested, control messages and data payload are transmitted separately on the two wireless channels so as to avoid control-data collisions. Data-data collision avoidance is achieved by the newly proposed "double sense" mechanism which is simple enough and suitable for CC communications. The DSMA-S protocol follows the same line of "double sense" mechanism and improves the access one step further. The "double sense" mechanism performs on a single shared channel in DSMA-S along with the "mandatory waiting" mechanism. Further more, energy conservation ability is provided by the "mandatory clearance" mechanism to clear channel when packet collision happens.

3. Another MAC protocol RSMA (Receiver Sense Multiple Access) is proposed for the CR communication. RSMA efficiently manage the CR communication and achieve excellent collision avoidance property by taking good advantage of mesh router to advertise an ongoing packet transmission (control or data) to all contending mesh clients.

4. These MAC protocols are precisely analyzed by a newly constructed mathematic model based on the conventional busy period analysis method. With this model, the system throughput, expected access delay, blocking probability and energy consumption are mathematical analyzed with the simulation results precisely matching the analytical curves.

5. On each layer of wireless mesh network protocol stack, a number of misbehaviors, attacks might happen since there is no sufficient network monitoring and protection mechanisms implemented in the backbone network. In this area, the conventional "network traffic flow" concept is extended and implemented in the wireless mesh network. A new concept "Meshflow" is defined for the purpose of intrusion detection, terminal monitoring, application profiling and traceback. A "Meshflow" record indicates a number of packets that share the same characteristics such as source and destination address, type of service, transport protocols, etc. Services, terminals, protocols can all be profiled by the "Meshflow" based functionalities and thus be monitored. As a result, any abnormal protocol performance, terminal misbehavior can be detected immediately when by real-time monitored "Meshflow" records. Furthermore, by utilizing a recursive mechanism, attackers or malicious users can be traced back from the victim according to the Meshflow records.

1.3 Publications

Book Chapters

1. Feiyi Huang and Yang Yang, "Medium Access Control Protocols in Hybrid Multi-hop Wireless Networks," *Chapter 17, Volume II: Practice and Standards, Medium Access Control in Wireless Networks (Book)*, to be published by Nova Science Publishers, Inc.

2. Feiyi Huang and Yang Yang, "Medium Access Control for Wireless Mesh Networks," invited by *Handbook of Wireless Ad Hoc and Sensor (book)*, to be published by Springer (London).

Journals/Magazines

3. Yang Yang, Feiyi Huang, Xuanye Gu, Mohsen Guizani, and Hsiao-Hwa Chen, "Double Sense Multiple Access for Wireless Ad Hoc Networks," *Computer Networks (Elsevier)*, vol. 51, no. 14, pp. 3978-3988, Oct. 2007.

4. Feiyi Huang, Yang Yang and Liwen He, "Flow Based Network Monitoring and Traceback Mechanism for Securing Wireless Mesh Networks," to appear in *IEEE Wireless Communications Magazine, (Special Issue on Wireless Ad Hoc/Sensor Networks Security)*, Oct. 2007.

Patent(s)

5. Feiyi Huang and Liwen He, "Method and Apparatus for Monitoring a Digital Network," *British Telecommunication (BT) patent A30981*, 2006, European Patent Pending.

Conference

6. Feiyi Huang and Yang Yang, "Double Sense Multiple Access Protocol for

Hidden Terminal Avoidance in Wireless Ad Hoc Networks," poster session, *ACM SIGCOMM*, Aug. 2004.

7. Feiyi Huang, Yang Yang, Xuanye Gu, and Yonghua Song, "Throughput Analysis of Double Sense Multiple Access Protocol," in *Proceedings of IEE 3G Conference*, pp. 604~608, London, Oct. 2004.

8. Yang Yang, Feiyi Huang, Xuanye Gu, Mohsen Guizani, and Hsiao-Hwa Chen, "Double Sense Multiple Access for Wireless Ad Hoc Networks," in *Proceedings of The Third International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QShine)*, Aug. 2006.

9. Feiyi Huang and Yang Yang, "An Energy Efficient Medium Access Control Protocol for Wireless Mesh Access Networks," *Wireless World Research Forum (WWRF) 17th meeting: Serving and managing users in a heterogeneous environment*, Oct. 2006.

10. Feiyi Huang and Yang Yang, "Receiver Sense Multiple Access Protocol for Wireless Mesh Access Networks," in *Proceedings of IEEE International Conference on Communications (ICC)*, June, 2007.

11. Feiyi Huang and Yang Yang, "Energy Aware Collision Avoidance MAC protocol for Hybrid Multi-hop Networks," in *Proceedings of ACM Wireless Communications and Mobile Computing Conference (IWCMC)*, Aug., 2007.

12. Feiyi Huang and Yang Yang, "Cross-Layer Analysis of Receiver Sense Multiple Access Protocol in Wireless Mesh Access Networks," to appear in *Proceedings of IEEE ICC 2008*.

Chapter 2

Wireless Mesh Networks

In recent years, wireless mesh networks(MWN) [7; 8], together with related applications and services, have been actively researched. New applications include digital home, broadband and wireless home Internet access, community and neighborhood networking, enterprise networking, metropolitan area networks, building automation, heath and medical systems, public safety and security surveillance systems, intelligent transportation systems, emergency and disaster networking, etc [9]. Generally speaking, a WMN is a group of self-organized and self-configured mesh clients and mesh routers interconnected via wireless links (Fig. 2.1). Mesh clients can be different kinds of user devices with wireless network interface cards (NIC), such as PCs, laptops, PDAs and mobile phones. They have limited resources and capabilities in terms of energy supply, processing ability, radio coverage range, etc. Wireless mesh routers can be access points (AP) of wireless local area network (WLAN), sink nodes of wireless sensor network, base stations (BS) of cellular network, or furthermore, a special kind of hardware device that has multiple types of radio technologies and able to work properly in each of these networks. Mesh routers are usually much more powerful than clients in terms of computation

Figure 2.1: Infrastructure of Wireless Mesh Networks [7]

and communication capabilities, and have continuous power supply. They usually stay static and supply connections and services for mesh clients.

Ad Hoc mode interconnections via wireless meshing among mesh routers (router-to-router RR links) construct the wireless mesh backbone network. There are several Internet gateways locate at the edge of the backbone network so as to provide Internet access for the mesh network. For efficient reasons, wired line connections are usually utilized for these gateways between a gateway and the Internet, as well as between a gateway and mesh routers. An universal radio technology is usually used for the entire backbone network although there might be a number of heterogeneous networks, e.g. WLAN, cellular, WPAN. In order to join in an existing mesh network that using a different radio technology, one additional wireless interface has to be equipped on the mesh router that does not use the common radio. On the other hand,

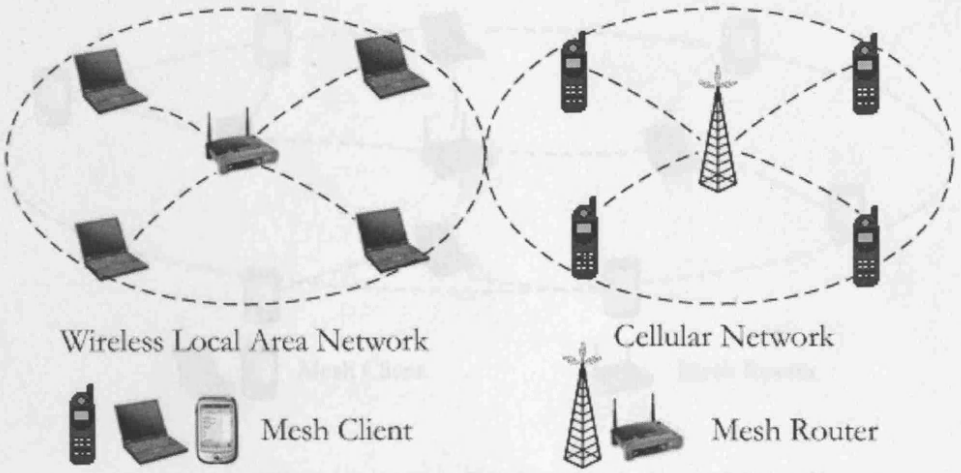

Figure 2.2: Infrastructure of Centralized Networks

multiple radio technologies coexisting in one wireless mesh backbone network is also possible. However, difficulty in implementation and costly requirement on hardware make it less attractive in real network. When a new/existing router joins/leaves the backbone, the network will be self-organized and self-configured accordingly. As the mesh routers usually stay static, and the backbone topology changes only when new routers join in and existing routers fail or leave.

The structure of wireless mesh access network is very different from the backbone network. Fig. 2.2 illustrates the conventional centralized network structure wherein clients access to WMN through via client-to-router (CR) wireless link. The mesh router manages all access requests from clients within that access network, and supplies Internet connection for them. The access procedure from clients to the router follows the corresponding access mechanisms of that access network, e.g. CSMA/CA.

On the other hand, wireless mesh access network enables Ad Hoc mode peer-to-peer interconnections among mesh clients, namely "client meshing".

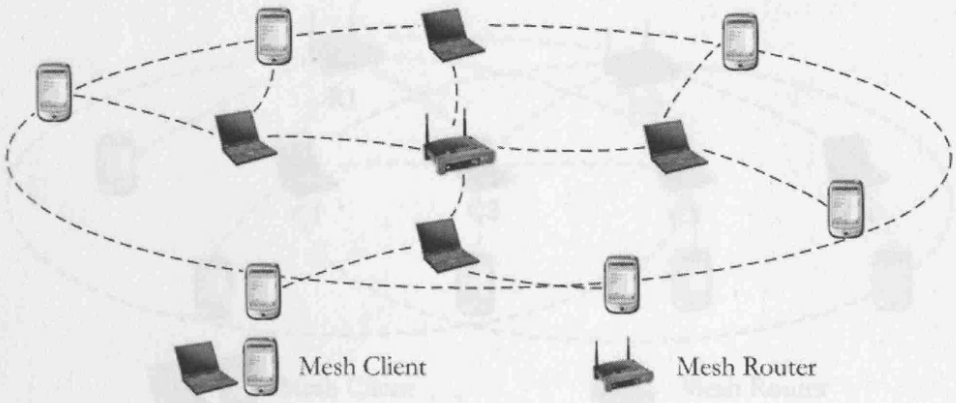

Figure 2.3: Client Meshing in Wireless Mesh Access Networks

It can be achieved among any type of clients that share the same radio technology. As shown in Fig. 2.3, with "client meshing" mesh clients that stay outside of the radio coverage range of a mesh router can rely on other intermediate clients to relay packets for them to get WMN access network connections. Thus, packets from a mesh client that stay far away from the mesh router have to travel through a multi-hop hybrid client-to-client (CC) and client-to-router (CR) wireless link before reaching its destination. The number of hops is determined by the geographic position of the mesh client and organization structure of the access network. In this case, wireless mesh access network operates in a hybrid Ad Hoc and infrastructure modes. Client meshing enlarges the coverage range of WMN access network, improves flexibility for clients to access a WMN. More importantly, it enables direct interconnections among mesh clients without the support from mesh routers.

As illustrated in Fig. 2.4, a mesh client, e.g. client **C1**, can communicate with a client within the same access network, e.g. **C2** via direct CC link, **C1** – **C2**, rather than a two hop CR link of **C1** – **R1** and **R1** – **C2**. A multi-hop CC link enables direct access to a mesh client that stays within another access

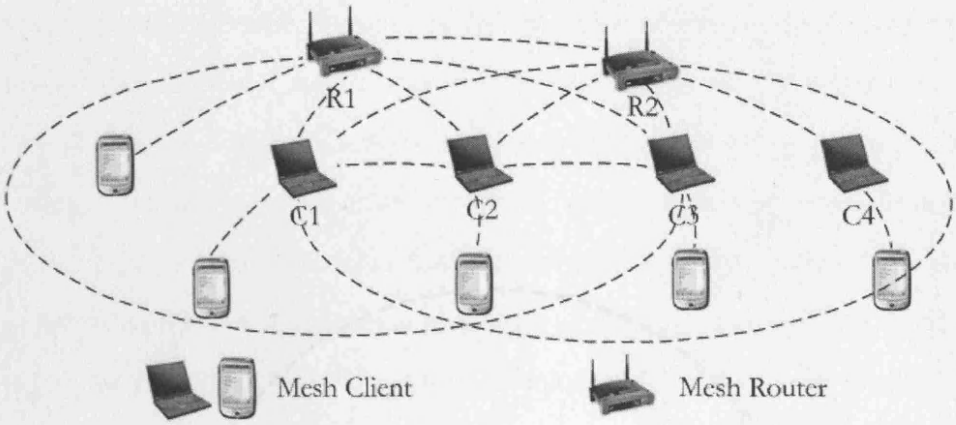

Figure 2.4: Wireless Client Meshing

network, e.g. **C1 – C2 – C3**. As a result, traffic load on mesh routers can be efficiently released especially when network traffic load is heavy. However, mesh routers are usually strong enough to handle huge amount of requests and supply simultaneous service for clients. But mesh clients are relatively weak and have constraints on processing ability, power supply, etc. Thus, they are not suitable for relaying too much traffic for other clients unless client meshing connection has less hops, e.g. traffic from client **C1** to **C2**. According to the research in [10], transport capability, especially the TCP throughput, drops dramatically when the number of CC hop increases. Therefore, too long a multi-hop CC connection in WMN is not attractive at all. In other words, within a wireless mesh access network, the mesh router still takes the major role to manage the access and packet transmission procedures for mesh clients. Client meshing is an efficient supplementary access method for neighboring clients, e.g. **C1** and **C2** or **C2** and **C3** in Fig. 2.4. Pure client meshing constructs a complete distributed network that has the identical characteristic with the conventional Ad Hoc network and is less attractive in WMN.

The WMN network structure and connection characteristics determine a

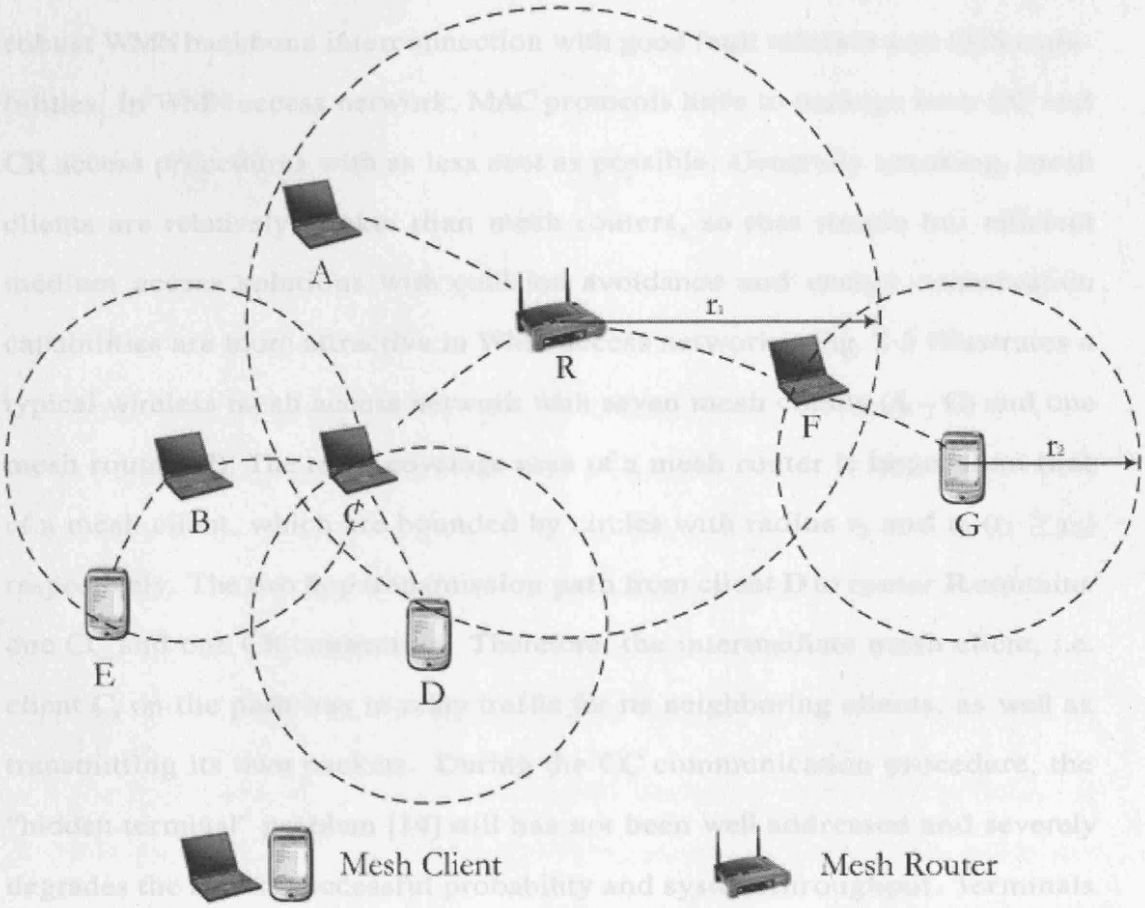

Figure 2.5: Infrastructure of Wireless Mesh Access Networks

number of problems and challenges in medium access control process. In WMN backbone network, mesh routers are usually powerful enough and have no constraints on computation, communication and energy supply. Thus, multi-radio, cognitive radio, multi-channel medium access control methodologies [11; 12; 13] are quite possible to be implemented to supply flexible and robust WMN backbone interconnection with good fault tolerant and QoS capabilities. In WMN access network, MAC protocols have to manage both CC and CR access procedures with as less cost as possible. Generally speaking, mesh clients are relatively weaker than mesh routers, so that simple but efficient medium access solutions with collision avoidance and energy conservation capabilities are more attractive in WMN access networks. Fig. 2.5 illustrates a typical wireless mesh access network with seven mesh clients (**A** – **G**) and one mesh router (**R**). The radio coverage area of a mesh router is larger than that of a mesh client, which are bounded by circles with radius r_1 and r_2 ($r_1 \geq r_2$) respectively. The two hop transmission path from client **D** to router **R** contains one CC and one CR connection. Therefore, the intermediate mesh client, i.e. client **C**, on the path has to relay traffic for its neighboring clients, as well as transmitting its own packets. During the CC communication procedure, the "hidden terminal" problem [14] still has not been well addressed and severely degrades the access successful probability and system throughput. Terminals that stand within the radio coverage range of the receiver (client **C**) but out of the coverage of the sender (client **D**), are hidden terminals of the sender (client **B**). Transmission from client **D** to **C** is interrupted if client **B** transmits packets to client **C** during the same period. On the other hand, traffic will be accumulated from multiple directions when it traverses through the network until it reaches the mesh router. This phenomenon makes the clients closer to the

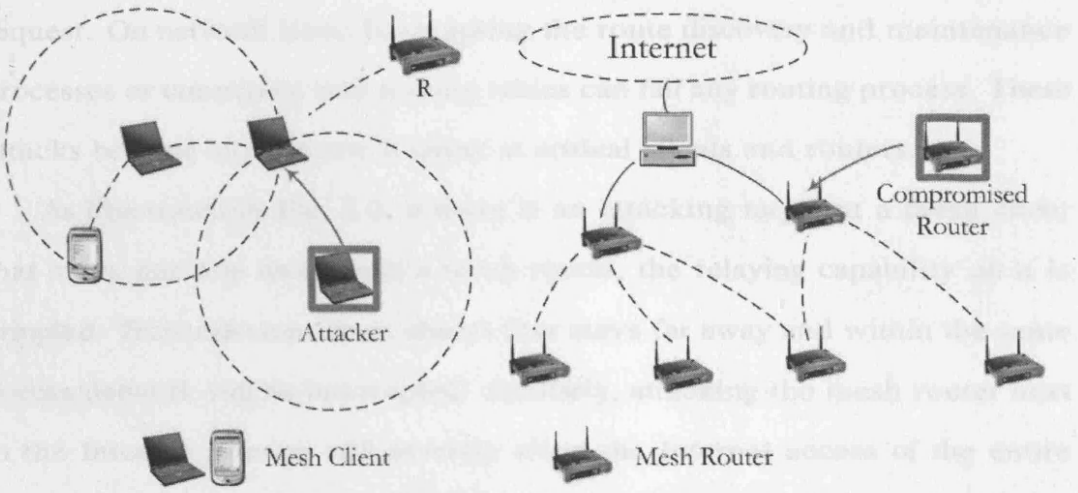

Figure 2.6: Attacking in Wireless Mesh Access Networks

router become traffic hot-spots and thus induces some critical problems such as unbalanced resource utilization and unsustainable system connectivity. Together with the hidden terminal problem, constraints of energy supply and limitations on computation and communication capabilities on mesh clients, make medium access control (MAC) protocols quite challenge to address these problems for CC and CR communications in wireless mesh access networks.

The open network structure and hybrid operation mode of WMN make it possible for malicious users or attackers to sneak in, disguise as legitimate users, compromise mesh routers or clients, misbehave with communication protocols and launch a variety of attacks against different wireless functionalities, services and applications. On physical layer, attackers can make use of the inherent vulnerability of radio frequency (RF) transmission and generate jamming signals to interfere with communications on wireless channels. On MAC layer, continuously broadcasting the request packets makes the common access channel be occupied at all times and deny the service for legitimate

request. On network layer, interrupting the route discovery and maintenance processes or tampering with routing tables can fail any routing process. These attacks become more severe if target at critical clients and routers.

As illustrated in Fig. 2.6, if there is an attacking target at a mesh client that stays one hop away from a mesh router, the relaying capability on it is crippled. Transmissions from clients that stays far away and within the same access network will be interrupted. Similarly, attacking the mesh router next to the Internet gateway will severely affect the Internet access of the entire mesh network. Therefore, it is quite necessary and challenging to develop an abnormal monitoring and protection mechanism to alleviate the harm caused by misbehavior, malicious usage and attacking.

Chapter 3

Background - The IEEE 802.11 MAC/Physical Specification

IEEE 802.11 technology is widely accepted as a promising solution in realizing wireless mesh networking. It can be optimized and upgraded to enable a hybrid Ad hoc and centralized structure and provide the access networking for wireless mesh network. In this chapter, the background knowledge of IEEE 802.11 physical and medium access control (MAC) characteristics, and the conventional "hidden terminal problem" are comprehensively reviewed.

IEEE 802.11 refers to a series of wireless local area network standards developed by IEEE standard committee working group 11 [16]. It includes both MAC and physical layers protocol specifications. The most popular and widely used standards are IEEE 802.11a, b and g whose major characteristics are summarized in Tab. 3.1.

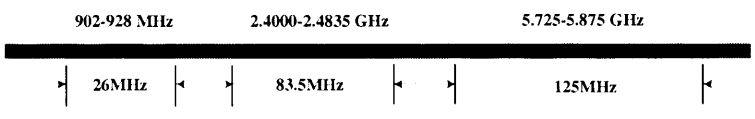

Figure 3.1: ISM Frequency Band

Table 3.1: IEEE 802.11 a, b and g [17]

Protocol	Release	Frequency	Channels	Modulation	Max Rate
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 (5 GHz)	19	OFDM /PSK&QAM	54 Mbps
802.11b	1999	2.4 -2.5 GHz (2.4 GHz)	11	DSSS/CCK	11 Mbps
802.11g	2003	2.4 -2.5 GHz (2.4 GHz)	11	OFDM/CCK	54 Mbps

3.1 Radio Techology

The basic difference among IEEE 802.11a, b and g is that the IEEE 802.11a [18] operates on the 5GHz UNII (Universal Networking Information Infrastructure) frequency band while the IEEE 802.11b [19] and g [20] use the 2.4GHz ISM (industrial, scientific, medical) band (Fig. 3.1). The 5GHz frequency band is much looser and does not have too many other technologies operating on the same band. Thus, it makes IEEE 802.11a technology that performs on this frequency band has little interference. However, most of UNII frequency bands are not international license free, which makes the 802.11a technology difficult to be adopted for commercial used. The OFDM (Orthogonal frequency-division multiplexing) [21] technology is utilized in 802.11a and 12 non-overlapping OFDM channels are available for parallel transmission, 8 for data payload and 4 for pilot. OFDM is a digital multi-carrier modulation scheme. And each sub-carrier is modulated with a conventional modulation algorithm (e.g. quadrature plitude modulation) at a low rate. Together with

the OFDM technology, IEEE 802.11a is able to achieve a maximum data rate of 54Mbps. The data rate is reduced to 48 Mbps, 36 Mbps, 24 Mbps, 12 Mbps, 9 Mbps, 6 Mbps and recursively back according to the wireless link quality. Different data rate can be achieved by different coding/modulation technologies, e.g. BPSK, QPSK, 16-QAM, 64-QAM [22], and the corresponding coding rate.

Because of using the license free 2.4GHz ISM frequency band (Fig. 3.1), IEEE 802.11b/g technologies are widely accepted and widely implemented. Unfortunately, there are a number of other technologies such as Bluetooth and Microwave which use this frequency band as well. This induces several interference source and reduces the operation efficiency of 802.11b/g. The IEEE 802.11b adopts spreading spectrum technologies [24], i.e. DSSS (Direct-sequence spread spectrum) and FHSS (Frequency-hopping spread spectrum) on the physical layer to improve the anti-interference property. With the DSSS mechanism, 11-14 channels (depending on different countries) are available for communication, wherein there are only 3 non-overlapping ones. The redundantly coded base-band data is multiplied with a PN (pseudo-noise) sequence and thus modulated to a wide spectrum band. Together with the CCK (complementary code keying) [25], it can achieve a maximum data rate of 11Mbps. This rate reduces to 5.5Mbps, 2 Mbps and 1 Mbps according to the signal and link quality by using less efficient modulation schemes such as QPSK and BPSK. The FHSS mechanism enables all wireless terminals operate on several of the overall 75 narrowband carrier frequencies which occupy separated frequency regions and referred as channels. Terminals select a list of channels, and periodically use one of selected channels then hop to another for only short period. This mechanism provides robust and secure transmis-

sion and it is preferred in military communication scenarios. However, modulation on narrowband restricts the transmission data rate and makes it not exceed 2Mbps. The IEEE 802.11g technology employs the OFDM mechanism rather than the DSSS or FHSS as in 802.11b, and thus reaches a maximum data rate up to 54Mbps like 802.11a. Fortunately, an IEEE 802.11g device is compatible with a 802.11b device which provides a significant advantage over the 802.11a technology.

3.2 Access Mechanism

The IEEE 802.11a, b and g protocols share the same MAC mechanism to provide reliable data transmission for upper layers. Two types of medium access mechanisms are defined: PCF (point coordination functions) and DCF (distributed coordination functions). PCF provides non-contention based access services via polling based mechanism with quality of service (QoS) guaranteed. The DCF functionality provides contention based random access service for asynchronous packet transmissions. In other words, packets transmission procedures are expected to be successful but not guaranteed in advance. In IEEE 802.11, PCF function is optional and can only implemented in the infrastructure mode, while the DCF function is mandatory and can be implemented in both infrastructure and Ad Hoc mode. The infrastructure and Ad Hoc network architecture is illustrated in Fig. 3.2. Without losing generality, the detailed access mechanisms of DCF and PCF are discussed based on it.

3.2.1 Distributed Coordination Function

3.2.1.1 Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA)

The CSMA/CA (carrier sense multiple access with collision avoidance) [15] is the basic access mechanism of DCF. Generally speaking, CSMA mechanism

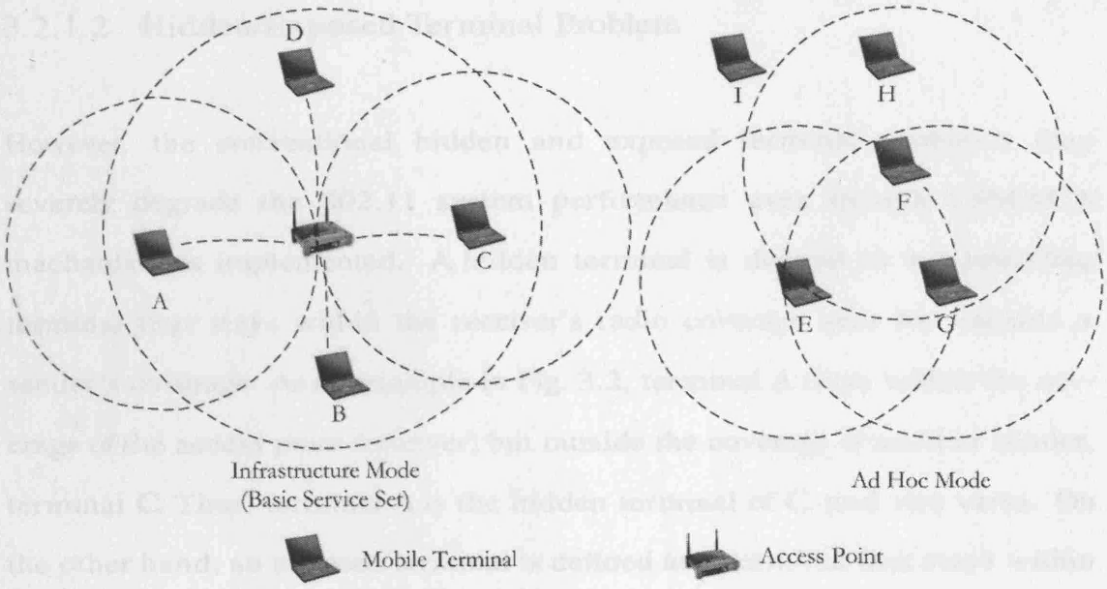

Figure 3.2: Infrastructure and Ad Hoc Network Architecture

refers to a "listen before talk" access procedure. It requires each mobile terminal listen to the radio channel of that BSS (basic service set) before transmitting. The carrier sensing is achieved by the clear channel assignment (CCA) algorithm to determine whether the carrier is occupied or idle according to power level of that channel. Transmission is only permitted if the channel is sensed idle. If the channel is busy, the terminal has to defer its transmission until the channel becomes idle again. According to the analysis in [96] and [97], CSMA greatly improves the channel utilization compared to the ALOHA mechanism (terminals transmit as soon as their data packets are ready). As an example in Fig. 3.2, if access point (AP) is sending a packet to terminal **B**, terminal **A** can sense a busy channel before a transmission. As a result, it is not allowed to send its packet(s) to the AP.

3.2.1.2 Hidden/Exposed Terminal Problem

However, the conventional hidden and exposed terminal problems may severely degrade the 802.11 system performance even though CSMA/CA mechanism is implemented. A hidden terminal is defined as a contending terminal that stays within the receiver's radio coverage area but outside a sender's coverage. As an example in Fig. 3.2, terminal **A** stays within the coverage of the access point (receiver) but outside the coverage of another sender, terminal **C**. Thus, terminal **A** is the hidden terminal of **C**, and vice versa. On the other hand, an exposed terminal is defined as a terminal that stays within the radio coverage area of a sender but outside the coverage of the receiver that is the target of that sender. In Fig. 3.2, if terminal **G** is the intended receiver of terminal **F**, terminal **H** becomes the exposed terminal of terminal **F**.

As an example in Fig. 3.2, if terminal **C** sends a packet to the access point, as a hidden terminal of it, terminal **A** will sense the channel of this BSS and conclude an idle medium. Terminal **A** will then transmit its packet simultaneously and interrupt with the ongoing transmission from terminal **C** at the access point. This phenomenon is known as the "hidden terminal problem" which can not be alleviated by the CSMA mechanism. The "hidden terminal problem" severely degrades the CSMA random access performance and affects functionalities of a 802.11 system. On the other hand, the "exposed terminal problem" degrades the system performance as well, especially in the Ad Hoc environment. In Fig. 3.2, if these is an ongoing packet transmission from terminal **F** to **G**, the terminal **H** will keep silence and defer its transmission to terminal **I** although it will not interfere the **F** to **G** communication.

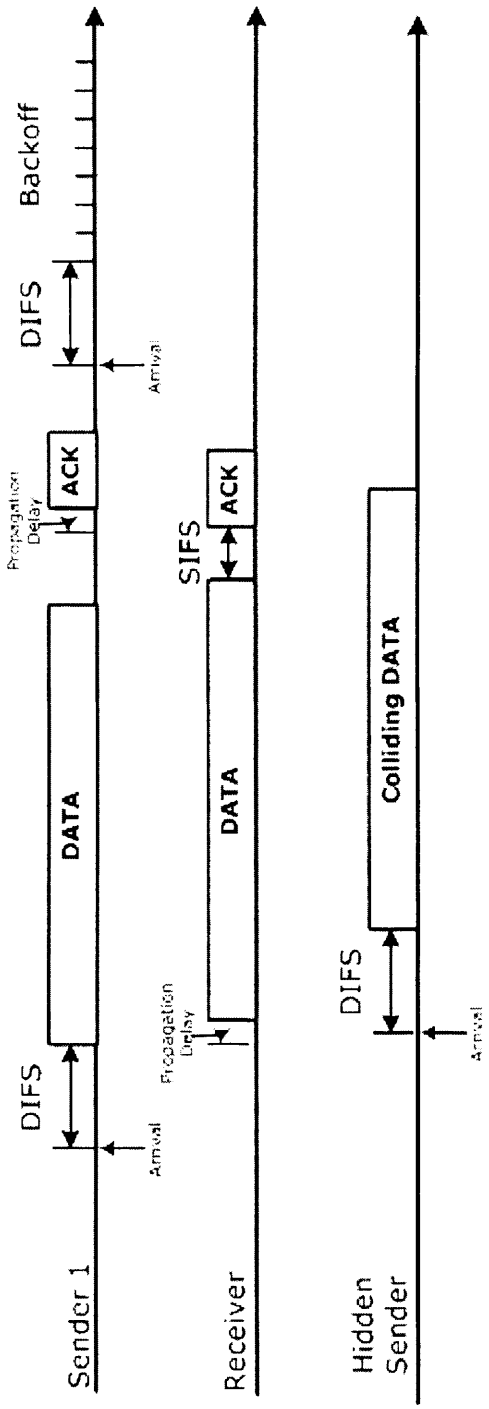

Figure 3.3: Basic Access Mechanism

3.2.1.3 802.11 DCF Basic Access Mechanism

The IEEE 802.11 DCF function includes two access mechanisms, one is the basic access mechanism and the other is the RTS-CTS access mechanism. As illustrated in Fig. 3.3, the basic access mechanism requires a terminal that has the packet transmission attempt sense the channel activity before transmitting packets. If the channel is idle for a period of DIFS (distributed interframe space) which is a protocol defined fixed value, packet transmission is permitted. Otherwise, the transmission is deferred until an entire DIFS period of idle channel is sensed. Then the sender generates a random backoff duration before transmitting payload according to the backoff mechanism, e.g. uniform distributed, binary exponential distributed [103], etc. Furthermore, terminals that finish a transmission have to enter the backoff state as well before transmitting another packet. This procedure is used to avoid continuously capturing the channel by some extreme active terminals. Every time the backoff mechanism is performed, terminals choose an initial value in the range between 0 and $2^i \cdot \omega$-1 wherein the ω is known as minimum contention window (CW), and the "i" refers to the number of failed transmissions of one attempt. After each unsuccessful transmission, the CW of that terminal is doubled until reach the maximum value, $CW_{max}=2^m CW_{min}$. The backoff timer is decremented as soon as the initial value is chosen and the channel activity is sensed idle. The decrement is suspended when the channel becomes busy, and reactivated again when the channel is idle for more than a DIFS period. In IEEE 802.11, the discrete time exponential backoff mechanism is used. As a result, the time during the backoff stage is slotted and transmission is performed at the beginning of the time slot immediately after backoff is finished. The duration of a time slot is determined by the 802.11 MAC

and physical layer characteristics, i.e. the summation of a clear channel assessment (CCA), a transmit-receive turn around time, a MAC processing delay and a radio propagation delay. When a sender finishes the packet transmission, it waits for the acknowledgement (ACK) packet until a specified timeout, ACK_Timeout. If the sender does not correctly receive the ACK within the timeout, it considers the transmission is failed and schedules a retransmission for that packet after a backoff process. If the packet is correctly received by the receiver, an ACK packet is transmitted back to the sender immediately after a short interframe space (SIFS) delay which is also a protocol defined value.

Unfortunately, the DCF basic access mechanism is severely threatened by the "hidden terminal problem". In Fig. 3.3, if a hidden terminal of sender 1 has a transmission attempt as well, it spends a DIFS period for channel sensing. Then packet is transmitted from the hidden sender and a collision occurs at the receiver side. In order to avoid this problem, IEEE DCF function defines a more reliable access mechanism, RTS-CTS-DATA-ACK four-way handshake mechanism.

3.2.1.4 802.11 DCF RTS-CTS Access Mechanism

The key components and major characteristics of the RTS-CTS based access mechanism are RTS, CTS and NAV. A terminal that has a packet transmission attempt follows the same access procedures of a DIFS waiting and backoff stages. After that, a short frame control packet, request to send (RTS) packet, is transmitted to handshake with the receiver and reserve the subsequent channel for payload transmission. The intended receiver will respond with another control packet, clear to send (CTS) packet, if it is able to receive the subsequent payload. Both the RTS and CTS packets contain basic information of the outgoing payload transmission, such as source and destination

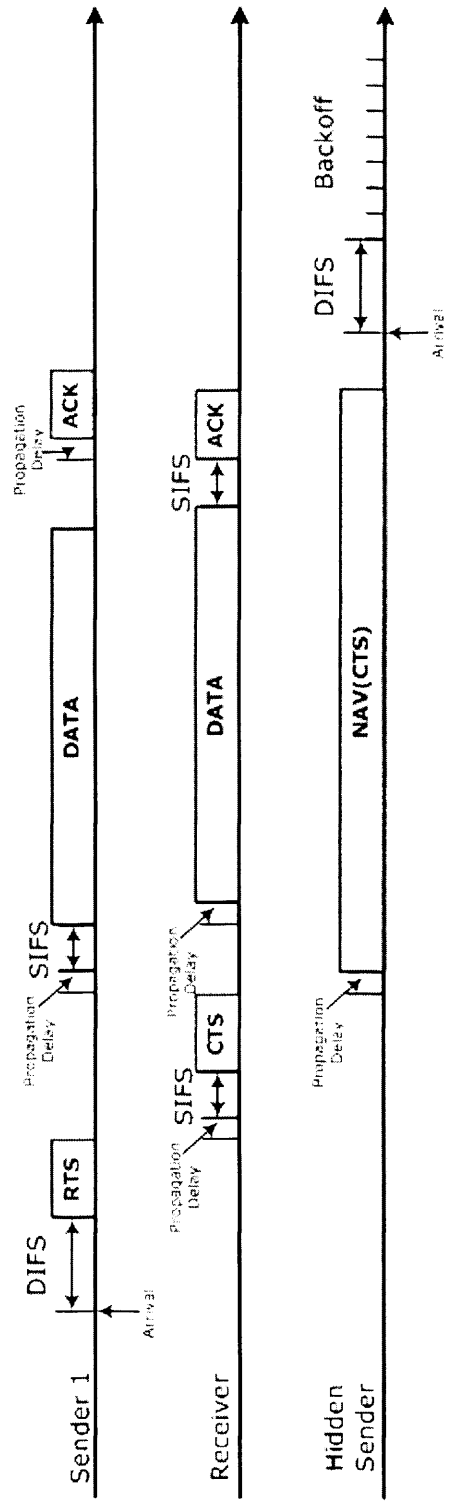

Figure 3.4: RTS-CTS Access Mechanism

terminals, the duration of the payload, etc. As a result, all listening terminals can get the latest updated network allocation vector (NAV) information which contains how long the channel will remain busy. As a result, the "hidden terminal problem" is well addressed as CTS packets from the receiver can update the NAV of hidden terminals and make them keep silence for a certain period (Fig. 3.4).

3.2.2 Point Coordination Function

Apart from the DCF function, the IEEE 802.11 MAC layer contains another access mechanism, namely point coordination function (PCF). PCF targets at providing contention-free multiple access service for real-time programs by polling mechanism with quality of service (QoS) supported [26]. IEEE 802.11 determines the PCF function as an optional mode while the DCF is mandatory. PCF divides the access procedure into separated contention based and contention-free based stages which severely degrades the system capacity. More importantly, a large percentage, around 90%, of non-real-time traffic within the current network [27] makes the PCF function less attractive and little implemented.

3.3 Signal Propagation Characteristics

The IEEE 802.11 DCF defines a pure packet level contending, (re)transmission and receiving process regardless of physical layer parameters. Packet transmissions are considered as fail when more than one packet arrive at the same receiver at the same time or within a certain period. From the physical layer's perspective, packets experience a radio propagation path loss [28], shadowing and Rayleigh fast fading [29] before reaching the receiver. At the receiver side, packets are demodulated against interference and noise. If the ratio of the

intended signal versus the interference plus the noise (SINR) is larger than the minimum SINR requirement of the receiver, the intended packet is able to succeed even there are other contending packets arrives at the same time.

3.3.1 Transmission Path Loss

When radio signal propagate, the power level degrades. The transmission path loss model predicts the area mean power of the radio at the distance d, denoted by W_a(d). A close-in power value W(d_0) is utilized as a reference to calculate the W_a(d) [22]:

$$\frac{W_a(d)}{W(d_0)} = \left(\frac{d_0}{d}\right)^{\beta} \tag{3.1}$$

The W(d_0) is calculated according to the line-of-sight path free space propagation path loss model [22].

$$W(d_0) = \frac{W_t \cdot \lambda^2}{(4\pi)^2 \cdot d_0^2} \tag{3.2}$$

wherein the λ is the wavelength and W_t is transmission power level. The equation 3.2 describes the radio propagation characteristics in an ideal environment without considering the multi-path propagation, shadowing and fading effect. Therefore, the value of d_0 has to be selected carefully. The β in equation 3.1 is knows as the path loss exponent which is an empirical parameter of the radio signal propagation environment listed in Table. 3.2.

The area mean power level at distance d is usually measured in dB and expressed by equation 3.3:

$$\left(\frac{W_a(d)}{W(d_0)}\right) = -10\beta log\frac{d}{d_0} \tag{3.3}$$

Table 3.2: Path Loss Exponent [30]

Environment		β
Outdoor	Free Space	2
	Shadowed Area	2.7 – 5
Indoor	Line-of-Sight	1.6 – 1.8
	Obstructed	4 – 8

Radio propagation path loss model predicts the power level at distance d as a deterministic function of d rather than a random variable.

3.3.2 Log-normal Shadowing

Shadowing occurs if the line-of-sight radio propagation is obstructed by some objects and induces the power at the receiver side slowly fluctuates over the area mean power. The fluctuation is an additive random variable on the area mean power level which follows a log-normal distribution. When expressed in dB, the local mean power with an additive Gaussian distributed random variable is shown in equation 3.4:

$$\left(\frac{W_a(d)}{W(d_0)}\right) = -10\beta log\frac{d}{d_0} + X_{dB} \tag{3.4}$$

The random variable X_{dB} has zero-mean and standard derivation δ_{dB}. This standard derivation measures the depth of shadowing which can be considered as irregularity of the radio propagation procedure. Some empirical value of δ_{dB} is listed in Tab. 3.3.

The probability density function of the local mean power $W_l(d)$ can be rewritten by:

Table 3.3: Log-normal Shadowing Standard Derivation [30]

Environment		δ_{dB}
Outdoor		4 – 12
Indoor (Office)		7 – 9.6
Indoor (Factory)	Line-of-Sight	3 – 6
	Obstructed	6.8

$$f(W_l(d)) = \frac{1}{\sqrt{2\pi}\delta_{dB}} \cdot exp\left(-\frac{1}{2\delta_{dB}^2} log^2\left(\frac{W_l(d)}{W_a(d)}\right)\right) \tag{3.5}$$

3.3.3 Rayleigh fading

The Rayleigh fading phenomenon is a fast statistical power fluctuation over the local mean power level which determined by the shadowing. It determines the instantaneous power level at the receiver side. The Rayleigh fading is mainly caused by movement of receiver, ratio of transmission bandwidth to the channel bandwidth and multiple transmission paths. In mathematics, the instantaneous power level w probability density function is expressed as:

$$f(w) = \frac{1}{W_l} \exp\left(-\frac{w}{W_l}\right) \tag{3.6}$$

3.3.4 Capture Model

The instantaneous power at the receiver side is the aggregation from several transmitters, say N, when simultaneous transmission happens. However, one of them may succeed if its power level is much larger than the summation of others plus the additive Gaussian while noise. This phenomenon is known as the capture effect [49] with the minimum required SINR T_c as the capture threshold . Signal i to interference plus noise ratio is usually expressed as:

$$SINR = \frac{w_i}{\sum_{j \neq i} w_j + n_0} \tag{3.7}$$

wherein n_0 is known as the power of the additive Gaussian white noise and w_j is power of signal j. If the concerned signal w_i has larger SINR than the required value at the receiver side, this radio signal can be received successfully. Thus the capture probability density function is expressed as:

$$f(w_i) = P\left(\frac{w_i}{\sum_{j \neq i} w_j + n_0} \geq T_c\right) \tag{3.8}$$

3.4 Summary

This chapter provides background knowledge of IEEE 802.11 DCF, the hidden terminal problem and radio propagation characteristics. These topics are highly related with the subsequent chapters of random access MAC protocol design and cross layer analysis. In the next chapter, a number of existing MAC solutions are reviewed. They are also classified according to the functionalities of them, such as collision avoidance capability, energy conservation capability, etc.

Chapter 4

Literature review – Problems and Solutions

As the wireless mesh access network has a hybrid structure of centralized and Ad Hoc architecture, the MAC layer access mechanisms proposed for wireless Ad Hoc, sensor and wireless local area network are potentially suitable for mesh networks. There are a number of papers that study the possibility of implementing existing MAC protocols to WMN. For example, [31] discusses the problems and perspectives of implementing the IEEE 802.11 MAC into WMN. The existing MAC protocols have been well studied and analyzed by many researchers, and classified by several methods. From the aspect of channel division, they are classified into single channel and dual/multiple channels, while from the aspect of session initiator, they are classified into sender initialized and receiver initialized. In this chapter, we study the targets of MAC protocols and provide a general solution to achieve that. Then a number of contention based MAC protocols are reviewed, discussed and classified according to the functionalities of the protocols and the problems resolved.

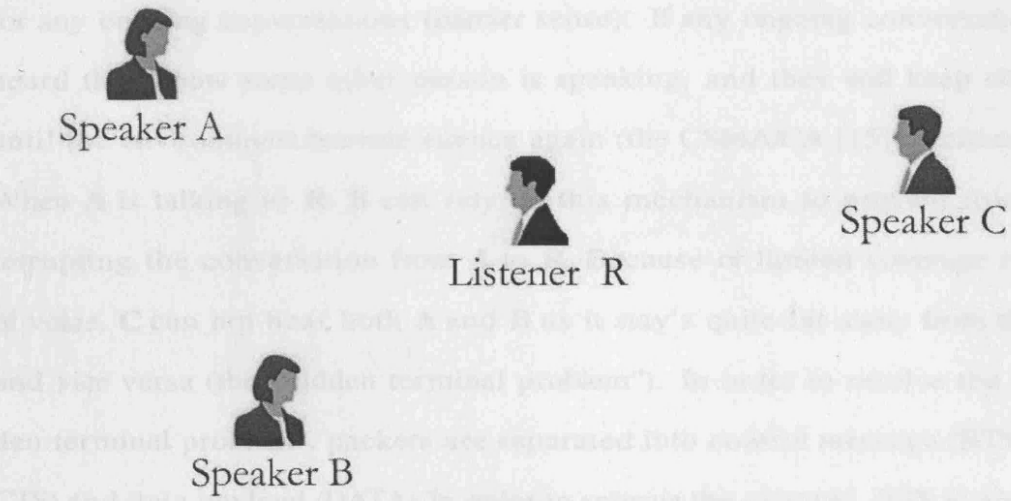

Figure 4.1: Contending Environment

4.1 Collision Avoidance

On MAC layer, packet level collisions usually happen when more than one packet arrives on the same channel, at the same receiver and at the same time (or within a certain period of time). The basic functionality of a MAC protocol is to avoid and resolve packet collisions as much as possible. As the "hidden terminal problem" is the major collision causer, most of existing protocols attempt to resolve this problem, e.g. RTS/CTS handshake based [32; 33; 34; 35] and busy tone based mechanisms [40].

In order to illustrate the access mechanism clearly, we take a hypothetic conversation scenario as an example and describe the general access procedure according to this example. In Fig. 4.1, when more than one speaker (**A**, **B** and **C**), who speak the same language (packet transmitted on the same channel) try to speak to the same listener (**R**), MAC protocols coordinate their transmissions and try to avoid collisions among them.

When **A**, **B** and **C** intend to speak to **R**, they listen to the environment

for any ongoing conversations (carrier sense). If any ongoing conversation is heard they know some other person is speaking, and they will keep silence until the environment become silence again (the CSMA/CA [15] mechanism). When **A** is talking to **R**, **B** can rely on this mechanism to prevent from interrupting the conversation from **A** to **R**. Because of limited coverage range of voice, **C** can not hear both **A** and **B** as it stay's quite far away from them, and vice versa (the "hidden terminal problem"). In order to resolve the "hidden terminal problem", packets are separated into control message (RTS and CTS) and data payload (DATA). In order to reserve the channel, RTS is usually transmitted without enough protection and easy to fail. In this example, the control message refers to the "hello" word, and the data payload refers to the content of conversations. The "hello" word contains the brief information of the outgoing conversation content, such as location of the speaker and listener (source and destination address), conversation duration (packet length), etc. There are a number of protocols that operated based on the RTS/CTS handshake to reserve the channel for safe DATA transmission.

4.1.1 RTS/CTS Handshake Based MAC

The MACA (Multiple Access Collision Avoidance) [32] MAC protocol is proposed in the early 90s of the last century. The RTS/CTS handshake process is proposed in it to improve the payload transmission successful probability in packet radio networks. The general access procedure of this series of protocols is illustrated in the Fig. 4.2. When a speaker has something to talk, he transmits a "hello" message (RTS) first of all instead of the conversation content directly. This "hello" message is used to contend for the conversation opportunity. In Fig. 4.2, speaker **C** succeeds in the contending phase and gets the right to talk to the listener **R**. He then receives a short "yes" message

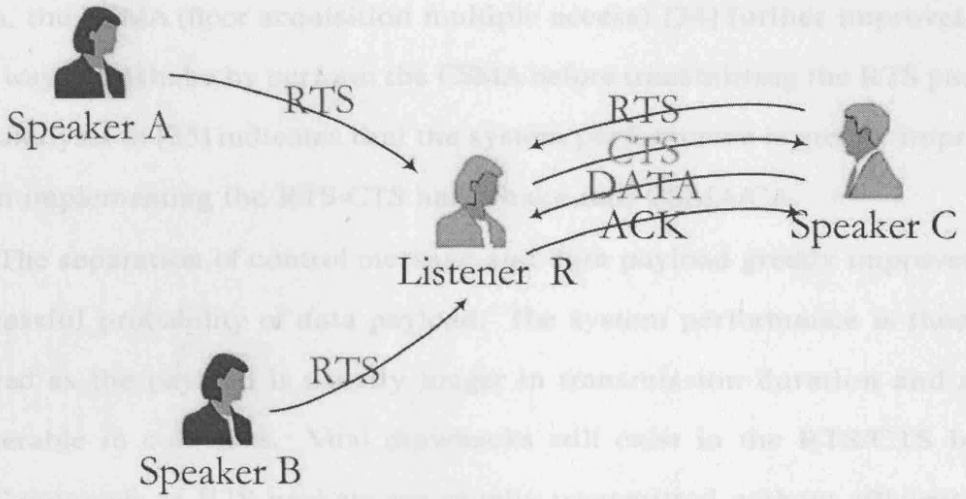

Figure 4.2: RTS/CTS Handshake

(CTS) from **R**. The CTS contains similar information with RTS such as source and destination address and duration of the transmission. When the CTS packet arrives at other contending senders (speaker **A** and **B**), they are aware of the busy period length of that listener and keep silence for corresponding duration. When the CTS arrives at the successful sender (speaker **C**), he regards the "yes" message as the permission of talking and start transmitting his DATA. A confirmation message (ACK) is sent back from the listener when the transmission is finished.

- The existing MAC protocols with sender initialized RTS/CTS based handshake process follow the general procedure described above. The MACAW (multiple access collision avoidance wireless) [33] protocol tries to adapt the MACA in the unreliable wireless network by introducing an acknowledgement control message, ACK. The ACK is transmitted back from the DATA receiver to the sender to confirm a successful payload transmission. The access procedure of MACAW is improved to a RTS-CTS-DATA-ACK four way handshake.

Then, the FAMA (floor acquisition multiple access) [34] further improves this four way handshake by perform the CSMA before transmitting the RTS packet. The analysis in [35] indicates that the system performance is greatly improved when implementing the RTS-CTS handshake into CSMA/CA.

The separation of control message and data payload greatly improves the successful probability of data payload. The system performance is then improved as the payload is usually longer in transmission duration and more vulnerable in collisions. Vital drawbacks still exist in the RTS/CTS based MAC protocols as RTS packets are usually transmitted without efficient protections. Collision among RTS packets is very difficult to avoid. According to the analysis in [36], frequent RTS collisions can also severely degrade the system performance. How to avoid or alleviate RTS-RTS collision as much as possible becomes an open issue of MAC protocol design and optimization.

4.1.2 Receiver Initialized MAC

There are a number of protocols that let the receiver to initialize the communication process rather than the sender. When the receiver become free, a control message named RTR (ready to receive) is transmitted to encourage potential senders to access the receiver one by one. These polling based protocols follow a general access procedure as illustrated in Fig. 4.3 as follows.

The invitation message is dedicated to one of the neighboring speakers of the listener, say RTR-C in Fig. 4.3. Non-intended speakers will hear the invitation message and then keep silence according to the information contained, e.g. speaker **A**. After exchanging DATA between the speaker and the listener, an acknowledgement message is sent to the speaker and the listener will continue to invite other speakers to talk.

The MACA-BI (multiple access collision avoidance by invitation) proposes

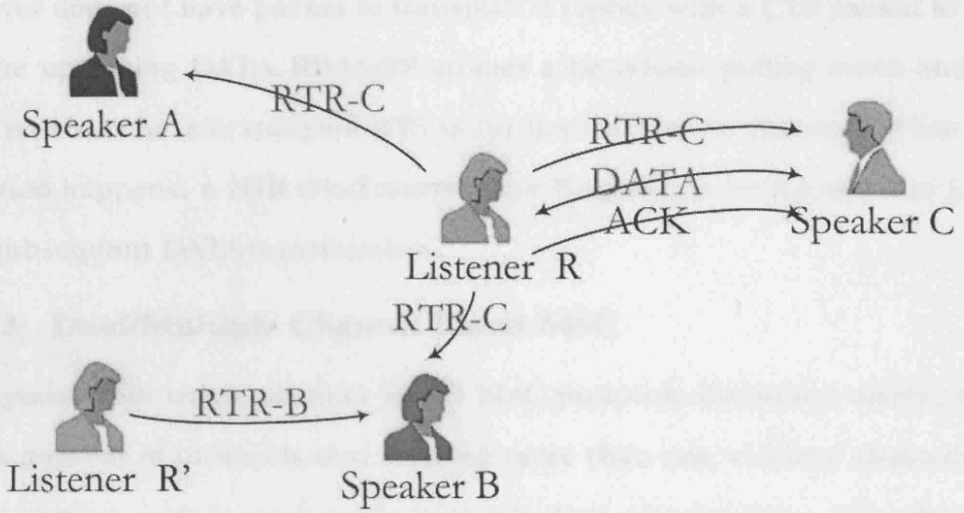

Figure 4.3: Receiver Initialized Protocols

the receiver initialized mechanism based on the MACA protocol. This polling based access mechanism has excellent collision avoidance capability. Data payload collision is completely avoided and control message collision is also efficiently alleviated. Unfortunately, the collision among control messages (RTR) still exists. In Fig. 4.3, if listener **R** and **R'** transmit invitation packet at the same time, the RTR packets (RTR-B and RTR-C) will collide with each other at speaker **B** and failed. The RIMA-SP /DP /BP (receiver initialized multiple access – simple polling /dual polling/ broadcast polling) [38; 39] follow the same line of receiver invitation and improve this kind of mechanism one step further. The RIMA-SP mechanism employs a RTR-DATA-ACK handshake. And the RIMA-DP mechanism further improves the protocol by change handshake process to RTR-DATA-DATA-ACK or RTS-CTS-DATA-ACK. The first DATA transmission is sent from the RTR receiver while the second DATA is sent from the RTR sender. More payload transmission is enabled by allowing a reverse payload transmission from the RTR sender to the RTR receiver. If the invited RTR

receiver does not have packet to transmit, it replies with a CTS packet to wait for the upcoming DATA. RIMA-BP utilizes a broadcast polling mode and the RTR receivers have to transmit RTS to further reserve the channel. When RTS collision happens, a NTR (No-Transmission-Request) is broadcasted to forbid the subsequent DATA transmission.

4.1.3 Dual/Multiple Channel Based MAC

Compared with single channel based MAC protocols discussed above, there are a number of protocols that utilizing more than one wireless channels for each wireless user to exclusively transmit their own packets. Two channels separation is another important implementation issue wherein both channels are used to transmit control messages and data packets separately and shared by each terminal. This type of protocols has inherent collision avoidance ability between control and data packets. By implementing random access MAC protocol on control channel only, the contending process happens on control channel only, so as to achieve collision free data payload transmission. One typical multi-channel implementation issue is assigning separated channel to each user for exclusive usage. There are usually several channels in a system which can be achieved by multiple access mechanisms like TDMA, FDMA and CDMA. As a result, collisions and interference among different users are efficiently alleviated or even avoided.

The IEEE 802.11 DCF (distributed coordination function) can be classified to a CDMA based multiple channel solution realized by a spread spectrum mechanism namely DSSS. Each node that communicates with the access point is assigned a pseudo noise (PN) code. The base band signal is then spread to a wide transmission band. The PN codes are orthogonal with each other so as to avoid interfere among users. Each PN code is then considered

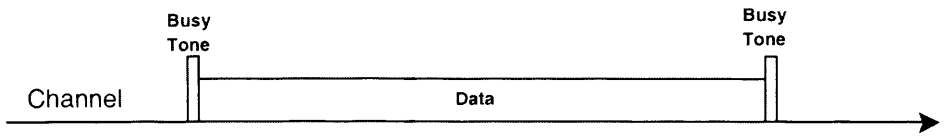

Figure 4.4: Busy Tone

as a separated channel.

Busy tone based MAC protocols are usually regarded as a special type of multiple channel issue. Busy tone signals occupy a separated and small (compared to the data transmission channel bandwidth) range of total available frequency bandwidth (Fig. 4.4). As a result, busy tone detection time is on the microsecond (ms) level. Busy tone signals can be transmitted with very simple method, for example a power impulse to indicate a busy tone is on without the conventional modulation and coding process. Thus, busy tone setting up and detecting time is considered as the major cost of busy tone based MAC protocols. Busy tone signals have only two statuses "on" and "off" so as to indicate the status of the channel(s) or indicate the state of individual terminals, "busy" and "idle". As an example in Fig. 4.5, a general access procedure of busy tone base random access MAC mechanism is provided. Speakers still use "hello" messages (RTS packets) to contend the listener. When one of them succeeds, instead of CTS, the listener broadcast a busy tone signal which can be considered as "wave hand" by the listener. This action indicates the RTS transmission is successful and the listener is waiting for the conversation. Note that the "wave hand" action can be performed along with the packet transmission. Thus, busy tone is able to be continuously broadcasted when the sender (speaker **C**) transmitting DATA until finished. Any other potential speakers (**A** or **B**) will then recognize the "wave hand" action and gets

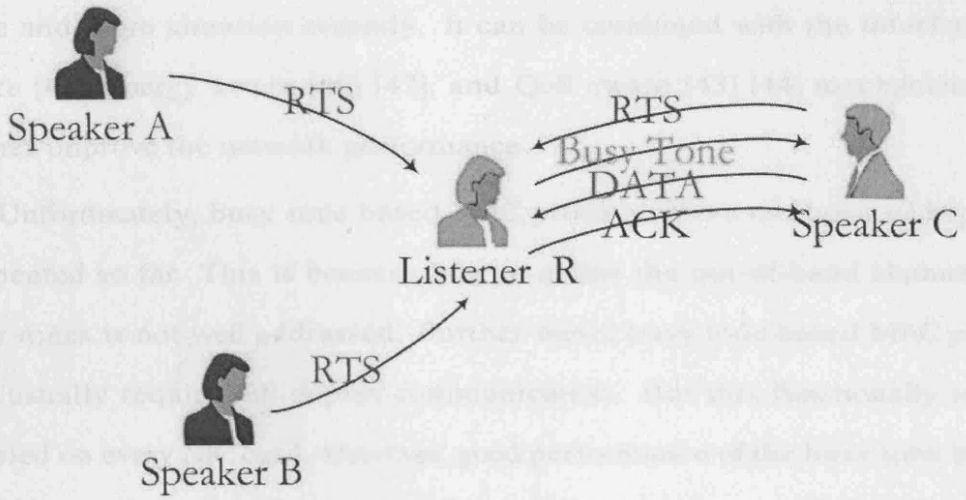

Figure 4.5: Busy Tone Based Protocols

aware of the busy status of the listener. They will keep silence and try to send RTS again until the busy tone is set off.

One of the most successful busy tone based MAC protocols is known as the dual busy tone multiple access (DBTMA) protocol [40]. In DBTMA, the control and data packets are transmitted on a single shared wireless channel. Two out of band busy tone signals are employed to indicate the status of terminal. BT_t indicates a terminal is transmitting RTS message and is broadcasted along with RTS transmission; while the BT_r indicates the terminal is receiving the data payload and is broadcasted when receiving DATA. According to the analysis, it is shown that the performance of DBTMA is much better than the RTS/CTS based protocols. The network performance is able to be greatly improved because of the busy tone assistance. In [41], the authors prove that the IEEE 802.11 MAC can be improved by busy tones; while in [42], it is proved that the TCP performance over wireless ad hoc networks is also improved because of busy tone assistance. Busy tone assisted MAC mechanism draws

more and more attention recently. It can be combined with the interference aware [45], energy aware [46] [47], and QoS aware [43] [44] mechanisms to further improve the network performance.

Unfortunately, busy tone based MAC protocols have not been widely implemented so far. This is because how to define the out-of-band channel for busy tones is not well addressed. Further more, busy tone based MAC protocols usually require full-duplex communication. But this functionally is not enabled on every NIC card. However, good performance of the busy tone based MAC protocols makes the implementation issue become an attractive topic.

4.2 Energy conservation

In the wireless communication environment, mobile terminals always have limited energy supply which makes the energy conservation become a continuous requirement. Generally speaking, the energy conservation capability is able to be optimized on each layer of protocol stack [51]. Here we consider the energy conservation only from the MAC/physical layer's perspective.

On mesh clients, energy is mainly spent on computation and communication, wherein the communication energy consumption takes the major part. The medium access procedure should be carefully designed to reduce the energy cost during the communication process: first of all, packet collision is the major energy waster, especially when traffic load is heavy [52; 53]. If collision happens, all involved packets are failed when capture effect [49] is not taken into account (from the pure MAC layer's perspective). They are scheduled for retransmission after a random backoff delay and contend to access the channel again. This involves a complicated process of sending, receiving, rescheduling and resending which waste a large amount of energy at the both

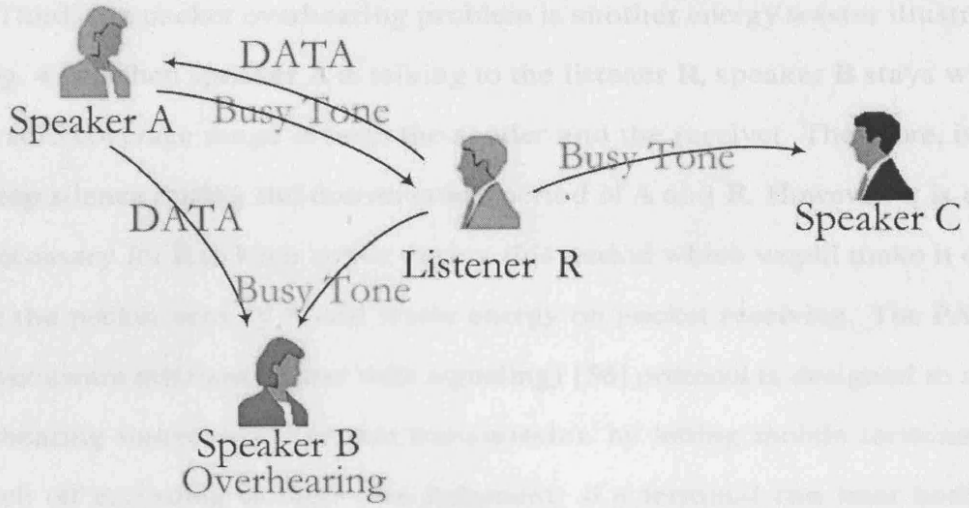

Figure 4.6: Packet Overhearing Problem

sides of senders and receivers. Thus, the packet collision is expected to be avoided as far as possible.

Second, mesh clients have to keep active and continuously sense carrier at all times to avoid missing any possible incoming packet (control or data). Thus, the idle listening procedure consumes a large amount of communication energy, e.g. the Idle: Receive: Send ratio is measured by 1:1.05:1.4 in [50]. The idle listening energy waste can be tackled by making mobile terminals wake up and sleep alternatively [54]. Thus, energy conservation can be alleviated with the cost of increasing access delay. Time slot scheme [55] is also able to reduce the energy cost on idle listening by dividing the time into equal sized slots and let the transmission be conducted at the beginning of each time slot. Then, packet receivers do not have to keep active all the time, but only at the beginning of each time slot. Time slot scheme requires the system to be perfectly synchronized. Thus, it is more suitable for the centralized structure networks rather the distributed ones.

Third, the packet overhearing problem is another energy waster illustrated in Fig. 4.6. When speaker **A** is talking to the listener **R**, speaker **B** stays within the radio coverage range of both the sender and the receiver. Therefore, it has to keep silence during the conversation period of **A** and **R**. However, it is quite unnecessary for **B** to keep active during this period which would make it overhear the packet sent by **A** and waste energy on packet receiving. The PAMAS (power aware medium access with signaling) [56] protocol is designed to avoid overhearing unnecessary packet transmission by letting mobile terminals to switch off according to their own judgment: if a terminal can hear both the busy tone from the listener and the DATA from the transmitter, he can then confirm he is not the intended receiver of the DATA packet. That terminal will then power itself off until the DATA transmission is finished so as to solve the overhearing problem.

From the physical layer's perspective, if the transmission power level is appropriately set, the packet is then able to arrive at the intended terminal with minimum power level required. Then the energy spent on packet transmission is reduced and at the same time the interference to other terminals which might induce collisions is reduced as well. With this methodology, MAC protocols are usually designed along with physical layer parameters, such as capture effect, SINR (signal to interference plus noise ratio), taken into account. This type of MAC protocol is summarized and discussed in the following part.

4.3 Interference Resistance

From the pure MAC layer's perspective, any simultaneous transmission that more than one packet arrive at the same receiver at the same time on the

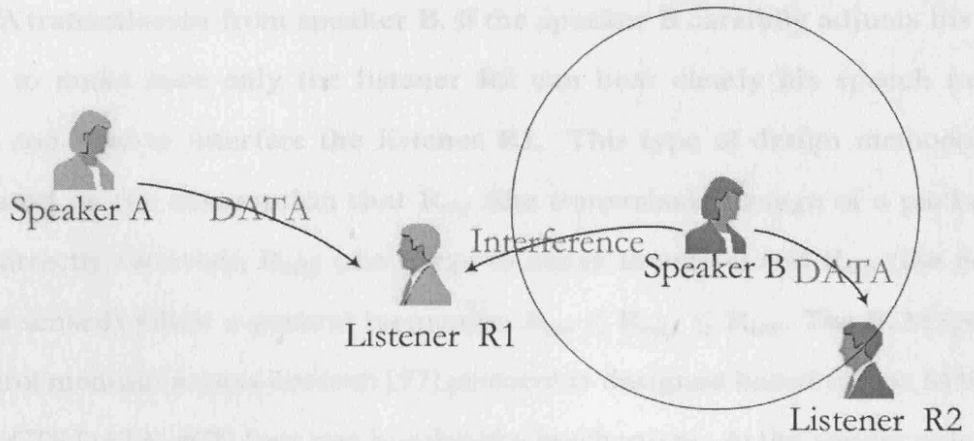

Figure 4.7: Transmission Interference

same channel will induce a packet collision. The unwanted packet is considered as the interference of the intended packet as illustrated in Fig. 4.7. This phenomenon will make the transmission from speaker **A** to listener **R1** failed. However, while considering the radio propagation characteristics, the power level of packets and signals will progressively fade when transmitted further. Thus, if the speaker **B** that transmits interfering packets stays far away from the listener **R1**, the interference is somehow tolerable. The interference tolerance capability highly depends on the signal to interference plus noise ratio (SINR). Interference is regarded as tolerable if the ratio between the intended signal and the interference plus noise has larger value than the required threshold.

According to this characteristic, carefully designing the transmission power level can reduce the interference among mobile terminals. One typical implementation is utilizing the power adaptive/interference aware mechanism over the pure MAC protocol, e.g. [61]. As an example in Fig. 4.7, when the listener **R1** is receiving DATA from the speaker **A**, he is able to hear another

DATA transmission from speaker **B**. If the speaker **B** carefully adjusts his volume to make sure only the listener **R2** can hear clearly his speech rather than too loud to interfere the listener **R1**. This type of design methodology is based on the assumption that R_{rec} (the transmission range of a packet to be correctly received), R_{intf} (the range to cause interfere) and R_{sen} (the range to be sensed) follow a general inequation $R_{rec} \leq R_{intf} \leq R_{sen}$. The PCM (power control medium access control) [57] protocol is designed based on the MACAW RTS-CTS-DATA-ACK four way handshake mechanism. At the sender side, the RTS is transmitted at the maximum power level. This power level is reduced to necessary level when transmitting DATA according to information included in the CTS packet sent back. The receiver transmits the CTS with the maximum power level as well and transmits ACK with reduced level according to the information included in DATA packet. This mechanism let the packet listener feedback to the speaker to inform minimum power volume required, and vice versa. As a result, radio transmission energy consumption is efficiently controlled with interference reduced at the same time. In [58], the DBTMA protocol is improved by selecting the appropriate transmission power level for busy tone signals and data packets. Busy tone signals broadcasted by the receiver are transmitted on the maximum power level to provide good protection of DATA protection during the packet receiving phase. The RTS and DATA packets are transmitted on the minimum power level to avoid interrupting other transmissions.

4.4 Rate Adaptation

When packets are transmitted on the unstable wireless links, unpredictable link fluctuation and interference determines the transmission rate is not able

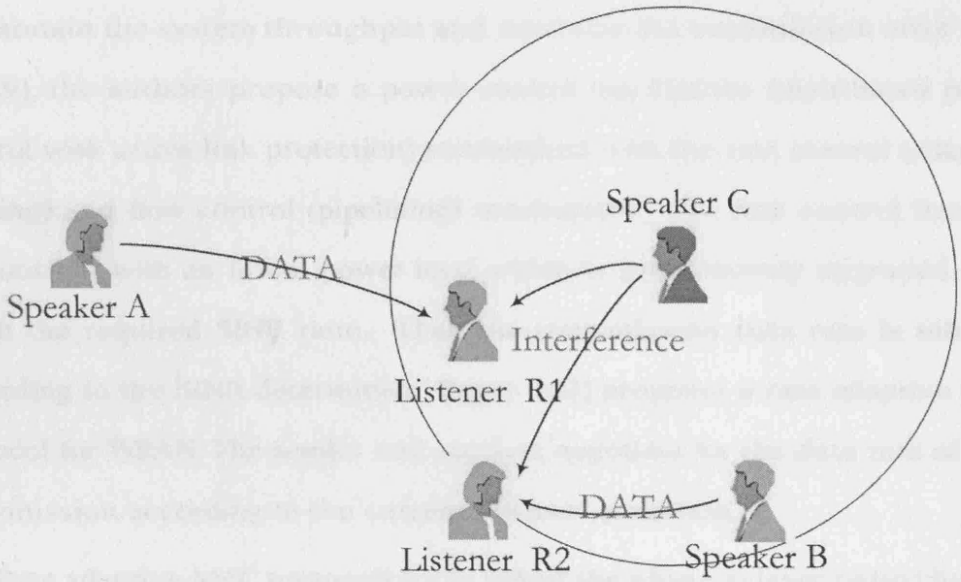

Figure 4.8: Rate Adaptive Protocols

to be fixed to a constant value. The rate usually varies according to the link quality and network environment. Generally speaking, a bad radio propagation environment requires packets be modulated by a more redundant mechanism to improve the interference resistance capability. The transmission rate is reduced at the same time. As an example in Fig. 4.8, if there are two ongoing transmissions from speaker **A** to listener **R1** and from **B** to listener **R2**, their transmission will be affected by the speaker **C**. If packets are transmitted on the same power level, the listener **R1** suffers more serious interference as it stays nearer to the interferer (speaker **C**) and farther to the intended sender (speaker **A**). As a result, speaker **A** has to transmit packet with much lower rate than speaker **B** to reduce error rate and retransmission times.

In order to deal with this problem, a number of solutions try to adapt the transmission rate according to the real-time SINR ratio at the receiver side. By monitoring the SINR, the optimal transmission rate can be selected

to maintain the system throughput and minimize the transmission error rate. In [59], the authors propose a power control mechanism (distributed power control with active link protection) combinated with the rate control (adaptive probing) and flow control (pipelining) mechanism. The first control frame is transmitted with an initial power level which is progressively upgraded until reach the required SINR ratio. Then the transmission data rate is selected according to the SINR determined. Paper [62] proposes a rate adaptive MAC protocol for WPAN. The sender and receiver negotiate for the data rate of next transmission according to the current channel condition.

Rate adaptive MAC protocols try to reflect the physical layer radio channel quality to the MAC layer and adjust the modulation method to satisfy physical layer requirements. Using a more redundant modulation mechanism will increase the packet transmission delay at the same time. As a result, the vulnerable period of packet transmission increase when transmission error rate decrease. Therefore, in order to balance transmission error rate and access delay, an appropriate modulation and coding mechanism should be carefully select.

4.5 Topology and Routing Control

In wireless mesh access networks, ad hoc and infrastructure modes are usually both used to support multi-hop data transmission from mesh clients to a mesh router. However, in case that all mesh clients stay within the radio coverage of the mesh router, they can communicate with the mesh router directly. The network topology is then a pure centralized architecture, as illustrated in Fig. 4.9(1), rather than the hybrid structure. If the transmission power of some clients, say client **C3**, is lowered down, the number of reachable neighbouring

terminals of **C3** is decreasing. If the communication range of **C3** is not able to cover the mesh router, some intermediate clients have to relay packet for it. Then, the network topology becomes a hybrid structure. By carefully adjust the power level of several clients within a WMAN, the network topology and packet transmission route are indirectly affected and controlled.

A number of benefits can be provided by the topology and routing control. As an example in Fig. 4.9(1), client **C3** and **C4** stay quite far away from the mesh router. Thus, their packet transmissions are quite sensitive to interference and noise at the receiver side and they usually have lower transmission data rate. If they transmit their packet through a multi-hop path of **C3-C1-R** and **C4-C2-R** respectively with radio coverage reduced, several benefits can be achieved: the transmission rate is improved with the interference reduced, the transmission successful rate is enhanced, and the traffic load on the mesh router is released.

This topology and routing control methodology can be achieved by both distributed and centralized manners. In the distributed manner, each client has to find the best route and the appropriate transmission power and rate by themselves. In order to achieve that, they have to monitor all transmissions of their neighbouring terminals to get enough information and make the decision. The centralized manner lets the mesh router to gather the information such as network traffic load, link quality, transmission successful rate, interference, etc. Then the mesh router is able to find an optimized network topology according to the information collected. Each mesh client can then be assigned with the transmission route and corresponding path.

With topology control scheme, the wireless mesh access network can be reconstructed to the architecture required, i.e. centralized or hybrid. Both

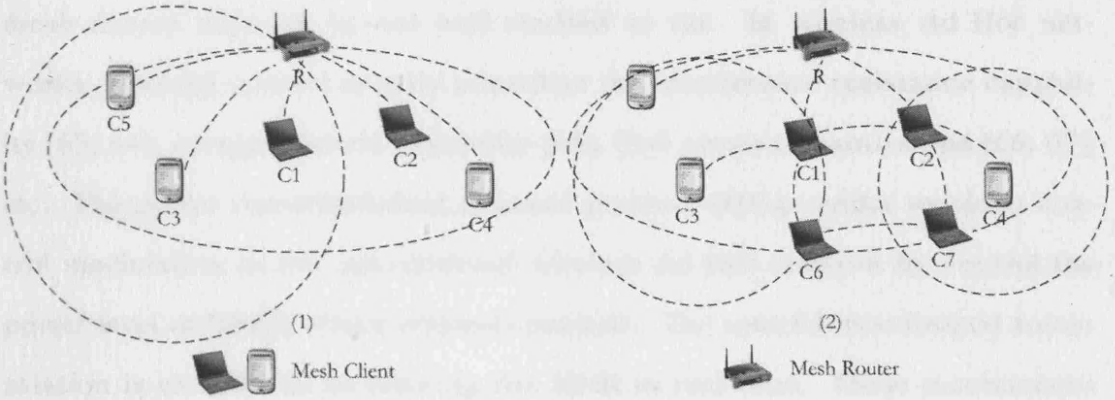

Figure 4.9: Topology Control Protocols

the centralized and hybrid network topologies have their advantages, disadvantages and requirements. For the centralized topology scenario (Fig. 4.9(1)), near-far effect damages the network severely and hence leads the clients staying further have lower successful access probability. However, each client can reach the mesh router via a one hop wireless connection which makes the access control easier to be performed and the access delay reduce quite a lot. The hybrid topology (Fig. 4.9(2)) is a good supplementary for the centralized mode. For communications between clients that stay one hop away from the mesh router, e.g. **C1** and **C2**, **C1-C2** client meshing is able to reduce traffic load and improve access successful rate on mesh router. For clients that stay far away from the mesh router, e.g. **C6** and **C7**, direct CC communication is obviously an optimized routing path for communications between them, i.e. the **C6-C7** link in Fig. 4.9(2). In order to decide the appropriate network topology, network traffic load situation on routing layer and the link quality on physical layer should be monitored in real time. As a result, network operation cost will increase unavoidably.

To the best of my knowledge, topology and routing control in wireless

mesh access network in not well studied so far. In wireless Ad Hoc networks, topology control usually considers the interference resistance capability [63; 64], energy efficient capability [65], QoS aware transmissions [66; 67], etc. The power controlled dual channel protocol [60] provides topology control mechanism in the conventional wireless Ad Hoc network by control the power level of RREQ (route request) packets. The interference-limited transmission is enabled by monitoring the SINR in real time. These mechanisms usually perform on a complete distributed manner with non-neglectable operation overhead in both computation and communication process. In wireless mesh access network, it is a better choice to let the mesh router to gather the network operation parameters and calculate the optimized network topology as well as implementing corresponding routing control mechanism based on that. The most challenging topic is to achieve efficient topology control with as little overhead as possible.

4.6 Physical/ MAC/Routing layer Misbehaviors and Countermeasures

The open network structure and ad hoc operation mode of WMNs make it possible for malicious attackers to sneak in, disguise as legitimate users, compromise mesh routers or clients, misbehave with communication protocols and launch a variety of attacks against different wireless functionalities, services and devices. Complicated authentication and data encryption algorithms [70] can prevent external attackers from entering the network and stealing valuable information. Besides, we need to use other techniques to address different security challenges and attacks in physical, MAC and network layers.

4.6.1 RF Jamming

In physical layer, attackers can make use of the inherent vulnerability of radio frequency (RF) transmission and generate jamming signals to interfere with communications between wireless users. Compared with mesh routers, wireless mesh clients have much less hardware resources (e.g. radio interface, power supply and data storage), processing power and communication capability. So they are more vulnerable to RF jamming attack. To generate strong interference at targeted users and wireless devices, RF jamming signal are usually narrow-band and have limited radio coverage range. So we can use wideband communication techniques, such as Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) to combat the interference of jamming signals. In additional, Orthogonal Frequency Division Multiplexing (OFDM) and Multiple-Input Multiple-Output (MIMO) techniques can be adapted to further improve the reliability and efficiency of data transmission over dynamic fading radio channels.

4.6.2 MAC Abusing

Contention-based MAC protocols are usually adopted in WMNs for wireless users to share the common wireless channel. In MAC layer, misbehaviors and attacks on the MAC layer [71] include selfish actions, misuse of access protocols and transmission forged packets/signals, so as to unfairly occupy wireless channel and resources. For example, a small backoff interval gives the corresponding user the advantages of getting access to the wireless channel quickly. The carrier sensing mechanism in many MAC protocols can be abused by falsely increasing waiting time in network allocate vector (NAV) or continuously broadcasting busy tone signals. As a result, the neighboring users will be kept in the silent/waiting status for long period and cannot ac-

cess the network for data transmission and reception. By Overhearing the NAV information and busy tone signals, an attacker can deliberately interrupt ongoing packet transmissions and resend forged packet to make the intended victim users and machines assuming their previous packet transmissions are not successful. In doing so, the victim users will be kept in working status and cannot enter the idle/sleep mode for saving energy. Forged packets with broadcasting address as the source will trigger all the listening users to broadcast these packets through the network, thus to waste energy and even jam normal packet transmissions. Such attacks are particularly damaging in wireless mesh access networks, because it can easily drain a mesh client of its limited battery power and destroy a multi-hop wireless path. To prevent MAC-layer abuses, misbehaviors and attacks, one solution is to use sophisticated authentication and encryption algorithms to enhance the handshake process in MAC protocols [72].

4.6.3 Routing Misbehavior

In network layer, typical routing misbehavior and attacks are to interrupt route discovery and maintenance process and tamper with routing table [73; 74]. For reactive on-demand routing protocols, such as Dynamic Source Routing (DSR) [75] and Ad hoc On-demand Distance Vector (AODV) [76], the source route and node list information in the Route Request (RREQ) and Route Reply (RREP) packets can be fabricated, replaced or deleted. An attacker can also advertise a route with false distance (shorter or longer) instead of the actual one in AODV to fail the routing protocol, reduce its efficiency, or even re-route important user data to somewhere else. For proactive table based routing protocols, such as Destination Sequenced Distance Vector (DSDV) [77] and Optimized Link State Routing (OLSR) [78], an attacker can

advertise modified routing table to lead all network traffic moving towards an intended address that might not exist, or generate routing loops. The attacker can then steal all packets and produce a sinkhole by selectively discarding any packets to disrupt the transmission of the network. Routing loop will cause data packets not be transmitted to their destinations, as well as waste many network resources, e.g. energy and storage, along the routing path. To address these routing misbehaviors and attacks, we can use the spanning tree protocol (STP) defined in IEEE 802.1D [79] to eliminate routing loops; and use geographic routing protocols to solve the routing table abusing problem by broadcasting geographic information. For on-demand routing protocols, unrealistic routes can be identified by a comprehensive routing discovering procedure with multiple neighboring machines and/or a comparison procedure of the time stamp and geographic information between source and destination. As a router behavior monitoring scheme, the "watchdog" [80] solution can identify malicious/compromised routers by monitoring the relaying or other behaviors, and apply the "path-rater" scheme to jump misbehaving routers. In order to deal with the threat of incorrect route temptation to on demand routing protocols, comprehensive routing discovering procedure is provided in [81]. By comparing the time stamp and geographic location information between route discovering packet's sender and receiver, a unrealistic route can be efficiently revealed. There are also a number secure routing protocols such as SRP [82], SEAD [83], Aridne [84], ARAN [85], SAODV [86; 87].

4.6.4 Flooding Attack

Among all these network security threat, Denial of Service (DoS) attack [88] and its derivation Distributed Denial of Service (DDoS) [89] are two classical attacking approaches which is easy to launch and hard to defend on almost

every layer of WMN. DoS/DDoS attack aims at the network resources (e.g. network bandwidth, energy [90]) and router/client resources (e.g. router/client memory, processing resource) to prevent them from providing good service to legitimate users [91]. Handshake messages, or other access control and collision avoidance packets on MAC layer, routing tables and route discovering packets on network layer, can be easily falsified to exclude some vital fields, include inexistent source or destination, or completely replaced by malformed ones. Normal operation of MAC message exchanging, route discovering and maintenance procedure will be suspended by these completely unreadable packets and tables. As a result, any additional requests from other network devices will not be replied by these terminals which struggle to resolve the received packets and tables. On the other hand, DoS can much easier be achieved by the well-known flooding attacks (TCP SYN flooding [92], ICMP flooding and UDP flooding). A DoS flooding makes use of overwhelming packets to exhaust resources on victim network, such as processing capability on individual devices and connection ability among network terminals. In WMN, DoS flooding is more damaging because of unstable wireless link, unbalanced usage of network resource and weaker network devices: mesh clients always have constraints on processing and energy capability; mesh routers next to the gateway and mesh clients close to the access point (mesh router) are normally heavier loaded; RF transmission is not able to supply satisfied bandwidth. A number of countermeasures [93; 94; 95] are developed to mitigate harms caused by DoS flooding: SYN cookies optimizes the TCP protocol by delaying the allocation of resource until the address of every client sent the request is verified; implementing firewall, rate-limiting and Access Control List (ACL) on routers to slow down an ongoing attack and prevent a outgoing DoS attack by

querying for enough information before processing requests. End-to-end authentication is suggested as well to make sure every user have a certification before using any network resource or access the wireless channel.

Chapter 5

Double Sense Multiple Access (DSMA)

In wireless mesh access network, wireless connections are consisted of CC (client-to-client) and CR (client-to-router) links. According to the network infrastructure illustrated in Fig. 2.5, this hybrid multi-hop system can be summarized as a spanning tree like transmission model shown in Fig. 5.1. In the model, mesh clients stay in geographic positions that are fanned-out. It is quite possible that more than one client on the boundary of sector (e.g. **D**, **E** and **F**) send their packets to the client/router (e.g. **A**) on the center. Both the CC and CR communications can be summarized as a multiple-sender-single-receiver random access process.

For CC communications, either the sender or the receiver are mesh clients. Each of them has limited resource on signal processing and wireless communication. According to this requirement, a simple mechanism "double sense" is proposed specifically for CC communications. Based on this mechanism, we propose two innovative busy tone based random access MAC protocols to deal with the packet collision problem, namely DSMA-D (double sense multiple access – double channel) and DSMA-S (double sense multiple access – single channel).

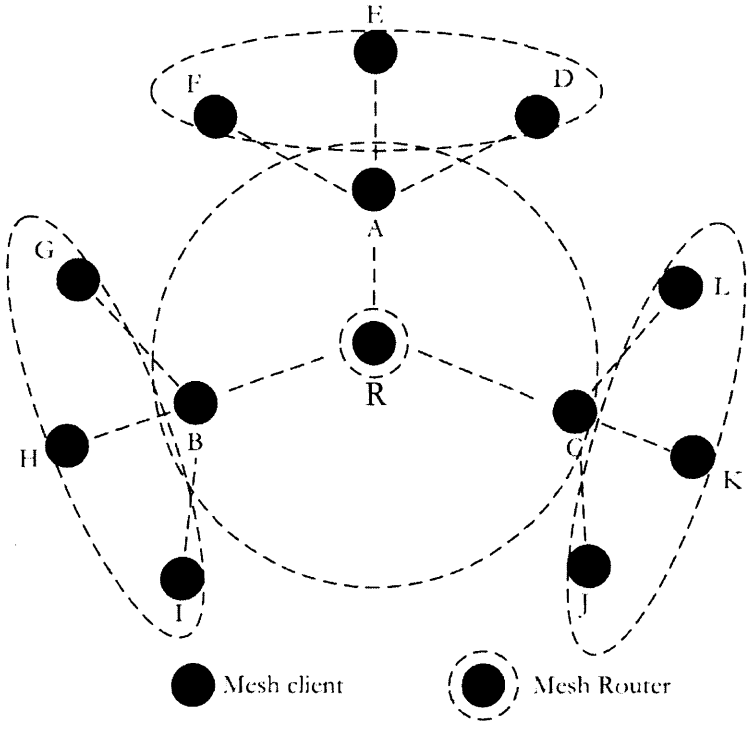

Figure 5.1: System Model

In DSMA (DSMA-D and DSMA-S), packets are separated and classified as control message and data payload. A control message represents an outgoing data payload transmission and contains brief information of it. The size of a data payload is much larger than a control message, thus it is longer in transmission time and more vulnerable for packet collisions. Therefore, it is extremely critical to guarantee a successful data payload transmission by avoiding control-data and data-data collisions. There are some presumptions given as follows:

1. Each mesh client has the same capability in terms of energy storage, power level, communication range and signal processing ability;
2. A full-duplex antenna is available on mesh clients which enables busy tone broadcasting along with packet transmission;
3. The mesh router is assumed to have no constraint on communication and processing ability, it has one dedicated full-duplex antenna for mesh access network.

Besides the above assumptions, channel efficiency and system throughput can be further improved by dividing both wireless channel(s) into time-synchronized slots. Transmitters are time synchronized with their intended receivers and transmit their packets only at the beginnings of time slots. Time synchronization can be achieved by using a common clock source from the mesh router within each wireless mesh access network. The length of a time slot, denoted by τ, should be set at least equal to the summation of the rise up and detection time of a busy tone signal, the maximum signal propagation delay within a terminal's radio coverage area, and the maximum packet processing delay. For the clients or the router with shorter signal propagation

and processing delay, they should wait until the beginning of the next time slot for further actions, e.g. sensing the busy tone signals and transmitting a new packet. In real implementations, slot length is selected slightly larger than the calculated or estimated value for the sake of system stability and reliability. For the sake of analysis, we choose to follow the tradition and assume τ is equal to the maximum propagation delay.

5.1 Double Sense Multiple Access – Double Channel (DSMA-D)

5.1.1 Access Mechanism of DSMA-D

The DSMA-D protocol uses two out-of-band busy tone signals BT_t and BT_r at the sender and the receiver side respectively, to indicate an occupied wireless channel. A control packet, request-to-send (RTS), is transmitted to reserve the channel for data payload (DATA) transmission. It contains brief information of the outgoing payload, such as the source and intended terminal ID, number of packets, priority level, etc. In order to avoid collisions between these two kinds of packets, RTS and DATA are transmitted through control and data channels, respectively. Channel is divided by using frequency or time division multiplexing (FDM or TDM). DATA-DATA collision avoidance can be achieved by the "double sense" mechanism , so as to guarantee the throughput performance. Access delay can be reduced by carefully specifying an appropriate retransmission policy (including a random backoff delay scheme), so as to avoid unnecessary time slot wastage. Note the improvement of channel efficiency and system throughput results in the reduction of access delay, and vice versa. The detailed algorithm of DSMA-D is analyzed step-by-step as follows.

Table 5.1: Access Mechanism of DSMA-D

DSMA-D Algorithm

Sender Side:

INPUT: a transmission attempt and the receiver's identity.

OUTPUT: the transmission attempt is failed or successful.

1. Check the status of both BT_r and BT_t at the beginning of next time slot.

2. IF either BT_r or BT_t is sensed, i.e. $BT_r = 1$ or $BT_t = 1$, THEN return failed.

3. ELSE do the following: (Both BT_r and BT_t signals are not sensed, i.e. $BT_r = 0$ and $BT_t = 0$.)

3.1 Send a RTS packet (including the receiver's identity) through the control channel and turn on the BT_t signal during the same period of time.

3.2 Check the status of BT_r signal at the beginning of next slot. Two time slots later, check it again. (The "double sense" mechanism.)

3.3 IF the BT_r signal is not sensed for the first time and sensed for the second time, i.e. $BT_r^1 = 0$ and $BT_r^2 = 1$, THEN do the following:

3.3.1 Send the DATA packet (including the receiver's identity) through the data channel and turn on the BT_t signal during the same period of time.

3.3.2 Return successful.

3.4 ELSE return failed.

Receiver Side:

INPUT: a RTS packet.

OUTPUT: a RTS transmission is successful or failed.

4. Keep receiving until the control channel become idle.

5. IF one RTS can be unpacked, setup BT_r signal; THEN return successful.

6. ELSE return failed.

Upon receiving a transmission attempt, i.e. a data packet and the receiver's identity, the transmitter follows the procedure in each data transmission or retransmission attempt as shown in Table 5.1. Atransmitter will sense both busy tone signals BT_t and BT_r at the beginning of next time slot (step 1). If neither BT_t nor BT_r is sensed, the RTS transmission is permitted (step 3). Otherwise, this attempt is regarded as fail (step 2). Note that the transmitter sends out a RTS packet (step 3.1) and then senses the BT_r signal twice (step 3.2) before making the decision (step 3.3) whether or not to send out its data packet through the data channel. If the attempt is failed, the corresponding data packet will be retransmitted after a random backoff delay. According to the specific QoS requirements for different real applications, the data packet may be discarded (blocked) after a certain number of failed retransmissions, or when the accumulated access delay exceeds the packet's life time. The receiver stays on the control channel and keeps listening any possible incoming RTS packets until this channel become idle again (step 4). If an intact RTS can be unpacked, BT_r signal is set up (step 5). Note that the two-slot gap between the double sensing actions of BT_r signal in step 3.2 is for compensating round-trip propagation delay. So the proposed DSMA-D protocol makes use of propagation delay to effectively prevent hidden terminals from generating DATA packet that collides with the existing DATA transmission.

As illustrated in Fig. 5.2, two mathematic models are constructed which are diverted from the Fig. 5.1 under two critical environments: all-hidden-sender and non-hidden-sender. In the all-hidden-sender environment, all packet senders stay out of the radio coverage of each other. Thus, they can not sense the BT_t signals broadcasted by senders, but the BT_r signal only that is broadcasted by the common receiver. In the non-hidden-sender environment,

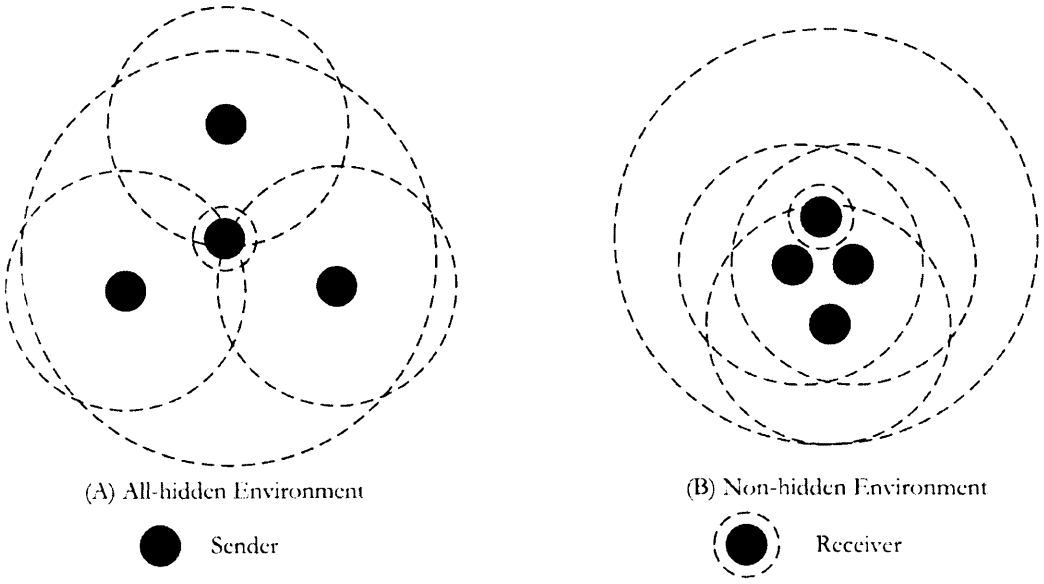

Figure 5.2: All-hidden and Non-hidden Environment

packet senders stay within the radio coverage range of each other. As a result, all packet senders are able to sense both the BT_r and all BT_t signals.

As an example, Fig. 5.3 shows the key features of DSMA-D access procedure in the all-hidden-sender environment. There are one receiver client **R** and seven transmitters, namely clients **A** to **G**. Senders cannot discover (sense) any BT_t signals, which are therefore omitted in the figure, from other transmitters so they always have $BT_t = 0$ in this case. Under the symmetric radio channel condition, the BT_r signal from the common packet receiver client **R** can be sensed by all those seven transmitters during a period of time, which is denoted by "BT_r Period" in the figure. As packet collisions occur only at the receiver, the channel status and access mechanism shown in Fig. 5.3 are from client **R**'s viewpoint. Hence, we observe one-slot propagation delay between "BT_r ON" and the beginning of a "BT_r Period", and between "BT_r OFF" and the end of a "BT_r Period". In this example, the lengths (transmission time)

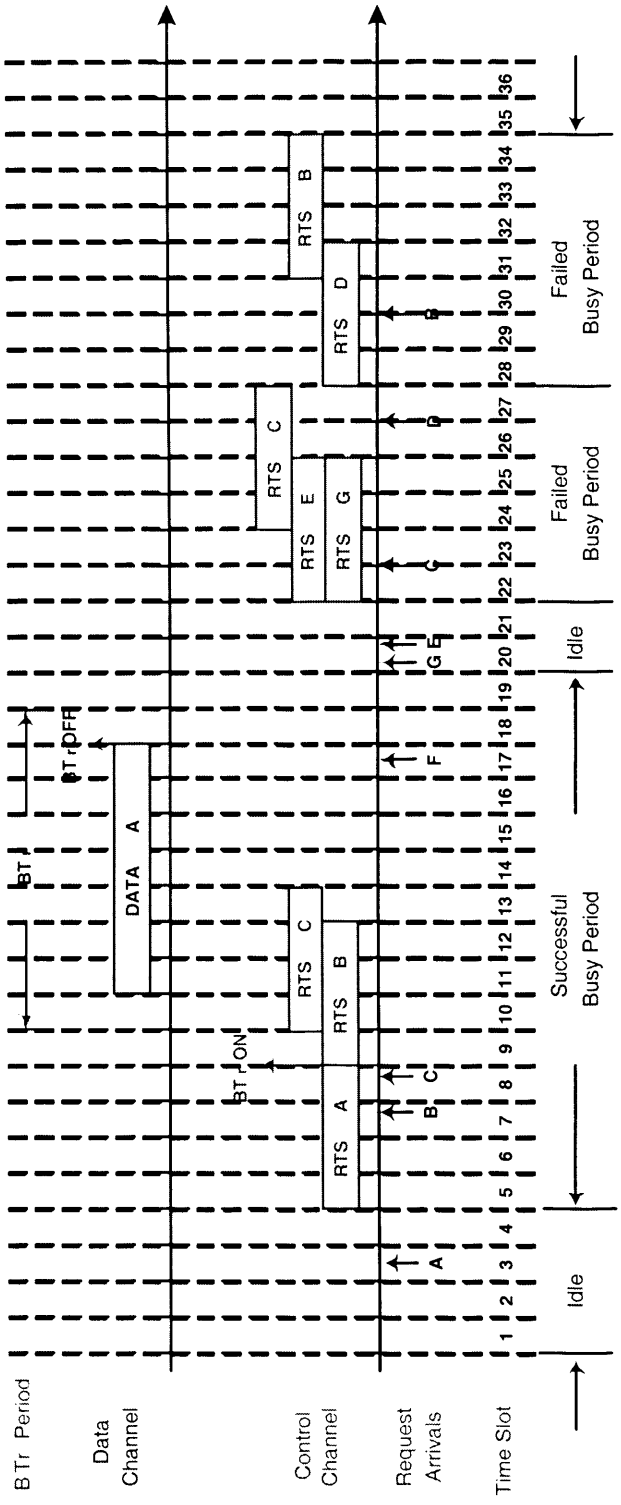

Figure 5.3: Access Procedure of DSMA-D, All-Hidden-Sender Environment.

of RTS and DATA are set to be four and seven time slots, respectively. In Fig. 5.3, a data transmission request arrives at client **A** within the third time slot. Since neither BT_t nor BT_r signal is sensed at the beginning of the fourth slot, **A** turns on its BT_t signal (not shown) and sends out a RTS packet, denoted by RTS-A. After one slot propagation delay, RTS-A arrives at the receiver client **R**. As soon as the whole RTS-A packet is correctly received (no packet collision), **R** turns on its BT_r signal at the end of the eighth slot as an acknowledgement. One-slot later, this BT_r signal can definitely be sensed by **R**'s neighboring clients (including the other six transmitters). Client **A** completes the transmission of RTS-A by the end of the seventh slot, it senses the BT_r signal twice at the beginnings of the eighth and tenth slots. The corresponding sensing results are "$BT_r^1 = 0$" and "$BT_r^2 = 1$". So client **A** knows that RTS-A has been correctly received by client **R** and the data channel has been reserved for DATA-A transmission (collision-free). It starts at the beginning of the tenth slot and arrives at client **R** after one-slot delay. Client **B** and **C** send their RTS at the beginning of eighth and ninth slots, respectively. They will not transmit their data packets because their double sensing results are "$BT_r^1 = 1$" and "$BT_r^2 = 1$". Clients **F** cannot even send out its RTS packets because it can sense the BT_r signal before the transmission attempt, i.e. $BT_r = 1$ in step 2 of the DSMA-D Algorithm. Clients **G**, **E** and **C** schedule their transmission and retransmission attempts at the 20^{th} and 22^{nd} slots. As senders are hidden to each other, they cannot discover other's BT_t signals so that send out their RTS packets. A collision occurs at the receiver **R** and those overlapped RTS packets are all destroyed. The three involved transmitters **G**, **E** and **C** will then obtain the same double sensing result, i.e. "$BT_r^1 = 0$, $BT_r^2 = 0$". Retransmission of **B** and **D** has the same access result of **G**, **E** and **C**: packet collision occurs and

the double sense results are "$BT_r^1 = 0, BT_r^2 = 0$". In the above cases, the transmission/retransmission attempts are failed and the corresponding terminals need to access the channel again after a random backoff delay, e.g. client **C** reschedule its first retransmission attempts during the 22^{rd} slot, but fail again. As illustrated in these examples, with the "double sense" mechanism and channel separation solution, DSMA-D provides sufficient information for packet transmitters. Thus they can make the right decision whether or not their DATA packet should be sent out immediately. In this way, DSMA-D completely solves the hidden terminal problem on data channel and guarantees collision free DATA transmission.

Fig. 5.4 illustrates the DSMA-D access procedure in the non-hidden-sender environment. Similarly, a data packet transmission request arrives at **A** within the 3^{rd} time slot and no busy tones are sensed at the beginning of the 4^{th} time slot. Client **A** turns on BT_t and start transmission RTS-A. This BT_t signal covers the channel from the beginning of the 5^{th} slot till the end of 8^{th} slot. If the RTS succeeds, the successful access procedure follows the same access steps of "double sense" and DATA transmission. The non-hidden-sender environment makes the BT_t signal be sensed by every contending client. Thus, client **B** and **C** that have transmission attempt arrive within 7^{th} and 8^{th} time slot are able to sense BT_t signal at the beginning of 8^{th} and 9^{th} slot. As a result, they won't transmit their RTS packets. In Fig. 5.4, client **D** and **E** schedule their transmission within the 20^{th} time slot. **D** can not sense the BT_t broadcasted by **E** since one time slot is required for BT_t propagation, and vice versa. Then, RTS collision happens and all involved packets are failed, i.e. RTS-D and RTS-E. If additional transmission attempt arrives within following part of collision period, e.g. client **F** schedules its transmis-

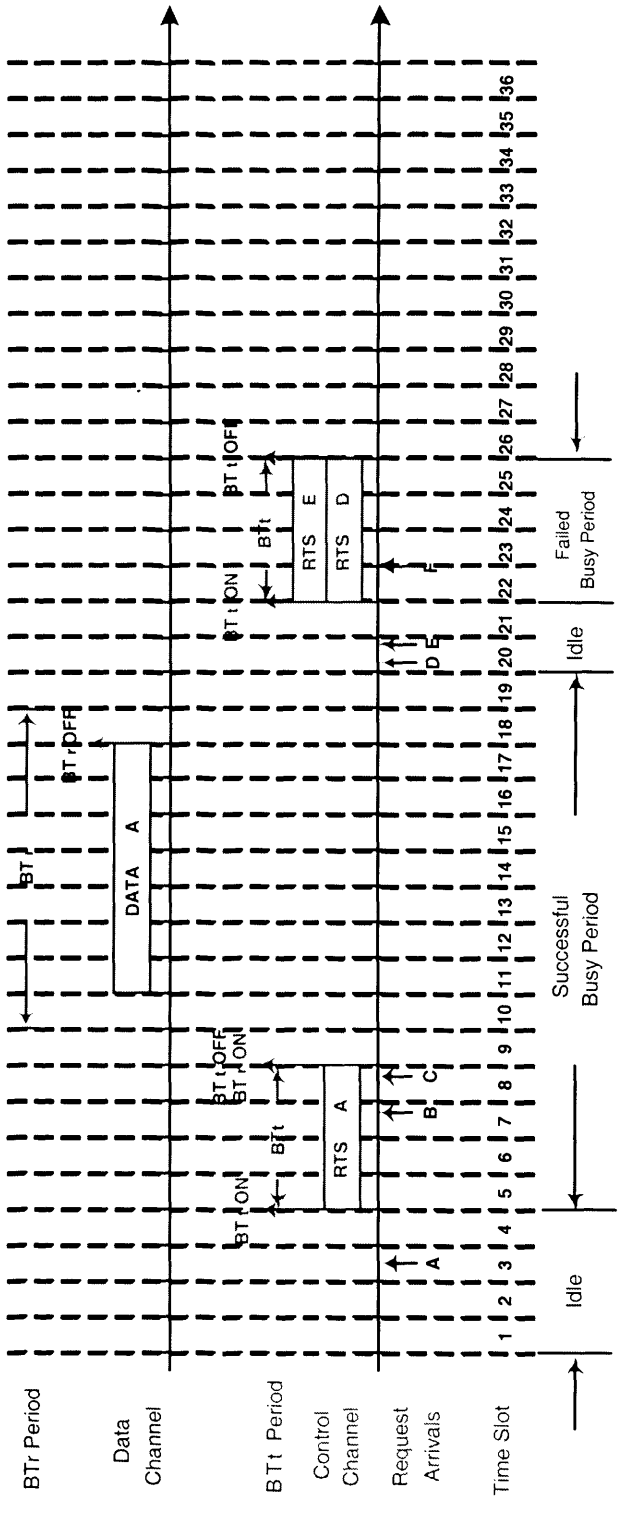

Figure 5.4: Access Procedure of DSMA-D, Non-Hidden-Sender Environment.

sion at the beginning of 23^{rd} sot, but it can not send RTS packet because of the BT_t signal is sensed.

As illustrated in this two examples, the vulnerable period of RTS packet is decreased in the non-hidden-environment. Thus, the DSMA-D performance in this environment are much better than the performance in the all-hidden-sender environment. However, in real applications, it is not reasonable to assume there are no hidden terminals at all. Thus, the performance in the all-hidden-sender and non-hidden sender environment actually indicate the lower bound and upper bound performance of DSMA-D, respectively.

5.1.2 Throughput, Delay and Blocking Probability Analysis of DSMA-D

In order to evaluate the efficiency of DSMA-D, a precise mathematic model is constructed to analyze the throughput, delay and blocking probability performance of DSMA-D in both all-hidden-sender and non-hidden-sender environment.

5.1.2.1 Throughput Analysis

Throughput performance is derived by using the conventional approach of busy period analysis [96; 97; 98; 99]. In the throughput analysis, transmissions are regarded as "discarded" when collision happens. Thus, the backoff state analysis and the Markov model in [100] is not taken into account. As all packet collisions and successful data transmissions occur only on the receiver, system throughput is defined as the average channel utilization ratio of receiver **R**. As shown in Fig. 5.3 and 5.4, "Busy" and "Idle" periods are defined by considering channel statuses. They appear alternatively and a pair of them (adjacent to each other) constitutes a transmission cycle. Busy periods can be further divided into "successful" and "failed" ones. With DSMA-D, a

collision-free RTS transmission can absolutely guarantee a successful DATA packet transmission. Therefore, a successful busy period contains a successful RTS and DATA packet transmission period. While a failed busy period has only overlapped, or collided, RTS packet transmissions. Let I, B_s and B_f denote the lengths of idle, successful and failed busy periods, respectively. The minimum value of I is zero, which occurs when two failed busy periods are adjacent neighbors. Within each successful busy period, the amount of time spent on transmitting the data packet is the useful channel utilization and denoted by U. System throughput S is defined as the average channel utilization over the average length of a transmission cycle, i.e.

$$S = \frac{E[U]}{E[I] + E[B]} = \frac{E[U]}{E[I] + E[B_s] \cdot p_s + E[B_f] \cdot (1 - p_s)} \tag{5.1}$$

where p_s is the success probability of a busy period or, equivalently, the success probability of a RTS packet transmission. Assume the combined arrival of new and delayed transmission attempts is a Poisson process with rate λ and assume no packet loss in radio transmission as well as no capture effect at the receiver. Without loss of generality, the transmission time of RTS and DATA packets are set to be γ and δ time slots (with the entire wireless channel), respectively.

Throughput in the All-Hidden-Sender Environment.

In the all-hidden-sender environment, signals from any contending sender can not be sensed by others. This makes the BT_t signal that sent along with a RTS packet loses its normal functionality. Thus, the entire transmission period of a RTS packet is vulnerable of collisions from simultaneous contending RTS transmissions. We assume the occupation ratio of control channel as C which ranges between 0 and 1 while the data channel as $D = 1 - C$. Therefore, the transmission duration of RTS and DATA in DSMA-D are $\gamma' = \gamma/C$ and

$\delta' = \delta/D$, respectively. The success probability p_s can be derived as [96; 97]:

$$p_{s(A)}^{DSMA-D} = \frac{\lambda\tau \cdot e^{-\gamma'\lambda\tau}}{1 - e^{-\lambda\tau}}, \tag{5.2}$$

wherein τ refers to the length of a time slot.

The length distribution of an idle period is given by:

$$P\{I = k\tau\} = e^{-\lambda k\tau} \cdot (1 - e^{-\lambda\tau}) \quad k = 1, 2, 3, \ldots . \tag{5.3}$$

So the average length of an idle period is:

$$E[I]_{(A)}^{DSMA-D} = \frac{e^{-\lambda\tau} \cdot \tau}{1 - e^{-\lambda\tau}}. \tag{5.4}$$

The length of a successful busy period is fixed and equal to the summation of the transmission time of a RTS packet, a DATA packet, and two round-trip propagation delay for turning on and off the BT_r signal, i.e.

$$B_{s(A)}^{DSMA-D} = (\gamma' + \delta' + 4) \cdot \tau. \tag{5.5}$$

Each successful busy period contains a successful DATA packet transmission, so the average channel utilization is simply given by:

$$E[U]_{(A)}^{DSMA-D} = D \cdot \delta'\tau \cdot p_{s(A)}^{DSMA-D}. \tag{5.6}$$

The minimum length of a failed busy period is equal to the transmission time of a RTS packet, i.e. $B_f \geq \gamma'\tau$. The distribution of B_f can be derived as (see Appendix A):

$$P\{B_f = (\gamma' + i)\tau\} = \begin{cases} \frac{(1-e^{-\lambda\tau}-\lambda\tau \cdot e^{-\lambda\tau}) \cdot e^{-\lambda\tau(\gamma'-1)}}{(1-e^{-\lambda\tau})(1-p_{s(A)}^{DSMA-D})}, & i = 0; \\ \\ \frac{e^{-\lambda\tau(\gamma'-1)} \cdot (1-e^{-\lambda\tau}) \cdot \alpha_i}{1-p_{s(A)}^{DSMA-D}}, & i \geq 1; \end{cases} \tag{5.7}$$

wherein the γ' is equivalent to the γ in Appendix A and α_i (i≥1) is an interim variable and is defined as:

$$\alpha_i = \begin{cases} 1, & 1 \le i \le \gamma' - 1; \\ 1 - e^{-\lambda\tau(\gamma'-1)}, & i = \gamma'; \\ \alpha_{i-1} - e^{-\lambda\tau(\gamma'-1)} \cdot \left(1 - e^{-\lambda\tau}\right) \cdot \alpha_{i-\gamma'}, & i \ge \gamma' + 1. \end{cases} \tag{5.8}$$

As a check, $\sum_{i=0}^{\infty} P\{B_f = (\gamma' + i)\tau\} = 1$. The detailed analysis of failed busy period is given in Appendix A.

The average length of a failed busy period is given by (see Appendix A):

$$E[B_f]_{(A)}^{DSMA-D} = \frac{\left(1 - e^{-\lambda\tau\gamma'}\right) \cdot \tau}{\left(e^{-\lambda\tau(\gamma'-1)} - e^{-\lambda\tau\gamma'}\right)\left(1 - p_{s(A)}^{DSMA-D}\right)} - \frac{\gamma'\tau \cdot p_{s(A)}^{DSMA-D}}{1 - p_{s(A)}^{DSMA-D}}. \tag{5.9}$$

By substituting (5.2), (5.4), (5.5), (5.6) and (5.9) into (5.1), system throughput is obtained as

$$\begin{aligned} S_{(A)}^{DSMA-D} &= \frac{D \cdot \lambda\tau \cdot \delta' e^{-\lambda\tau\gamma'}}{(\delta' + 4) \cdot \lambda\tau e^{-\lambda\tau\gamma'} + e^{\lambda\tau(\gamma'-1)}}, \\ &= \frac{D \cdot \delta' \cdot G}{(\delta' + 4) \cdot G + e^{(2\gamma'-1)G}}. \end{aligned} \tag{5.10}$$

where $G \triangleq \lambda\tau$ is referred to as "offered traffic".

Throughput in the Non-Hidden-Sender Environment.

In the non-hidden-sender environment, all RTS transmission is protected by BT_t signal after one slot propagation delay. Thus, the vulnerable period of RTS packet is only one time slot and the transmission successful probability is expressed as:

$$p_{s(N)}^{DSMA-D} = \frac{\lambda\tau \cdot e^{-\lambda\tau}}{1 - e^{-\lambda\tau}}. \tag{5.11}$$

Thus, the average channel utilization is:

$$E[U]_{(N)}^{DSMA-D} = D \cdot \delta'\tau \cdot p_{s(N)}^{DSMA-D}. \tag{5.12}$$

The length of a successful busy period is fixed and equal to the summation of the transmission time of a RTS packet, a DATA packet, and two round-trip propagation delay for turning on and off the BT_r signal, i.e.

$$B_{s(N)}^{DSMA-D} = (\gamma' + \delta' + 4) \cdot \tau . \tag{5.13}$$

Packet collision occurs only more than one RTS arrive within the same time slot. So the failed transmission probability is known as:

$$\begin{aligned} p_{f(N)}^{DSMA-D} &= 1 - p_{s(N)}^{DSMA-D}, \\ &= \frac{1 - e^{-\lambda\tau} - \lambda\tau \cdot e^{-\lambda\tau}}{1 - e^{-\lambda\tau}} . \end{aligned} \tag{5.14}$$

and the collision period length is:

$$B_{f(N)}^{DSMA-D} = \gamma' \cdot \tau. \tag{5.15}$$

The average length of the idle period is the same with the all-hidden-sender scenario:

$$E[I]_{(N)}^{DSMA-D} = \frac{e^{-\lambda\tau} \cdot \tau}{1 - e^{-\lambda\tau}} . \tag{5.16}$$

By substituting (5.11), (5.12), (5.15), (5.13) and (5.16) into (5.1), system throughput is obtained as:

$$\begin{aligned} S_{(N)}^{DSMA-D} &= \frac{D \cdot \delta' \tau \cdot \frac{\lambda\tau \cdot e^{-\lambda\tau}}{1-e^{-\lambda\tau}}}{\frac{e^{-\lambda\tau} \cdot \tau}{1-e^{-\lambda\tau}} + (\gamma' + \delta' + 4)\tau \cdot \frac{\lambda\tau \cdot e^{-\lambda\tau}}{1-e^{-\lambda\tau}} + \gamma'\tau \cdot \frac{1-e^{-\lambda\tau}-\lambda\tau \cdot e^{-\lambda\tau}}{1-e^{-\lambda\tau}}}, \\ &= \frac{D \cdot \delta' \cdot G}{(\delta' + 4) \cdot G + \gamma' \cdot (e^G - 1) + 1}. \end{aligned} \tag{5.17}$$

where $G \triangleq \lambda\tau$ is referred to as "offered traffic".

5.1.2.2 Access Delay and Blocking Probability Analysis

Access delay D is defined as the duration from the generation of a transmission attempt to the moment it is successfully transmitted [103]. We assume the synchronization process takes a fixed value of delay denoted by

D_0 in our analysis. A uniform distributed backoff procedure with (random variable W and ($W \geq 1$)) is performed after every unsuccessful transmission/retransmission before reaching the maximum retransmission threshold, say r_{max}. A packet transmission attempt is discarded (blocked) when its failed retransmissions reaches r_{max}. According to the access mechanism of DSMA-D, the different duration of access delay is calculated after each packet transmission or retransmission attempt.

Access Delay Distribution in All-Hidden-Sender Environment.

According to DSMA-D algorithm, a transmitter needs to check the status of both BT_t and BT_r signals before sending out its RTS packet. In the all-hidden-sender environment, as BT_t from senders are not able to be sensed by hidden terminals, the BT_r status from receiver determines further actions.

CASE I: NO RTS PACKET IS TRANSMITTED.

Within one transmission cycle, the average length of BT_r period is $(\delta' + 2)\tau \cdot p_{s(A)}^{DSMA-D}$. It consists of a δ' period DATA transmission and a round-trip propagation delay for BT_r raising up and turning off $(\delta' + 2)$. The BT_r period is conditioned with a successful RTS transmission probability ($p_{s(A)}^{DSMA-D}$). So the probability that the BT_r signal is sensed (hence no RTS packet is transmitted) is given by:

$$\begin{aligned} p_{1(A)} &= \frac{(\delta' + 2)\tau \cdot p_{s(A)}^{DSMA-D}}{E[I]_{(A)}^{DSMA-D} + E[B]_{(A)}^{DSMA-D}}, \\ &= \frac{(\delta' + 2) \cdot G}{(\delta' + 4) \cdot G + e^{(2\gamma' - 1)G}}. \end{aligned} \tag{5.18}$$

For this case, in order to avoid the transmitter sensing the same BT_r signal again, the corresponding backoff delay $D_{1(A)}$ before the next retransmission attempt should be set longer than $(\delta' + 1)$ time slots. We let:

$$D_{1(A)} = (W + \delta' + 1) \cdot \tau. \tag{5.19}$$

where W ($W \geq 1$) is a random variable selected according to the specific backoff policy

CASE II: $\mathrm{BT}_r^1 = 1$ AND $\mathrm{BT}_r^2 = 1$.

Except for "Case I", a RTS packet is transmitted in the remaining three cases. The "double sense" mechanism will then be used to determine whether or not a data packet transmission should follow. The probability that the double sensing results are "$\mathrm{BT}_r^1 = 1$" and "$\mathrm{BT}_r^2 = 1$" is given by:

$$\begin{aligned} p_{2(A)} &= \frac{2\tau \cdot p_{s(A)}^{DSMA-D}}{E[I]_{(A)}^{DSMA-D} + E[B]_{(A)}^{DSMA-D}}, \\ &= \frac{2G}{(\delta' + 4) \cdot G + e^{(2\gamma' - 1)G}}. \end{aligned} \tag{5.20}$$

In this case, the intended RTS packet transmission fails but the receiver has successfully received a RTS packet from another transmitter. For example, clients **B** and **C** in Fig. 5.3 experience this situation. To ensure the failed transmitter's next retransmission attempt not occurring within the same BT_r period, the corresponding backoff delay $D_{2(A)}$ is set as:

$$D_{2(A)} = (W + \delta' + 3) \cdot \tau. \tag{5.21}$$

CASE III: $\mathrm{BT}_r^1 = 0$ AND $\mathrm{BT}_r^2 = 1$.

This is the successful case for RTS and DATA transmissions. Within a transmission cycle, in order to guarantee a successful RTS transmission, the idle period should be more than one RTS duration. Thus, the average length $E[I_s]_{(A)}^{DSMA-D}$ of the idle period that guarantees a successful RTS (and DATA) packet transmission can be derived as:

$$\begin{aligned} E[I_s]_{(A)}^{DSMA-D} &= \sum_{i=0}^{\infty} (i+1)\tau \cdot P\left\{I = (\gamma' + i)\tau\right\}, \\ &= \frac{e^{-\gamma' G} \cdot \tau}{1 - e^{-G}}. \end{aligned} \tag{5.22}$$

And the probability that the double sensing results are "$\mathrm{BT}_r^1 = 0$" and "$\mathrm{BT}_r^2 = 1$" is simply given by:

$$\begin{aligned} p_{suc(A)}^{DSMA-D} &= \frac{E[I_s]_{(A)}^{DSMA-D}}{E[I]_{(A)}^{DSMA-D} + E[B]_{(A)}^{DSMA-D}}, \\ &= \frac{1}{(\delta' + 4) \cdot G + e^{(2\gamma'-1)G}}. \end{aligned} \tag{5.23}$$

The corresponding delay $D_{3(A)}$ is equal to the summation of the transmission times of RTS packet, data packet, and a two-slot round-trip propagation delay, i.e.

$$D_{3(A)} = (\gamma' + \delta' + 2) \cdot \tau. \tag{5.24}$$

CASE IV: $\mathrm{BT}_r^1 = 0$ AND $\mathrm{BT}_r^2 = 0$.

In this case, RTS-RTS packet collision occurs. All the involved (overlapped) RTS packets are destroyed (cannot be correctly received by the receiver) and should be retransmitted. The probability of this case can be simply calculated as:

$$\begin{aligned} p_{4(A)} &= 1 - p_1 - p_2 - p_{suc(A)}^{DSMA-D}, \\ &= \frac{e^{(2\gamma'-1)G} - 1}{(\delta' + 4) \cdot G + e^{(2\gamma'-1)G}}. \end{aligned} \tag{5.25}$$

To avoid a repeated collision with the same RTS packets, the corresponding backoff delay $D_{4(A)}$ is set as:

$$D_{4(A)} = (W + 2\gamma' - 2) \cdot \tau. \tag{5.26}$$

Access Delay Distribution in Non-Hidden-Sender Environment.

In the non-hidden-sender environment, as each BT_t signal can be successfully sensed by all packet senders. The busy tone coverage period increases significantly in this scenario which affects the access delay distribution.

CASE I: BT_r IS SENSED.

Within one transmission cycle, the average length of BT_r period is $(\delta'+2)\tau \cdot p_{s(N)}^{DSMA-D}$. That is a $\delta'+2$ BT_r coverage length, conditioned a successful RTS transmission. So the probability that the BT_r signal is sensed (hence no RTS packet is transmitted) is given by:

$$\begin{aligned} p_{1(N)} &= \frac{(\delta'+2)\tau \cdot p_{s(N)}^{DSMA-D}}{E[I]_{(N)}^{DSMA-D} + E[B]_{(N)}^{DSMA-D}}, \\ &= \frac{(\delta'+2)\cdot G}{(\delta'+4)\cdot G + \gamma' \cdot (e^G - 1) + 1}. \end{aligned} \tag{5.27}$$

For this case, in order to avoid the transmitter sensing the same BT_r signal again, the corresponding backoff delay $D_{1(N)}$ before the next retransmission attempt should be set longer than $(\delta'+1)$ time slots. We let:

$$D_{1(N)} = (W + \delta' + 1)\cdot \tau . \tag{5.28}$$

where W ($W \geq 1$) is a random variable selected according to the specific retransmission policy

CASE II: BT_t IS SENSED.

The length of a BT_t period is $\gamma'\tau$ conditioned with at least one RTS arrive within a time slot $(1-e^{-\lambda\tau})$. Thus, the probability of sensing a BT_t signal is:

$$\begin{aligned} p_{2(N)} &= \frac{\gamma'\tau \cdot (1-e^{-\lambda\tau})}{E[I]_{(N)}^{DSMA-D} + E[B]_{(N)}^{DSMA-D}}, \\ &= \frac{\gamma' \cdot (1-e^{-G})^2 \cdot e^G}{(\delta'+4)\cdot G + \gamma' \cdot (e^G - 1) + 1}. \end{aligned} \tag{5.29}$$

In this case, in order to avoid the transmitter sensing the same BT_t signal again, the corresponding backoff delay $D_{2(N)}$ before the next retransmission attempt should be set longer than $(\gamma'$ - 1) time slots. $D_{2(N)}$ is set as:

$$D_{2(N)} = (W + \gamma' - 1)\cdot \tau . \tag{5.30}$$

CASE III: $BT_r^1 = 0$ AND $BT_r^2 = 1$.

Apart from the above two cases, a RTS packet is transmitted in the remaining two cases. The "double sense" mechanism will then be used to determine whether or not DATA transmission should follow. Double sensing results of "$BT_r^1 = 0$" and "$BT_r^2 = 1$" indicates the successful case for RTS and DATA transmissions. Within a transmission cycle, in order to guarantee a successful RTS transmission, the idle period should be more than one time slot. Thus, the average length $E[I_s]_{(N)}^{DSMA-D}$ of the idle period that guarantees a successful RTS (and DATA) packet transmission can be derived as:

$$\begin{aligned} E[I_s]_{(N)}^{DSMA-D} &= \sum_{i=0}^{\infty} (i+1)\tau \cdot P\{I = (1+i)\tau\} , \\ &= \frac{e^{-G} \cdot \tau}{1 - e^{-G}} . \end{aligned} \tag{5.31}$$

And the probability that the double sensing results are "$BT_r^1 = 0$" and "$BT_r^2 = 1$" is simply given by:

$$\begin{aligned} p_{suc(N)}^{DSMA-D} &= \frac{E[I_s]_{(N)}^{DSMA-D}}{E[I]_{(N)}^{DSMA-D} + E[B]_{(N)}^{DSMA-D}} , \\ &= \frac{1}{(\delta' + 4) \cdot G + \gamma' \cdot (e^G - 1) + 1} . \end{aligned} \tag{5.32}$$

The corresponding delay $D_{3(N)}$ is equal to the summation of the transmission times of RTS packet, data packet, and a two-slot round-trip propagation delay, i.e.

$$D_{3(N)} = (\gamma' + \delta' + 2) \cdot \tau . \tag{5.33}$$

CASE IV: $BT_r^1 = 0$ AND $BT_r^2 = 0$.

In this case, RTS-RTS packet collision occurs. All the involved (overlapped) RTS packets are destroyed (cannot be correctly received by the receiver) and should be retransmitted. The probability of this case can be simply

calculated as:

$$\begin{aligned} p_{4(N)} &= 1 - p_1 - p_2 - p_{suc(N)}^{DSMA-D}, \\ &= \frac{2G + \gamma' \cdot (1 - e^{-G})}{(\delta' + 4) \cdot G + \gamma' \cdot (e^{G} - 1) + 1}. \end{aligned} \tag{5.34}$$

When "double sense" is finished, the collision period has also finished as well. The corresponding access delay $D_{4(N)}$ is simply equal to the backoff delay:

$$D_{4(N)} = W \cdot \tau. \tag{5.35}$$

Average Access Delay and Blocking Probability

Let R denote the total number of retransmissions needed before a successful RTS/DATA packet transmission. When the backoff delay range is much larger than DATA transmission time slots, packet transmissions and retransmissions are "almost" independent. Thus R can be accurately approximated by a geometrically distributed random variable with the success transmission probability p_{suc} as the parameter. Conditioning on $R \leq r_{max}$, the retransmission distribution of those successful data packets is given by

$$P\{R = r \mid R \leq r_{max}\} = \frac{p_{suc}^{DSMA-D}(1 - p_{suc}^{DSMA-D})^r}{1 - (1 - p_{suc}^{DSMA-D})^{r_{max}+1}}, \quad r = 0, 1, 2, \ldots, r_{max}. \tag{5.36}$$

And the blocking probability P_B is defined as

$$P_B = P\{R > r_{max}\} = (1 - p_{suc}^{DSMA-D})^{r_{max}+1}. \tag{5.37}$$

Thus, the access blocking probability in the all-hidden-sender and the non-hidden-sender environments are given by:

$$P_{B(A)} = P\{R > r_{max}\} = (1 - p_{suc(A)}^{DSMA-D})^{r_{max}+1}. \tag{5.38}$$

and

$$P_{B(N)} = P\{R > r_{max}\} = (1 - p_{suc(N)}^{DSMA-D})^{r_{max}+1}. \tag{5.39}$$

The mean value of R is given by:

$$E[R]^{DSMA-D} = \frac{(1-p_{suc}^{DSMA-D}) - (p_{suc}^{DSMA-D} r_{max}+1)(1-p_{suc}^{DSMA-D})^{r_{max}+1}}{\left[1-(1-p_{suc}^{DSMA-D})^{r_{max}+1}\right]\cdot p_{suc}^{DSMA-D}}. \tag{5.40}$$

There are four cases of access delay D_1, D_2, D_3 and D_4 with corresponding probabilities p_1, p_2, p_{suc}^{DSMA-D} and p_4. So we let M and N ($0 \leq M+N \leq R$) denote the numbers of failed transmission attempts due to the Cases I and II, respectively. The joint distribution of R, M and N is given by

$$P\{R=r, M=m, N=n\} = \binom{r}{m}\binom{r-m}{n} p_{suc}^{DSMA-D} p_1^m p_2^n p_4^{r-n-m}. \tag{5.41}$$

The mean values of M and N can be derived as

$$E[M]^{DSMA-D} = \frac{\left(\frac{p_1}{p_1+p_{suc}^{DSMA-D}}\right) - \left(\frac{p_{suc}^{DSMA-D} r_{max}}{p_1+p_{suc}^{DSMA-D}}+1\right)\cdot\left(\frac{p_1}{p_1+p_{suc}^{DSMA-D}}\right)^{r_{max}+1}}{\left[1-\left(\frac{p_1}{p_1+p_{suc}^{DSMA-D}}\right)^{r_{max}+1}\right]\cdot\frac{p_{suc}^{DSMA-D}}{p_1+p_{suc}^{DSMA-D}}}, \tag{5.42}$$

and

$$E[N]^{DSMA-D} = \frac{\left(\frac{p_2}{p_2+p_{suc}^{DSMA-D}}\right) - \left(\frac{p_{suc}^{DSMA-D} r_{max}}{p_2+p_{suc}^{DSMA-D}}+1\right)\cdot\left(\frac{p_2}{p_2+p_{suc}^{DSMA-D}}\right)^{r_{max}+1}}{\left[1-\left(\frac{p_2}{p_2+p_{suc}^{DSMA-D}}\right)^{r_{max}+1}\right]\cdot\frac{p_{suc}^{DSMA-D}}{p_2+p_{suc}^{DSMA-D}}}. \tag{5.43}$$

Let $D_{1,i}$, $D_{2,j}$ and $D_{4,k}$ denote the i^{th}, j^{th} and k^{th} backoff delay due to the Cases I, II and IV, respectively. The total access delay D is given by

$$\begin{aligned} D^{DSMA-D} &= D_0 + D_3 + \sum_{i=1}^{M} D_{1,i} + \sum_{j=1}^{N} D_{2,j} + \sum_{k=M+N+1}^{R} D_{4,k} \\ &= D_0 + D_3 + \tau\cdot\sum_{l=1}^{R} W_l + M\cdot D_1 + N\cdot D_2 + (R-M-N)\cdot D_4 \end{aligned} \tag{5.44}$$

where W_l represents the random backoff delay value due to the l^{th} failed transmission. In this chapter, the distribution of W_l is assumed the same for all

transmitting terminals and all retransmission attempts. So we obtain the same average value $E[W_l] = E[W]$, irrespective of different terminals and retransmission times. The average of access delay is therefore

$$\begin{aligned} E[D]^{DSMA-D} &= D_0 + D_3 + E[W] \cdot E[R]^{DSMA-D} + D_1 \cdot E[M]^{DSMA-D} \\ &+ D_2 \cdot E[N]^{DSMA-D} + D_4 \cdot (E[R]^{DSMA-D} \\ &- E[M]^{DSMA-D} - E[N]^{DSMA-D}) \end{aligned} \tag{5.45}$$

By substituting equation (5.18), (5.20) and (5.23) into (5.40), (5.42) and (5.43) the $E[R]^{DSMA-D}$, $E[M]^{DSMA-D}$ and $E[N]^{DSMA-D}$ in the all-hidden-sender environment are derived, and we have $E[R]_{(A)}^{DSMA-D}$, $E[M]_{(A)}^{DSMA-D}$ and $E[N]_{(A)}^{DSMA-D}$. Further more, substituting these values as well as using (5.19), (5.21), (5.24) and (5.26) to replace the D_1, D_2, D_3 and D_4 in (5.45), we get the expected delay as:

$$\begin{aligned} E[D]_{(A)}^{DSMA-D} &= D_0 + D_{3(A)} + E[W] \cdot E[R]_{(A)}^{DSMA-D} + D_1 \cdot E[M]_{(A)}^{DSMA-D} \\ &+ D_{2(A)} \cdot E[N]_{(A)}^{DSMA-D} + D_{4(A)} \cdot (E[R]_{(A)}^{DSMA-D} \\ &- E[M]_{(A)}^{DSMA-D} - E[N]_{(A)}^{DSMA-D}) \\ &= (\gamma' + \delta' + 3)\tau + E[W]E[R]_{(A)}^{DSMA-D} + E[M]_{(A)}^{DSMA-D}(\delta' + 1)\tau \\ &+ E[N]_{(A)}^{DSMA-D}(\delta' + 3)\tau + (E[R]_{(A)}^{DSMA-D} \\ &- E[M]_{(A)}^{DSMA-D} - E[N]_{(A)}^{DSMA-D})(2\gamma' - 2)\tau \,. \end{aligned} \tag{5.46}$$

Using the same method, the average access delay in the non-hidden-

sender environment is known as:

$$\begin{aligned} E[D]_{(N)}^{DSMA-D} &= D_0 + D_{3(N)} + E[W] \cdot E[R]_{(N)}^{DSMA-D} + D_1 \cdot E[M]_{(N)}^{DSMA-D} \\ &+ D_{2(N)} \cdot E[N]_{(N)}^{DSMA-D} + D_{4(N)} \cdot (E[R]_{(N)}^{DSMA-D} \\ &- E[M]_{(N)}^{DSMA-D} - E[N]_{(N)}^{DSMA-D}) \\ &= (\gamma' + \delta' + 3)\tau + E[W]E[R]_{(N)}^{DSMA-D} + E[M]_{(N)}^{DSMA-D}(\delta' + 1)\tau \\ &+ E[N]_{(N)}^{DSMA-D}(\gamma' - 1)\tau \,. \end{aligned} \tag{5.47}$$

5.1.2.3 Analytical/Simulation Results and Discussion

Analytical curves are plotted according to the equations of throughput, delay and blocking probability, i.e. equation (5.10), (5.17), (5.38), (5.39), (5.46) and (5.47). The simulation that operates on a C++ platform describes the random access channel of a receiver when a number of transmission attempts try to access this channel. The process of transmission attempt arrival follows the Poisson distribution. For concept prove, the DSMA-D is simulated only in the all-hidden-sender environment to verify the accuracy of the throughput, delay and blocking probability analysis.

In theory, the channel separation scheme of DSMA-D reduces the channel utilization ratio since the control and data packets are transmitted alternatively on dedicated control and data channels. The system throughput is therefore severely affected and reduced. Without losing generality, we use FDM to achieve the channel separation wherein control and data channel occupy fixed part of wireless spectrum bandwidth to transmit RTS and DATA, respectively. Thus the channel separation refers to the wireless spectrum bandwidth division for control and data channels in our simulation.

Fig. 5.5 illustrates the DSMA-D channel throughput versus offered load

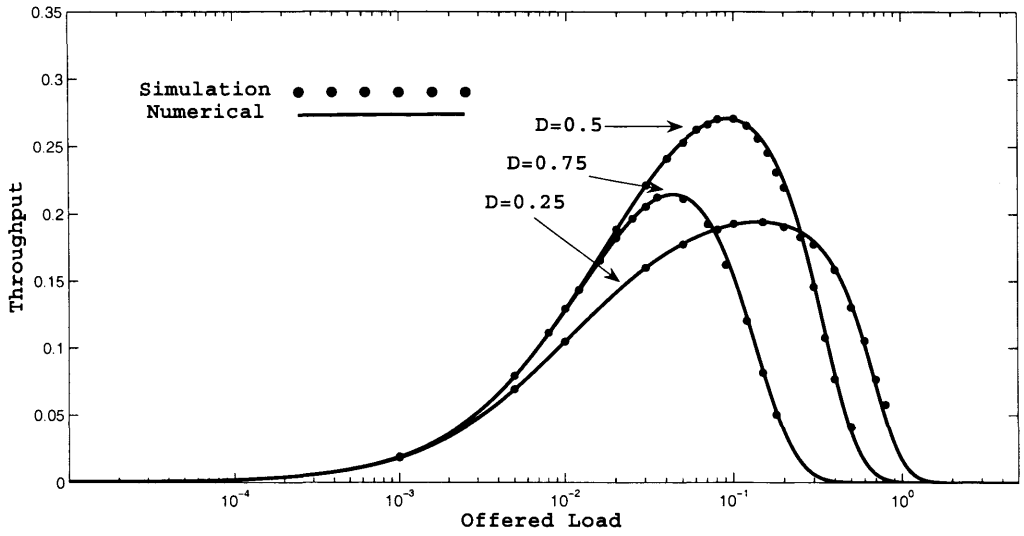

Figure 5.5: Throughput DSMA-D, $\gamma = 3$, $\delta = 20$, $D = 0.25, 0.5, 0.75$, All-Hidden-Sender Environment.

with the data channel bandwidth occupation ratio (D) as the parameter in the all-hidden-sender environment. Packet sizes of RTS and DATA are fixed to 3 and 20 time slots transmission times, respectively. With DSMA-D, the RTS and DATA transmission time are closely related to the channel separation ratio which are 3/(1-D) and 20/D, respectively. The analytical results shown in solid lines, plotted according to equation (5.10), are perfectly verified by the simulation results given in marks. If less bandwidth is spent on DATA transmission, RTS can be transmitted within shorter duration which reduces the vulnerable time of access procedure. In Fig. 5.5, the D=0.25 curve shows this kind of channel separation scenario which makes system more tolerable on heavier offered load. Unfortunately, at the same time, the control channel keeps idle during the long term DATA transmission period. It greatly reduces the wireless spectrum utilization ratio and is not attractive in real applica-

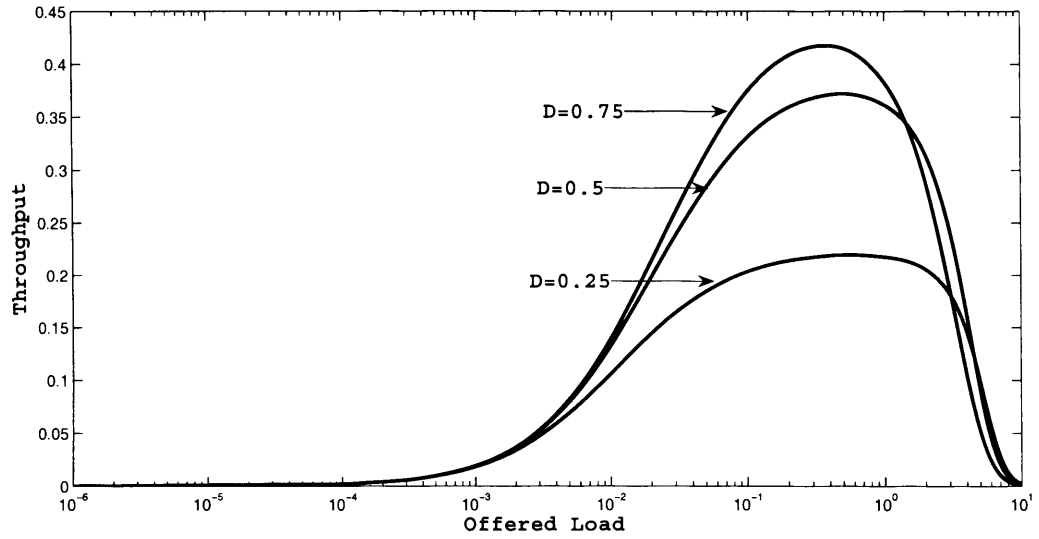

Figure 5.6: Throughput DSMA-D, $\gamma = 3$, $\delta = 20$, $D = 0.25, 0.5, 0.75$, Non-Hidden-Sender Environment.

tions. On the other hand, if large bandwidth is spent on data channel, e.g. D=0.75, RTS packet have to be transmitted for a long period. This severely increases the vulnerable time of RTS transmission and affects the successful probability of it. Thus the channel throughput performance is severely degraded. If similar bandwidth is spent on control and data channels, RTS successful probability and data transmission time are balanced. Better channel throughput is obtained as illustrated by the D=0.5 curve in Fig. 5.5. Therefore in real applications, by carefully set the channel separation ratio, system can be adjusted to satisfy different requirements.

Fig. 5.6 illustrates the numerical results of DSMA-D throughput in the non-hidden-sender environment calculated according to equation (5.17). The major difference with the throughput in the all-hidden sender environment is that the channel division case of D=0.75 has the best throughput perfor-

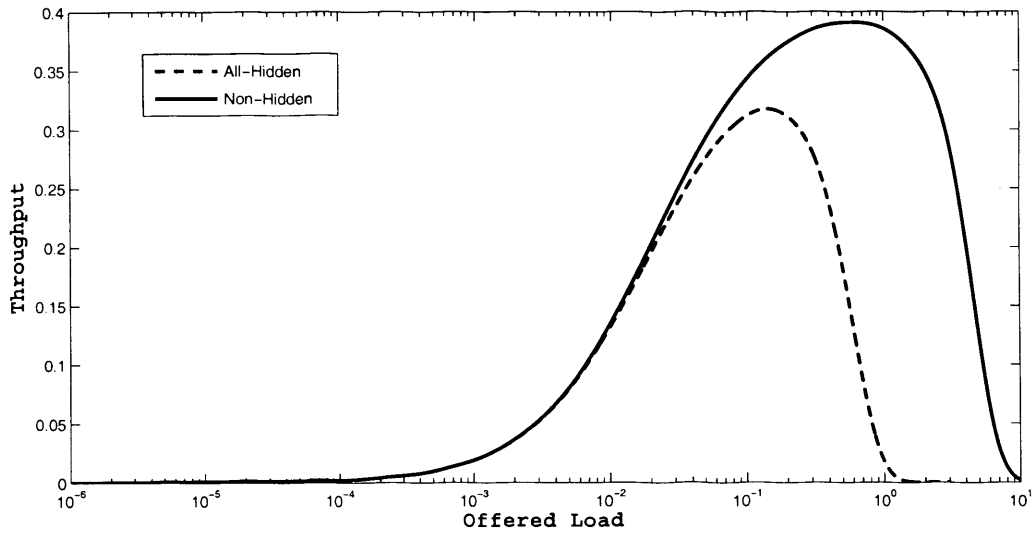

Figure 5.7: Throughput DSMA-D, $D = 0.5$, $\gamma = 2$, $\delta = 20$, All-hidden and Non-hidden Sender Environments.

mance. This is because in the non-hidden-sender environment, the BT_t signal that broadcasted by the RTS sender can be successfully sensed by all contending senders. As a result, the vulnerable period of the RTS transmission reduces to only one time slot in any kinds of channel division cases. If more channel resource is provided to the data transmission, e.g. D=0.75, better channel utilization and system throughput can be achieved.

Fig. 5.7 compares the throughput performance of DSMA-D in all-hidden-sender and non-hidden-sender environments. The all-hidden-sender environment essentially describes the worst network scenario in real applications while the non-hidden-sender environment is the idea scenario. The DSMA-D performs quite different in these two environments because the BT_t signal is broadcasted by RTS senders: in the non-hidden-sender environment, BT_t is able to reach all contending terminals while in the all-hidden-sender envi-

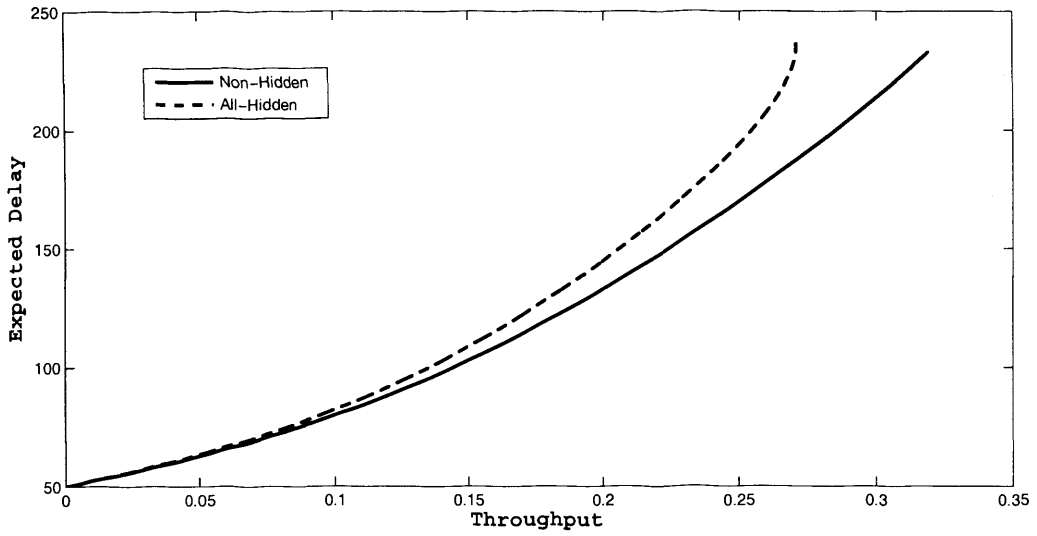

Figure 5.8: Delay DSMA-D, $D = 0.5$, $\gamma = 3$, $\delta = 20$, r_{max}=5, $E[W] = 50$, All-Hidden and Non-Hidden Sender Environments.

ronment, BT_t from any terminal can not be sensed by one another. The two curves in Fig. 5.7 (plotted according to equation (5.10) and (5.17)) indicate the throughput upper bound and lower bound of DSMA-D. Similarly, the Fig. 5.8 (plotted according to equation (5.46) and (5.47)) and 5.9 (plotted according to equation (5.38) and (5.39)) illustrate the boundaries of Delay and blocking probability performance, respectively. In real applications, the throughput, delay and blocking probability performance will locate at the area between the solid line and dashed line.

Fig. 5.10 and Fig. 5.11, both plotted according to equation (5.10), show the channel throughput versus the offered traffic G of DSMA-D in the all-hidden-sender environment with RTS and DATA packet sizes (γ and δ) as parameters, respectively; while Fig. 5.12 and Fig. 5.13, calculated according to equation (5.17), show the throughput performance in the non-hidden-sender environ-

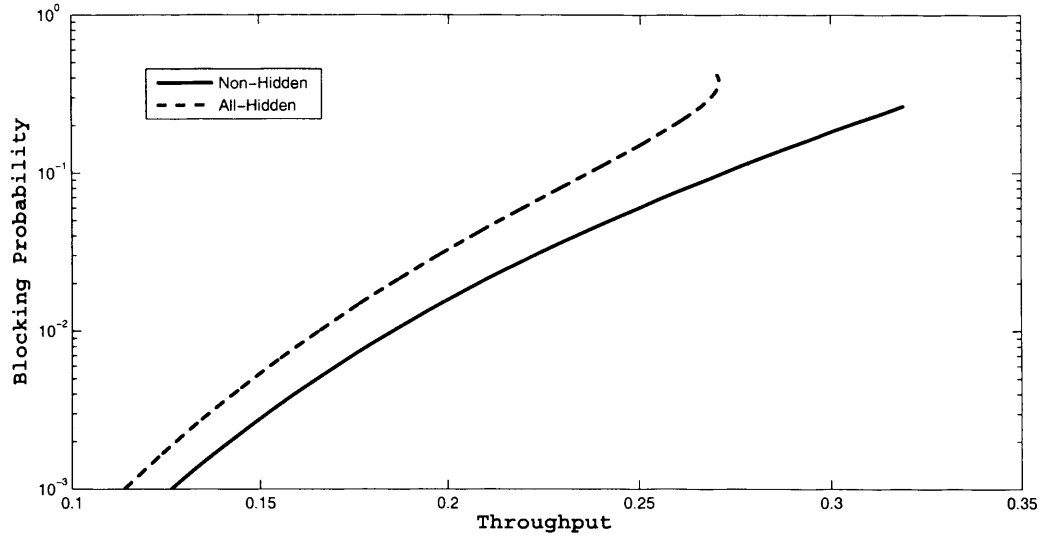

Figure 5.9: Blocking Probability DSMA-D, $D = 0.5$, $\gamma = 3$, $\delta = 20$, r_{max}=5, $E[W] = 50$, All-Hidden and Non-Hidden Sender Environments.

ment. The analytical results shown in solid lines are perfectly verified by the simulation results shown in marks. As expected, the throughput performance is closely related to the ratio between γ and δ. Generally speaking, a larger throughput can be obtained with a larger ratio of δ/γ. However, transmitting very long data packets may not be appropriate in many cases, especially when the radio channel condition is not stable enough. Obviously, using effective access control protocol to transfer small data packet (comparable with the size of RTS) is not attractive at all. Therefore, the obtained curves in the two figures are very useful for traffic sizing in real applications, wherein the tradeoff relationship between the throughput, packet size, power consumption, and radio channel condition should be considered.

Fig. 5.14 and Fig. 5.15, plotted according to equation (5.46) and (5.38) respectively, illustrate the expected (average) access delay and blocking prob-

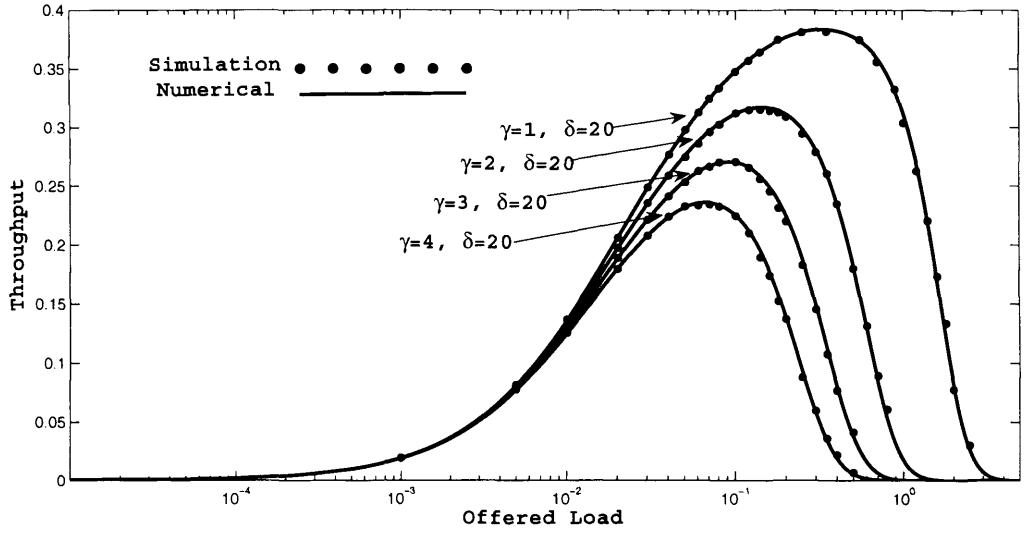

Figure 5.10: Throughput DSMA-D, $D = 0.5$, $\gamma = 1, 2, 3, 4$, $\delta = 20$, All-Hidden-Sender Environment.

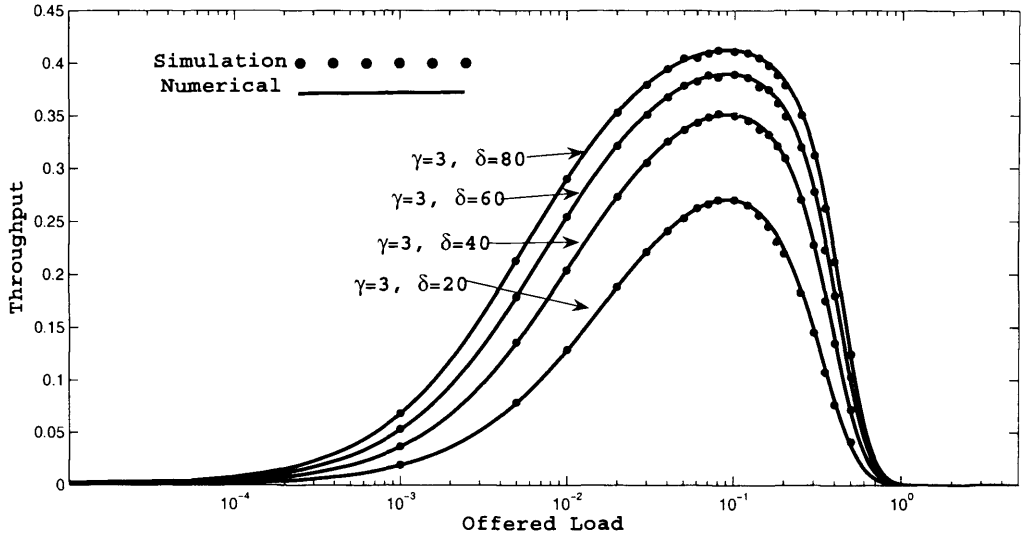

Figure 5.11: Throughput DSMA-D, $D = 0.5$, $\gamma = 3$, $\delta = 20, 40, 60, 80$, All-Hidden-Sender Environment.

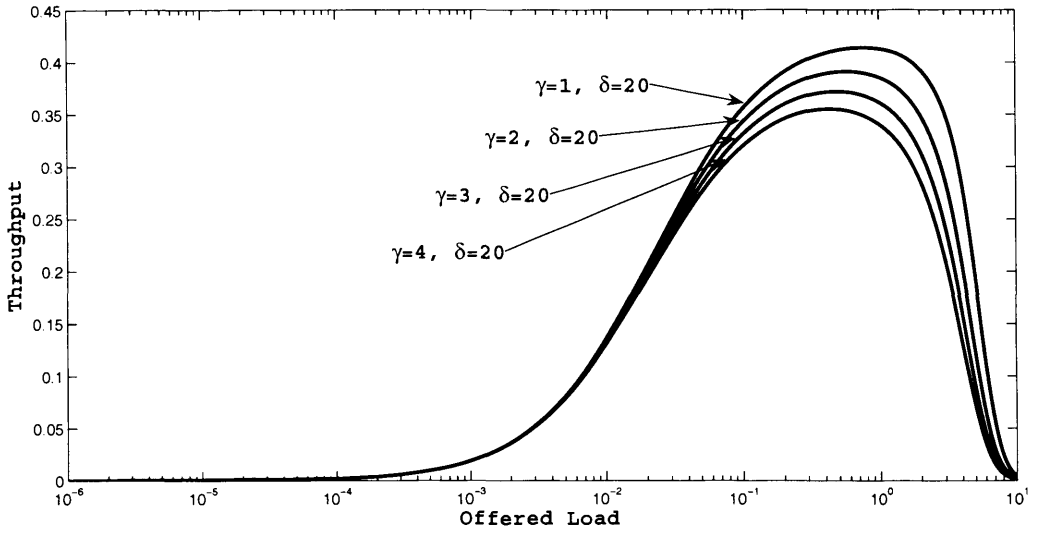

Figure 5.12: Throughput DSMA-D, $D = 0.5$, $\gamma = 1, 2, 3, 4$, $\delta = 20$, Non-Hidden-Sender Environment.

ability performance with maximum retransmission r_{max} as a parameter in the all-hidden-sender environment. While Fig. 5.16 and Fig. 5.17, plotted according to equation (5.47) and (5.39) respectively, illustrate the expected (average) access delay and blocking probability performance in the non-hidden-sender environment. It is shown that larger value of r_{max} is related to longer access delay and smaller blocking probability. This indicates the tradeoffs between system access delay performance and blocking probability. If the transmission attempts are keen to be transmitted, larger value of r_{max} has to be set. The system average access delay increases at the same time, unavoidably. On the other hand, if the system expected delay is the key feature, better performance could be achieved by decreasing the maximum retransmission limitation r_{max}. As a result, transmission attempts are more likely to be discarded (blocked) after a number of failure transmissions.

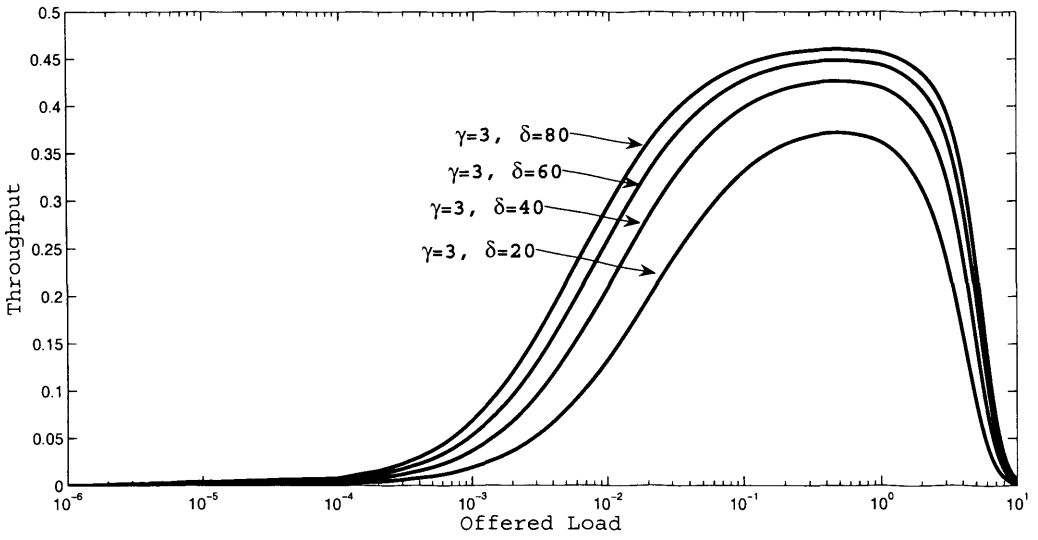

Figure 5.13: Throughput DSMA-D, $D = 0.5$, $\gamma = 3$, $\delta = 20, 40, 60, 80$, Non-Hidden-Sender Environment.

5.2 Double Sense Multiple Access – Single Channel (DSMA-S)

As introduced in the Chapter 4, mesh clients spend their energy on packet (re)transmitting and receiving during a communication process. When packet collision happens, a large amount of energy is wasted on packet transmission, retransmission and receiving on both sides of senders and receivers. As the major energy waster, packet collision is expected to be avoided or alleviated by several random access protocols. However, collision among control packets is quite difficult to be avoided since control packets are transmitted to reserve the channel without guarantee of success. The throughput analysis of DSMA-D illustrates that frequent collision among control packet will induce a very large duration of collision period. System throughput is severely degraded, especially when traffic is heavy. DSMA-S utilizes the "double sense"

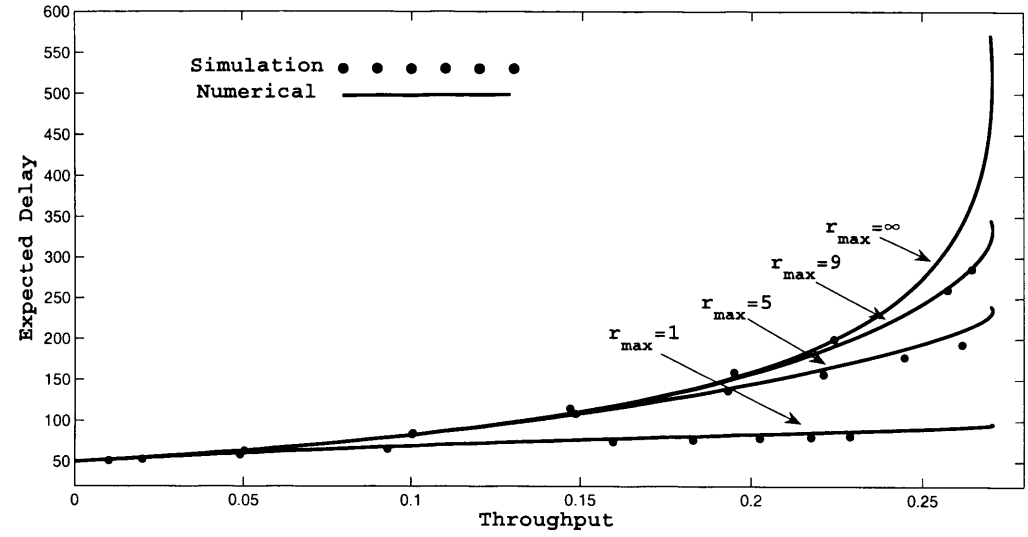

Figure 5.14: Delay DSMA-D, $D = 0.5$, $\gamma = 3$, $\delta = 20$, $E[W] = 50$, All-Hidden-Sender Environment.

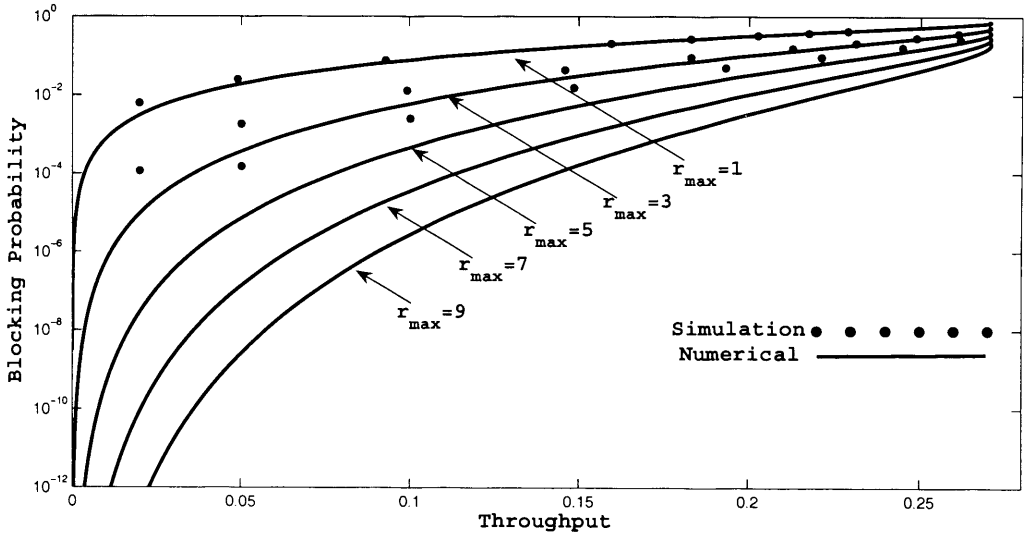

Figure 5.15: Blocking Probability DSMA-D, $D = 0.5$, $\gamma = 3$, $\delta = 20$, $E[W] = 50$, All-Hidden-Sender Environment.

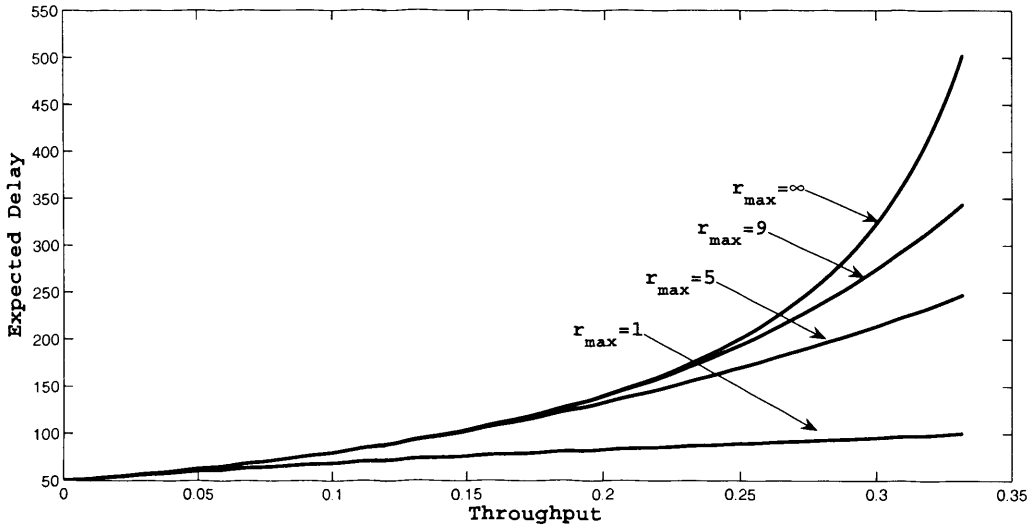

Figure 5.16: Delay DSMA-D, $D = 0.5$, $\gamma = 3$, $\delta = 20$, $E[W] = 50$, All-Hidden-Sender Environment.

mechanism along with a novel "mandatory waiting" mechanism to avoid RTS-DATA collision and proposes a "mandatory clearance" mechanism to resolve the RTS-RTS collision problem and alleviate the harm caused by RTS-RTS collision. This mechanism makes contending terminals aware of a packet collision situation, stopping transmitting additional packets that destine to fail and increasing the collision period length. As a result, both senders and receivers are rescued from the collision state and the energy waste because of packet collision is greatly reduced.

5.2.1 Access Mechanism of DSMA-S

The DSMA-S protocol uses two out-of-band busy tone signals BT_c and BT_r signal at the receiver side only. Thus, both of the two signals can be efficiently sensed by all contending senders. BT_c indicates a packet collision among RTS packets while the BT_r signal indicates a successful RTS transmission. In order

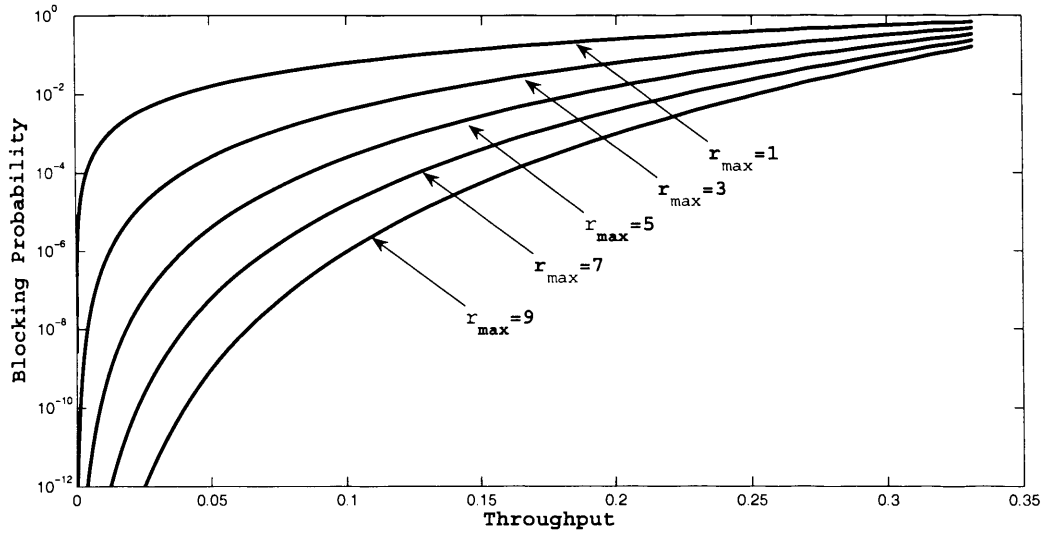

Figure 5.17: Blocking Probability DSMA-D, $D = 0.5$, $\gamma = 3$, $\delta = 20$, $E[W] = 50$, All-Hidden-Sender Environment.

to maximize the channel utilization ratio, both control and data packets are transmitted on a shared wireless channel. With "double sense" mechanism, DSMA-S can inherently eliminate DATA-DATA collisions. In addition, there is a "mandatory waiting" mechanism (collision avoidance) at the sender side to protect transmissions against RTS-DATA collisions and a "mandatory channel clearance" mechanism (collision resolution) at the receiver side to alleviate damages from RTS-RTS collisions. This single channel collision avoidance and collision resolution mechanisms can greatly improve channel efficiency, system throughput and access delay performance. The detailed access mechanism of DSMA-S is analyzed step-by-step as follows. Note that the busy tone signals, BT_C and BT_T , are broadcasted by the common receiver. Thus, busy tone signals can be sensed by every sender regardless it is a hidden terminal or not. As a result, the DSMA-S protocol performs the same in both

all-hidden-sender and non-hidden-sender environments.

The DSMA-S algorithm is summarized in Table 5.2. The transmitter sends out a RTS packet (step 3.1) and then senses BT_r signal twice (step 3.2) before making the decision (step 3.3) whether or not to send out its DATA packet. A "mandatory waiting" (step 3.3.1) is carried out before transmitting the DATA to consume other contending RTS packets initialized during the round-trip propagation period, so as to avoid RTS-DATA collisions. The receiver keep listening incoming control packets for only one RTS transmission period (step 4). Then it tries to unpack the information received and setup busy tone signals accordingly. Successful RTS resolving indicates a collision free control packet transmission. Then BT_r is setup to inform the sender to transmit DATA (step 5). On the other hand, if no intact control packet that can be resolved, it indicates a RTS-RTS collision occurs. BT_c is setup for a certain period of time to cancel other outgoing RTS transmissions (step 6), so as to avoid continuous RTS-RTS collision. Thus, the DSMA-S protocol can effectively prevent hidden terminals from generating contending RTS during DATA transmission and minimize the RTS-RTS collision period.

As an example, Fig. 5.18 shows the access mechanism of DSMA-S for one receiver client **R** and seven transmitters, namely clients **A** to **G**. Under the symmetric radio channel condition, the $BT_r(BT_c)$ signal from the common packet receiver client **R** can be sensed by all the seven transmitters during a period of time, which is denoted by "$BT_r(BT_c)$ Period" in the figure. There is one-slot propagation delay between "$BT_r(BT_c)$ ON" and the beginning of a "$BT_r(BT_c)$ Period", and between "$BT_r(BT_c)$ OFF" and the end of a "$BT_r(BT_c)$ Period". In Fig. 5.18, a transmission attempt request arrives at client **A** within the third time slot. Since neither BT_c nor BT_r signal is sensed at the begin-

Table 5.2: Access Mechanism of DSMA-S

DSMA-S Algorithm

Sender Side:

INPUT: a data packet and the receiver's identity.

OUTPUT: a transmission attempt is failed or successful.

1. Check the status of BT_c and BT_r signals at the beginning of next time slot.

2. IF either BT_c or BT_r signal is sensed, i.e. $BT_c = 1$ or $BT_r = 1$, THEN return failed.

3. ELSE do the following: (Both BT_c and BT_r signals are not sensed, i.e. $BT_c = 0$ and $BT_r = 0$.)

3.1 Send a RTS packet (including the receiver's identity).

3.2 Check the status of BT_r signal at the beginning of next slot. Two time slots later, check it again. (The "double sense" mechanism.)

3.3 IF the BT_r signal is not sensed for the first time and sensed for the second time, i.e. "$BT_r^1 = 0$" and "$BT_r^2 = 1$", THEN do the following:

3.3.1 "Mandatory waiting" and then Send the data packet (including the receiver's identity).

3.3.2 Return successful.

3.4 ELSE return failed.

Receiver Side:

INPUT: a RTS packet.

OUTPUT: a RTS transmission is successful or failed.

4. Unpack RTS packet(s) received after one RTS transmission time (i.e. receive RTS packet for γ slots).

5. IF the RTS is able to be unpacked, setup BT_r signal; THEN return successful.

6. ELSE setup BT_c signal, THEN return failed. ("Mandatory clearance")

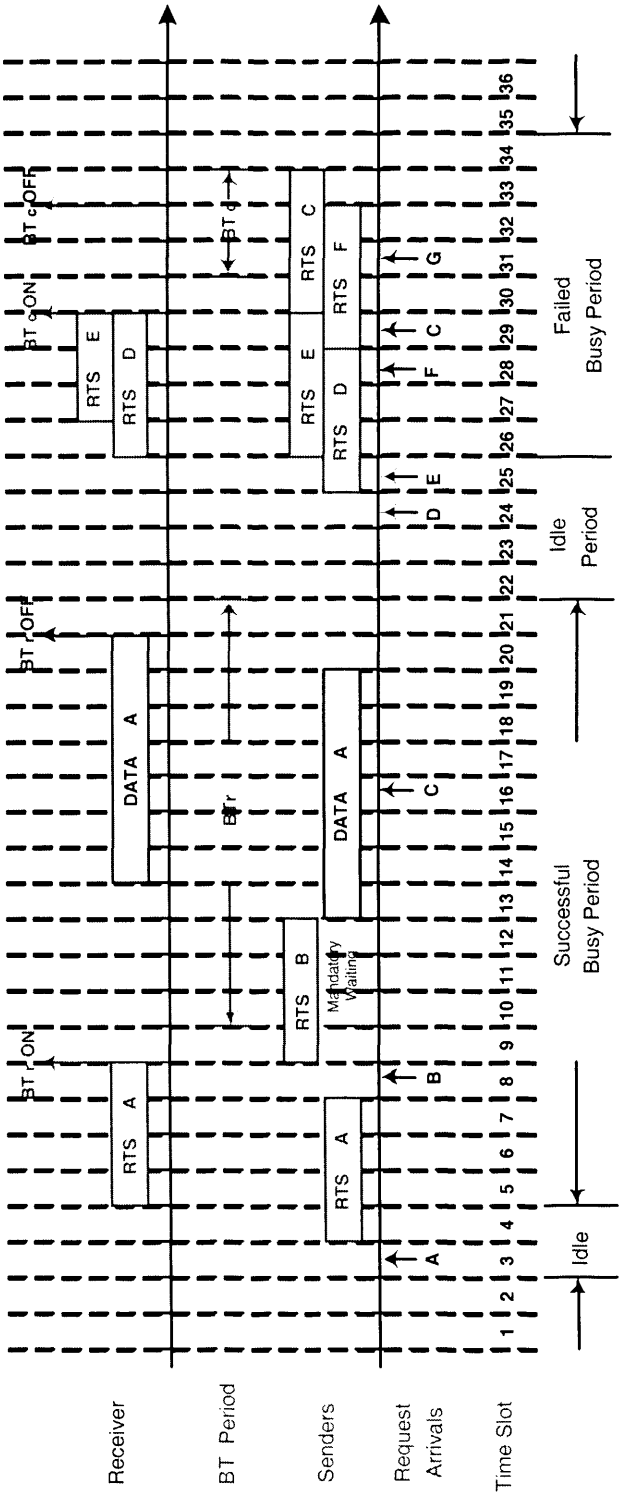

Figure 5.18: Access Mechanism of DSMA-S

ning of the fourth slot, **A** sends out a RTS packet, denoted by RTS-A. After one slot propagation delay, RTS-A arrives at the receiver client **R**. As soon as one RTS transmission finishes at the end of eighth slot, client **R** unpacks control packet(s) received and turns on its BT_r signal at the beginning of the ninth slot as an acknowledgement. One-slot later, this BT_r signal can definitely be sensed by **R**'s neighboring clients (including the seven transmitters). Client **A** completes the transmission of RTS-A by the end of the seventh slot, it senses BT_r signal twice at the beginnings of the ninth and 11^{th} slots. The corresponding sensing results are "$BT_r^1 = 0$" and "$BT_r^2 = 1$". Then client **A** knows that RTS-A has been correctly received by **R** and the subsequent channel has been reserved for its DATA packet transmission (collision-free). Then client **A** enters the "mandatory waiting" state until the end of 12^{th} slot to consume other contending RTS transmissions initialized within the seventh and eighth slots (RTS-B). Client **B** sends its RTS packet at the beginning of ninth slot and will not transmit its DATA packets because its double sensing results are "$BT_r^1 = 1$", "$BT_r^2 = 1$". Clients **C(G)** cannot even send out RTS packet when they sense the BT_r (BT_c) signal before transmitting the attempt. Simultaneous RTS transmissions results in a packet collision at the receiver **R** and those overlapped RTS packets are all destroyed. The four involved transmitters **D**, **E**, **F** and **C** will then obtain the same BT_r double sensing result, i.e. "$BT_r^1 = 0$", "$BT_r^2 = 0$". Note that client **R** keeps listening on incoming packets for only one RTS transmission time then tries to unpack at the end of 29^{th} slot. The RTS-E is spitted and missed the final slot on client **R**. Thus the overlapped transmissions of the RTS-D and part of RTS-E will be destroyed and none of them can be successfully received by client **R**. As a result, BT_c turns on at the beginning of 30^{th} time slot to inform the collision status on client **R** and

mandatory cancel other outgoing contending RTS. In the above three cases (case 1 client **B**, case 2 client **C** and **G**, case 3 client **D**, **E**, **F** and **C**), the transmission/retransmission attempts are failed and the corresponding terminals need to access the channel again after a random backoff delay, e.g. client **C** reschedule their first retransmission attempts at the 29^{th} slot, but fail again. As illustrated in these examples, with the "mandatory waiting" mechanism, the "double sense" mechanism can also provide collision free DATA transmission, i.e. no DATA-RTS and DATA-DATA collisions, on the single wireless channel. Unfortunately, RTS packets are sent out without guarantees of success in order to reserve the wireless channel for subsequent DATA transmission and RTS-RTS collisions still exist. The "mandatory channel clearance" mechanism provides a collision resolution solution to minimize the RTS-RTS collision length. Throughput and access delay are therefore greatly improved.

5.2.2 Throughput, Delay and Blocking Probability Analysis of DSMA-S

The general performance attributes such as throughput, delay and blocking probability of DSMA-S are analyzed according to the mathematic model constructed for analyzing DSMA-D. We utilize the same analysis method and obtain the throughput, delay and blocking probability performance results as follows.

5.2.2.1 Throughput

In DSMA-S, a RTS packet is transmitted via the entire wireless channel without any protection from busy tone signals. Therefore, the success probability of a packet transmission attempt p_s is

$$p_s^{DSMA-S} = \frac{\lambda\tau \cdot e^{-\gamma\lambda\tau}}{1 - e^{-\lambda\tau}}. \tag{5.48}$$

The average length of an idle period is the same with that of DSMA-D, i.e.

$$E[I]^{DSMA-S} = E[I]^{DSMA-D} = \frac{e^{-\lambda\tau} \cdot \tau}{1 - e^{-\lambda\tau}}. \tag{5.49}$$

The length of a successful busy period is fixed and equal to the summation of the transmission times of a RTS and DATA packet, a mandatory waiting time and two round-trip propagation delay for turning on and off the BT_r signal, i.e.

$$B_s^{DSMA-S} = (2 \cdot \gamma + \delta + 3) \cdot \tau. \tag{5.50}$$

The average channel utilization is simply given by:

$$E[U]^{DSMA-S} = \delta\tau \cdot p_s^{DSMA-S}. \tag{5.51}$$

As the receiver can discover a packet collision immediately when it happens, the length of a fail busy period is fixed and contains the transmission time of a RTS packet, mandatory channel clearance time (BT_c duration) and a round-trip propagation delay of BT_c signal, i.e.

$$B_f^{DSMA-S} = (2 \cdot \gamma + 1) \cdot \tau. \tag{5.52}$$

By substituting (5.48), (5.49), (5.50), (5.51) and (5.52) into (5.1), the system throughput is obtained as:

$$\begin{aligned} S^{DSMA-S} &= \frac{\lambda\tau \cdot \delta e^{-\lambda\tau\gamma}}{(\delta + 2) \cdot \lambda\tau \cdot e^{-\lambda\tau\gamma} + 2\gamma \cdot (1 - e^{\lambda\tau}) + 1}, \\ &= \frac{\delta \cdot G \cdot e^{-G\gamma}}{(\delta + 2) \cdot G \cdot e^{-G\gamma} + 2\gamma \cdot (1 - e^{-G}) + 1}. \end{aligned} \tag{5.53}$$

where $G \triangleq \lambda\tau$ is referred to as "offered traffic".

5.2.2.2 Access Delay and Blocking Probability

According to DSMA-S algorithm, a transmitter needs to check the status of both BT_c and BT_r signals before sending out its RTS packet. It then relies

on the "double sense" result of BT_r to make decision of data transmission or backoff.

CASE I: NO RTS PACKET IS TRANSMITTED.

Within one transmission cycle, the average lengths of BT_r and BT_c periods are $(\delta+\gamma+1)\tau \cdot p_s^{DSMA-S}$ and $(\gamma-1)\tau \cdot (1-p_s^{DSMA-S})$, respectively. Therefore, the probabilities that the BT_r and BT_c signals are sensed (hence no RTS packet is transmitted) are given by:

$$\begin{aligned} p_{11} &= \frac{(\delta+\gamma+1)\tau \cdot p_s^{DSMA-S}}{E[I]^{DSMA-S} + E[B]^{DSMA-S}}, \\ &= \frac{(\delta+\gamma+1) \cdot G \cdot e^{(-\gamma G)}}{(\delta+2) \cdot G \cdot e^{-2G} + 2\gamma \cdot (1-e^{-G}) + 1} \end{aligned} \tag{5.54}$$

$$\begin{aligned} p_{12} &= \frac{(\gamma-1)\tau \cdot (1-p_s^{DSMA-S})}{E[I]^{DSMA-S} + E[B]^{DSMA-S}}, \\ &= \frac{(\gamma-1) \cdot G \cdot (1-e^{(-G)} - e^{(-\gamma G)})}{(\delta+2) \cdot G \cdot e^{-2G} + 2\gamma \cdot (1-e^{-G}) + 1}, \end{aligned} \tag{5.55}$$

respectively.

For this case, in order to avoid sensing the same BT_r and BT_c signals again, the corresponding backoff delays D_{11} and D_{12} before the next retransmission attempt should be set longer than $(\delta+\gamma)$ and $(\gamma-2)$ time slots, respectively. We let:

$$D_{11} = (W+\delta+\gamma) \cdot \tau . \tag{5.56}$$

$$D_{12} = (W+\gamma-2) \cdot \tau . \tag{5.57}$$

CASE II: $BT_r^1 = 1$ AND $BT_r^2 = 1$.

In the remaining three cases, "double sense" mechanism will then be used to determine whether or not a DATA transmission should follow. Within the round-trip propagation time of RTS and BT_r, a contending RTS can be transmitted collision free but it will fail because of the "double sense" results are

"$BT_r^1 = 1$" and "$BT_r^2 = 1$", e.g. client **B** in Fig. 5.18. The corresponding probability is given by:

$$\begin{aligned} p_2 &= \frac{2\tau \cdot p_s^{DSMA-S}}{E[I]^{DSMA-S} + E[B]^{DSMA-S}}, \\ &= \frac{2G \cdot e^{(-G)}}{(\delta+2) \cdot G \cdot e^{-\gamma G} + 2\gamma \cdot (1 - e^{-G}) + 1}. \end{aligned} \tag{5.58}$$

Retransmission are scheduled to avoid occurring within the same BT_r period. The corresponding backoff delay D_2 is set as:

$$D_2 = (W + \delta + \gamma + 2) \cdot \tau. \tag{5.59}$$

CASE III: $BT_r^1 = 0$ AND $BT_r^2 = 1$.

This is the successful case for RTS and DATA transmissions. The average length $E[I_s]^{DSMA-S}$ of the idle period that guarantees a successful RTS (and DATA) packet transmission equals to that of DSMA-D

$$E[I_s]^{DSMA-S} = E[I_s]^{DSMA-D} = \frac{e^{-\gamma G} \cdot \tau}{1 - e^{-G}}. \tag{5.60}$$

The probability that the double sensing results are "$BT_r^1 = 0$" and "$BT_r^2 = 1$" is simply:

$$\begin{aligned} p_{suc}^{DSMA-S} &= \frac{E[I_s]^{DSMA-S}}{E[I]^{DSMA-S} + E[B]^{DSMA-S}}, \\ &= \frac{e^{(-G)}}{(\delta+2) \cdot G \cdot e^{-\gamma G} + 2\gamma \cdot (1 - e^{-G}) + 1}. \end{aligned} \tag{5.61}$$

The corresponding delay D_3 equals to the summation of the transmission time of RTS packet, DATA packet, a mandatory waiting time, and a two-slot round-trip propagation delay, i.e.

$$D_3 = (\delta + 2 \cdot \gamma + 1) \cdot \tau. \tag{5.62}$$

CASE IV: $BT_r^1 = 0$ AND $BT_r^2 = 0$.

In this last case, packet collision occurs among RTS packets. All the involved (overlapped) RTS packets are destroyed (cannot be correctly received by the receiver) and should be retransmitted. The BT_c signal is setup to announce this situation and to perform a mandatory channel clear so as to prevent continuous collision. The probability of this case can be simply calculated as

$$p_4 = 1 - p_{11} - p_{12} - p_2 - p_{suc}^{DSMA-S} . \tag{5.63}$$

To avoid a repeated overlap with the same collision period, the corresponding access delay D_4 is set as:

$$D_4 = (W + 2 \cdot \gamma + 1) \cdot \tau . \tag{5.64}$$

Average Access Delay and Blocking Probability

There are five cases of access delay D_{11}, D_{12}, D_2, D_3 and D_4 with corresponding probabilities p_{11}, p_{12}, p_2, p_{suc}^{DSMA-S} and p_4. Let R denote the total number of retransmissions needed before a successful RTS/DATA packet transmission. Conditioning on $R \leq r_{max}$, the retransmission distribution of those successful data packets is given by

$$P\{R = r \mid R \leq r_{max}\} = \frac{p_{suc}^{DSMA-D}(1 - p_{suc}^{DSMA-D})^r}{1 - (1 - p_{suc}^{DSMA-D})^{r_{max}+1}}, \quad r = 0, 1, 2, \ldots, r_{max}. \tag{5.65}$$

And the blocking probability P_B is defined as

$$P_B^{DSMA-S} = P\{R > r_{max}\} = (1 - p_{suc}^{DSMA-S})^{r_{max}+1} . \tag{5.66}$$

The mean value of R is given by:

$$E[R]^{DSMA-S} = \frac{(1 - p_{suc}^{DSMA-S}) - (p_{suc}^{DSMA-S} r_{max} + 1)(1 - p_{suc}^{DSMA-S})^{r_{max}+1}}{\left[1 - (1 - p_{suc}^{DSMA-S})^{r_{max}+1}\right] \cdot p_{suc}^{DSMA-S}} . \tag{5.67}$$

We let L and M denote the numbers of failed transmission attempts due to sensing the BT_r and BT_c signals in Cases I. And N denotes the number of

failed transmissions due to the Cases II, wherein $0 \leq L+M+N \leq R$. The joint distribution of R, L, M and N is given by

$$P\{R=r, L=l, M=m, N=n\} = \binom{r}{l}\binom{r-l}{m}\binom{r-l-m}{n} \cdot p_{suc}^{DSMA-S}\, p_{11}^{l}\, p_{12}^{m}\, p_{2}^{n}\, p_{4}^{r-n-m}. \tag{5.68}$$

Similarly, the mean values of L, M and N are derived as [23]:

$$E[L]^{DSMA-S} = \frac{\left(\frac{p_{11}}{p_{11}+p_{suc}^{DSMA-S}}\right) - \left(\frac{p_{suc}^{DSMA-S} r_{max}}{p_{11}+p_{suc}^{DSMA-S}}+1\right)\cdot\left(\frac{p_{11}}{p_{11}+p_{suc}^{DSMA-S}}\right)^{r_{max}+1}}{\left[1-\left(\frac{p_{11}}{p_{11}+p_{suc}^{DSMA-S}}\right)^{r_{max}+1}\right]\cdot\frac{p_{suc}^{DSMA-S}}{p_{11}+p_{suc}^{DSMA-S}}}, \tag{5.69}$$

$$E[M]^{DSMA-S} = \frac{\left(\frac{p_{12}}{p_{12}+p_{suc}^{DSMA-S}}\right) - \left(\frac{p_{suc}^{DSMA-S} r_{max}}{p_{12}+p_{suc}^{DSMA-S}}+1\right)\cdot\left(\frac{p_{12}}{p_{12}+p_{suc}^{DSMA-S}}\right)^{r_{max}+1}}{\left[1-\left(\frac{p_{12}}{p_{12}+p_{suc}^{DSMA-S}}\right)^{r_{max}+1}\right]\cdot\frac{p_{suc}^{DSMA-S}}{p_{12}+p_{suc}^{DSMA-S}}}, \tag{5.70}$$

and

$$E[N]^{DSMA-S} = \frac{\left(\frac{p_{2}}{p_{2}+p_{suc}^{DSMA-S}}\right) - \left(\frac{p_{suc}^{DSMA-S} r_{max}}{p_{2}+p_{suc}^{DSMA-S}}+1\right)\cdot\left(\frac{p_{2}}{p_{2}+p_{suc}^{DSMA-S}}\right)^{r_{max}+1}}{\left[1-\left(\frac{p_{2}}{p_{2}+p_{suc}^{DSMA-S}}\right)^{r_{max}+1}\right]\cdot\frac{p_{suc}^{DSMA-S}}{p_{2}+p_{suc}^{DSMA-S}}}. \tag{5.71}$$

Let $D_{11,i}$, $D_{12,j}$, $D_{2,k}$ and $D_{4,o}$ denote the i^{th}, j^{th}, $k^{th}$and o^{th} backoff delay due to the Cases I (p_{11} and p_{11}), II and IV, respectively. The total access delay D is given by

$$\begin{aligned} D &= D_0 + D_3 + \sum_{i=1}^{L} D_{11,i} + \sum_{j=1}^{M} D_{12,j} + \sum_{k=1}^{N} D_{2,k} + \sum_{k=L+M+N+1}^{R} D_{4,o} \\ &= D_0 + (2\gamma+\delta+1)\tau + \tau\cdot\sum_{l=1}^{R} W_l + L(\delta+\gamma)\tau + M(\gamma-2)\tau \\ &\quad + N(\delta+\gamma+2)\tau + (R-L-M-N)(2\gamma'+1)\tau\,. \end{aligned} \tag{5.72}$$

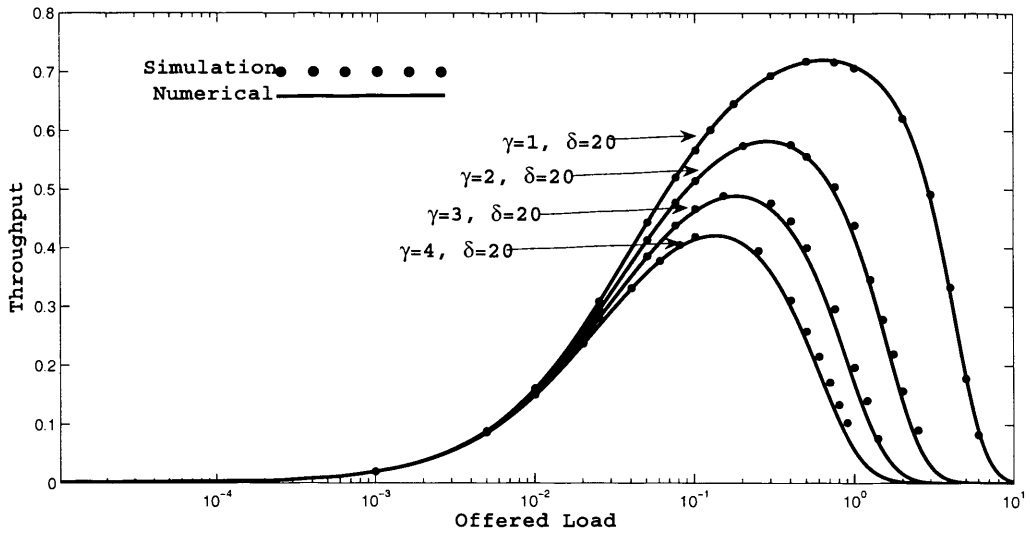

Figure 5.19: Throughput DSMA-S, $\gamma = 1, 2, 3, 4$, $\delta = 20$.

The average of access delay is therefore

$$\begin{aligned} E[D]^{DSMA-S} &= (2\gamma + \delta + 2)\tau + E[W]E[R] \cdot \tau + E[L](\delta + \gamma)\tau \\ &+ E[M]^{DSMA-S}(\gamma - 2)\tau + E[N]^{DSMA-S}(\delta + \gamma + 2)\tau \\ &+ (E[R]^{DSMA-S} - E[L]^{DSMA-S} - E[M]^{DSMA-S} \\ &- E[N]^{DSMA-S})(2\gamma + 1)\tau . \end{aligned} \tag{5.73}$$

5.2.2.3 Analytical/Simulation Results and Discussion

Fig. 5.19 and Fig. 5.20 illustrate the throughput performance of DSMA-S while Fig. 5.21 and Fig. 5.22 illustrate the delay and blocking probability performance. The solid lines in Fig. 5.19 and Fig. 5.20 are calculated according to equation (5.53) and solid lines in Fig. 5.21 and Fig. 5.22 are calculated according to equation (5.73) and (5.66), respectively. DSMA-S simulation also operates on a C++ platform that describes the random access channel of a receiver when a number of transmission attempts try to access this channel. The

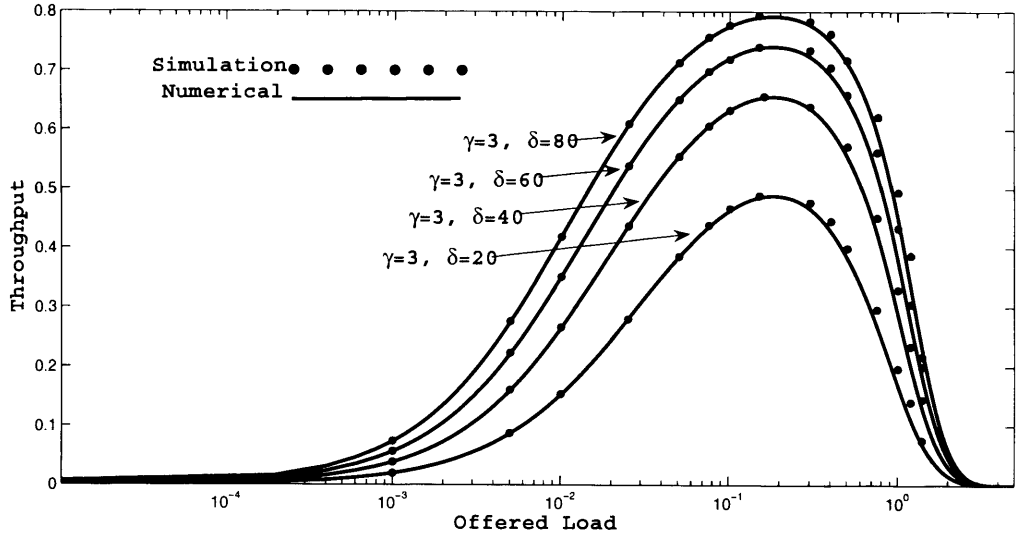

Figure 5.20: Throughput DSMA-S, $\gamma = 3$, $\delta = 20, 40, 60, 80$.

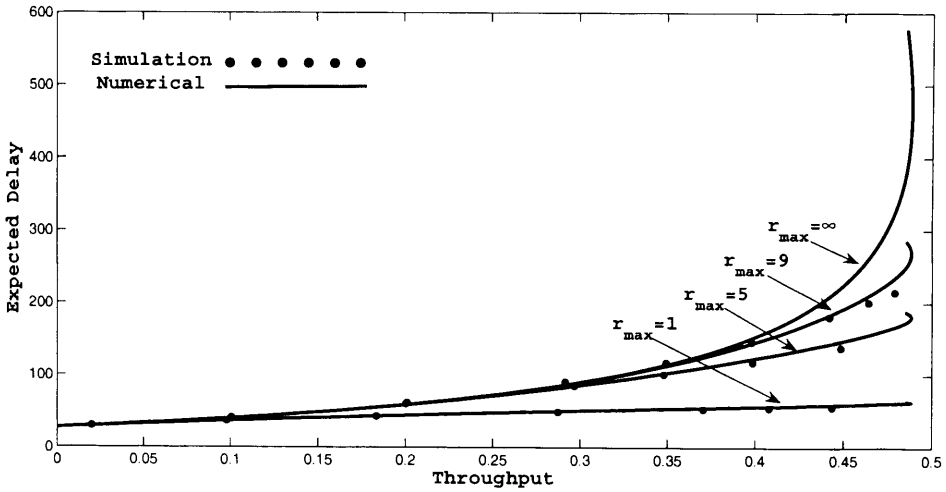

Figure 5.21: Delay DSMA-S, $\gamma = 3$, $\delta = 20$, $E[W] = 50$.

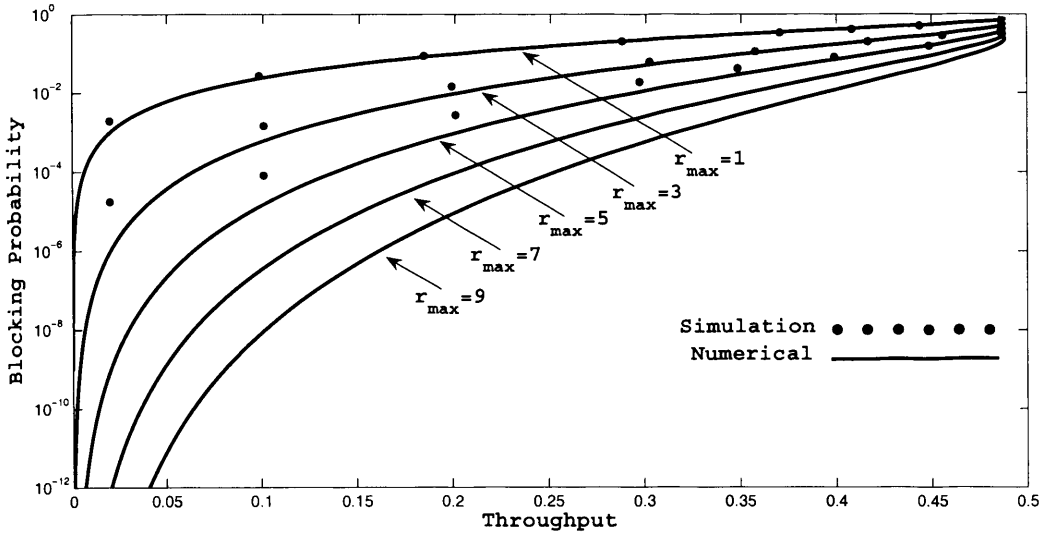

Figure 5.22: Blocking Probability DSMA-S, $\gamma = 3$, $\delta = 20$, $E[W] = 50$.

simulation results are shown in markers in Fig. 5.21, 5.22 and Fig. 5.21(5.22) which are obtained by setting different parameters, i.e. RTS packet length (γ), DATA length (δ) and maximum retransmission times (r_{max}), respectively.

Similarly with DSMA-D, a larger ratio of δ/γ can achieve a better throughput performance illustrated by Fig. 5.19 and Fig. 5.20. In Fig. 5.21 and Fig. 5.22, larger value of r_{max} is able to achieve better blocking probability performance but worse delay performance. The analytical results are illustrated in solid lines while the simulation results in marks. In Fig. 5.22, the simulation results match better with the analytical curve when r_{max} is smaller. This is because for smaller r_{max} and larger E[W] (uniform-distributed random backoff delay W with the mean value E[W], set to 50 in Fig. 5.21 and Fig. 5.22) values, the combined new and retransmitted traffic is less "bursting". Therefore, the arrival correlation of retransmitted packets is greatly reduced and the combined new and retransmitted traffic is more Poisson-like, which results in

a better match between simulation and analytical results for DSMA-S. Similarly, by comparing the Fig. 5.22 and Fig. 5.15, it is found that the simulation marks match with the analytical curves better in DSMA-S than in DSMA-D. In Fig. 5.15, with the same size of RTS and DATA packets, DSMA-D takes 6 and 40 slots to transmit RTS and DATA respectively under the channel separation ratio of D=0.5. The DATA duration of DSMA-D is closer to E[W] than DSMA-S which makes the combined traffic in DSMA-D much less Poisson-like. Thus, simulation results in Fig. 5.15 deviate more from analytical ones than in Fig. 5.22.

5.2.3 Energy Consumption of DSMA-S

As discussed in Chapter 4, energy consumption on each mesh client during a communication process is spent on useful packet sending and receiving, colliding packet sending and receiving as well as terminal idle listening. Among them, energy cost during a packet collision process occupies a large amount of total energy wastage. Existing MAC solutions are usually able to protect the data payload transmissions against collisions. But unfortunately, control packet collisions are very difficult to be completely avoided. How to alleviate the control packet collision problem as far as possible, reduce the cost when packet collision occurs, prevent from severe damage on system performance and rescue both senders and receiver from the collision status become very important topics to be resolved.

DSMA-S is proposed with the target of energy conservation. First of all, slotted time is used which lets every action be performed at the beginning of time slots so as to reduce the idle listening energy consumption. Secondly, each packet receiver switches on its antenna and try to receive contending control packet for only γ slots, which just covers the duration of a control

packet. By doing that, the packet receiver is able to determine a collided control packet transmission after γ slots listening period. Unnecessary listening of subsequent collided control packets is avoided so as to save the energy consumption on the packet receiver side. Thirdly, when control packet collision happens, the receiver will not be able to correctly resolve a control packet after a γ slots' listening. Then, the BT_c signal is setup to let all contending terminals be aware of an ongoing packet collision and cancel their outgoing transmissions. According to this access principle, the system energy consumption distribution is analyzed in details as follows.

Energy Consumption Distribution.

According to the access mechanism of DSMA-S, when RTS is correctly received, collision free DATA transmission is guaranteed. Energy consumption E is defined as the average system energy cost on succeeding a RTS transmission. It includes energy spent on sending and receiving packet, as well as energy spent on broadcasting and sensing busy tone signals. On a per time slot basis, they are denoted by *E_Send*, *E_Rec*, *E_BT_Bro* and *E_BT_Sense*, respectively. Successful or failed RTS transmission will induce different steps of access procedure and consequently different amounts of energy consumption of the system.

CASE I. SUCCESSFUL TRANSMISSION

According to the access mechanism, a RTS packet is sent out if the preamble busy tone sense is free (e.g. In Fig. 5.18, client **A** senses for any busy tone signal at the beginning of 4^{th} slot), and the transmission succeeds if there is no contending RTS arrives within the vulnerable period (i.e. from the beginning of 3^{th} till the end of 6^{th} slot). Therefore, the probability of guaranteeing a successful RTS transmission is:

$$p_1 = p_s = \frac{\lambda\tau \cdot e^{-\gamma\lambda\tau}}{1 - e^{-\lambda\tau}}. \tag{5.74}$$

A succeed RTS transmission involves a pair of RTS-DATA sending and receiving, busy tone sense, double sense and a BT_r broadcasting and sensing process. Thus, the corresponding energy consumption is:

$$\begin{aligned} E_1 = (E\_Send + E\_Rec) \cdot (\gamma + \delta) + E\_BT\_Bro \cdot \\ (\gamma + \delta + 1) + 3 \cdot E\_BT\_Sense. \end{aligned} \tag{5.75}$$

CASE II. FAILED TRANSMISSION

During last slot of the first RTS and the slot immediately after (e.g. 7^{th} and 8^{th} slots in In Fig. 5.18), contending RTSs (e.g. RTS-B) will not interrupt the existing RTS and subsequent DATA transmission because of the "mandatory waiting" mechanism. All contending RTS transmissions are failed because of a "$BT_r^1 = 1$" and "$BT_r^2 = 1$" double sense result. If there are i RTS packets involved in this status, the probabiltiy is given by:

$$p_{2i} = \frac{\beta^i \cdot (\lambda\tau)^{i+1} \cdot e^{-(\gamma+\beta+1)\lambda\tau}}{(1 - e^{-\lambda\tau}) \cdot i!}. \tag{5.76}$$

wherein $\beta(=2\tau)$ indicates 7^{th} and 8^{th} slots in In Fig. 5.18.

Since the receiver stops receiving RTS packets after γ slots' receiving period, energy consumption in this case includes only the energy spent on the senders. Each sender will experience a preamble busy tone sense, RTS transmission and double sense process. Thus, the corresponding energy consumption is:

$$E_2 = (\gamma \cdot E\_Send + 3 \cdot E\_BT\_Sense) \cdot i. \tag{5.77}$$

CASE III. COLLIDED TRANSMISSION

If there are other contending RTS packets transmitted during the vulnerable period (e.g. RTS-D and RTS-E), a packet collision happens and all overlapped RTS packets are failed. Assuming there are j overlapping RTS packets involved in a collision period, the probability is given by:

$$p_{3j} = \frac{(\lambda\tau)^{j+1} \cdot e^{-(\gamma+\beta+1)\lambda\tau}}{(1-e^{-\lambda\tau}) \cdot j!} \cdot ((\gamma+\beta)^j - \beta^j). \tag{5.78}$$

When a packet collision happens, a mesh client spends energy on busy tone sense, RTS sending and double sense at the sender side. While at the receiver side, a RTS period (γ slots) receiving and BT_c broadcasting ($\gamma - 1$ slots) process minimizes the energy spent on receiving damaged packets. The system energy consumption is given by:

$$\begin{aligned} E_3 = {} & (\gamma \cdot E\_Send + 3 \cdot E\_BT\_Sense) \cdot (j+1) + \\ & \gamma \cdot E\_Rec + (\gamma - 1) \cdot E\_BT\_Bro. \end{aligned} \tag{5.79}$$

Average Energy Consumption.

In order to succeed a RTS-DATA transmission, the system may experience RTS failed transmission (collision) and useless transmission (no response). Thus, the average system energy cost is defined as the non-successful RTS transmission energy consumption in succeeding one RTS-DATA procedure, which can be shown as:

$$
\begin{aligned}
E[E] &= (\sum_{i=1}^{\infty} p_{2i} \cdot E_2 + \sum_{j=1}^{\infty} p_{3i} \cdot E_3) \; / p_1 \\
&= \frac{1}{p_1} \cdot (\gamma \cdot E\_Send + 3 \cdot E\_BT\_Sense) \cdot \\
&(\sum_{i=1}^{\infty} i \cdot p_{2i} + \cdot \sum_{j=1}^{\infty} (j+1) \cdot p_{3j}) + \frac{1-p_1}{p_1} \\
&\cdot (\gamma \cdot E\_Rec + (\gamma - 1) \cdot E\_BT\_Bro)
\end{aligned}
\tag{5.80}
$$

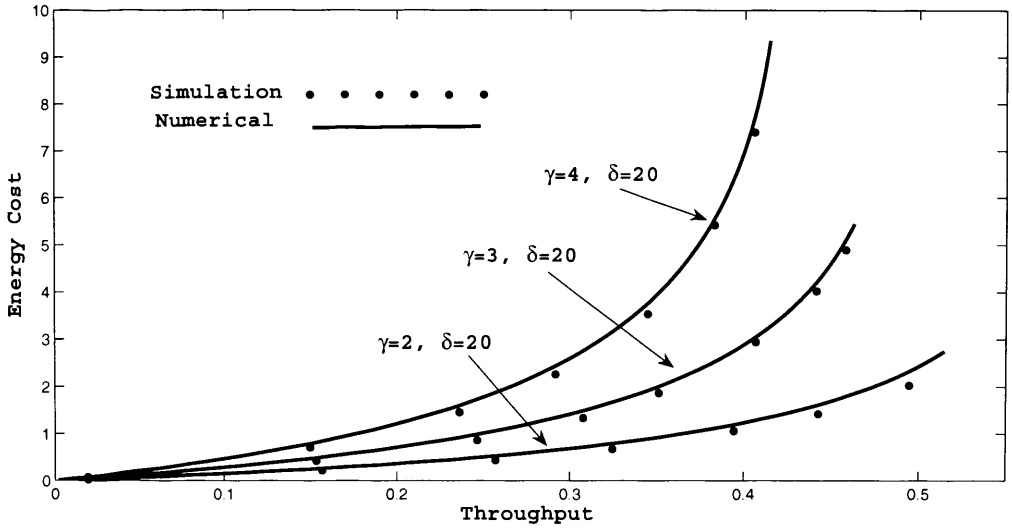

Figure 5.23: Energy Cost DSMA-S, $\gamma = 2, 3, 4$, $\delta = 20$.

Fig. 5.23 illustrates the system energy cost versus channel throughput for DSMA-S with γ and δ as parameters wherein the analytical curves are calculated according to equation (5.80). According to the performance value of Lucent 15dbm 2.4GHz Wavelane PCMCIA card, 1.82W is spent on transmission mode, 1.80W in receiving mode and 0.18W on standby mode. We assume that the energy consumed on sending packets per time slot is the energy unit ($E\_send = 1$). The E_Rec, E_BT_Bro and E_BT_Sense can reasonably be as-

sumed to 1, 0.5 and 0.5, respectively. The results in Fig. 5.23 indicates that the system energy cost is closely related to the δ/γ ratio. Larger δ/γ ratio can achieve better energy conservation to obtain the same system throughput.

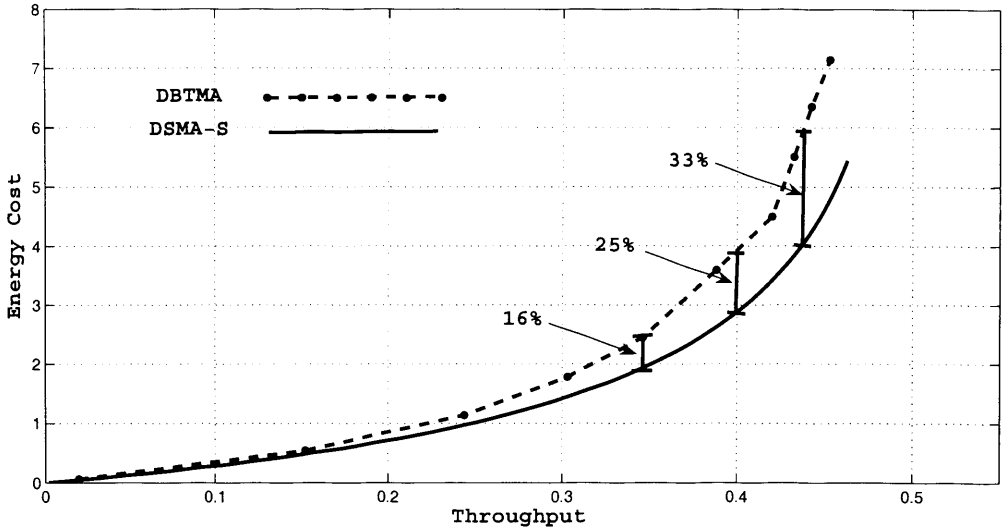

Figure 5.24: Energy Cost Comparison DSMA-S and DBTMA, $\gamma = 3$, $\delta = 20$.

Fig. 5.24 compares the energy cost performance for DSMA-S and DBTMA. Around 25% on average of energy conservation can be achieved by DSMA-S protocol. The collision period analysis in Appendix A indicates that the fail busy period is able to reach an extreme long period, even to infinity. By fixing the listening period of receiver to only γ slots, fault listening to collided packets is avoided without the possibility of missing any useful packet transmission. With the "mandatory channel clearance" mechanism, the RTS collision period are controlled and not larger than a fixed length. It greatly reduces the contending energy spent by senders and listening energy by receiver.

5.3 Summary

In this chapter, we propose a collision avoidance mechanism, "double sense", on random access channel to tackle the hidden terminal problem and avoid the collision among data payload. Two random access protocols, DSMA-D and DSMA-S that utilize the "double sense" mechanism on dual channel and single channel basis, respectively, are designed and analyzed. The performance comparison between them, as well as with another newly proposed random access protocol RSMA, is conducted in the next chapter.

Chapter 6

Receiver Sense Multiple Access (RSMA)

In wireless mesh access networks, ad hoc and infrastructure modes are usually both used to support multiple hop data transmission from mesh clients to a mesh router. Traffic will accumulate along the path towards the mesh router. The mesh clients close to the router will have more data to transmit and these packets are more likely to collide with each other. Thus, the final hop CR communication is usually heavily loaded and very sensitive to packet collisions. In this chapter, a collision avoidance random access MAC protocol "receiver sense multiple access" (RSMA) is proposed exclusively for the last-hop CR communication.

6.1 Receiver Sense Multiple Access (RSMA)

6.1.1 Access Mechanism of RSMA

CR communications are operated in a centralized basis with the mesh router as the common receiver. As mesh router is much more powerful in terms of communication and processing abilities, RSMA lets the mesh router to act a vital role in random access control. In RSMA, two out-of-band busy tone sig-

nals BT_t and BT_r are setup by the mesh router (receiver) only, to indicate an ongoing transmission of RTS and DATA, respectively. The BT_t is turned on immediately when a RTS packet arrives. BT_r is set up only if RTS is received successfully. As a result, the entire transmission time of DATA and part of RTS is covered and protected by busy tone signals. Transmission successful probability is greatly enlarged, which results in throughput improvement and delay reduction. The detailed algorithm of RSMA is given step-by-step in table 6.1.

A transmitter sends out a RTS packet (step 3.1) when channel becomes idle. Then it senses BT_r signal at the beginning of two slots later (step 3.2) before making the decision (step 3.3) whether to send out its DATA packet. The two time slots gap is to consume a round-trip propagation delay for RTS sending and BT_r arriving. The receiver (mesh router) keeps monitoring the common wireless channel activity for any possible incoming control packets from the mesh clients one hop away. It broadcasts BT_t signal (step 4) when start receiving a RTS packet without considering whether the RTS will succeed or not. By doing this, all terminals that have transmission attempts are silenced and the on-going RTS transmission is protected by BT_t signal. If the transmission is successful, the mesh router switches off the BT_t signal and turns on the BT_r signal (steps 5) so as to inform the RTS sender to transmit its DATA packet and provide continuous protection for it.

Fig. 6.1 takes an example of access mechanism and illustrates the access procedures of RTS for one receiver router **R** and seven transmitters, namely client **A** to client **G**. In Fig. 6.1, a data transmission request arrives at client **A** within the third time slot. Since neither BT_t nor BT_r signal is sensed at the beginning the next (forth) time slot, client **A** sends a RTS packet, denoted by

Table 6.1: Access Mechanism of RSMA

RSMA Algorithm

Sender Side (Mesh Client).

INPUT: a transmission attempt and the receiver's identity.

OUTPUT: the transmission attempt is failed or successful.

1. Check the status of both BT_t and BT_r signals at the beginning of next time slot.

2. IF either BT_t or BT_r signal is sensed, i.e. $BT_t = 1$ or $BT_r = 1$, THEN return failed.

3. ELSE do the following: (Both BT_t and BT_rsignals are not sensed, i.e. $BT_t = 0$ and $BT_r = 0$.)

   3.1 Send a RTS packet (including the receiver's identity).

   3.2 Check the status of BT_r signal at the beginning of two time-slot later.

   3.3 IF the BT_r signal is not sensed, i.e. $BT_r = 1$, THEN do the following:

      3.3.1 Send the DATA packet (including the receiver's identity).

      3.3.2 Return successful.

   3.4 ELSE return failed.

Receiver Side (Mesh Router):

INPUT: a RTS packet.

OUTPUT: a RTS transmission is successful or failed.

4. Turn on BT_t UPON start receiving RTS.

5. IF the RTS is correctly received.

   5.1 Switch off BT_t, turn on BT_r and wait for DATA packets,

   5.2 Return successful.

6. ELSE return failed.

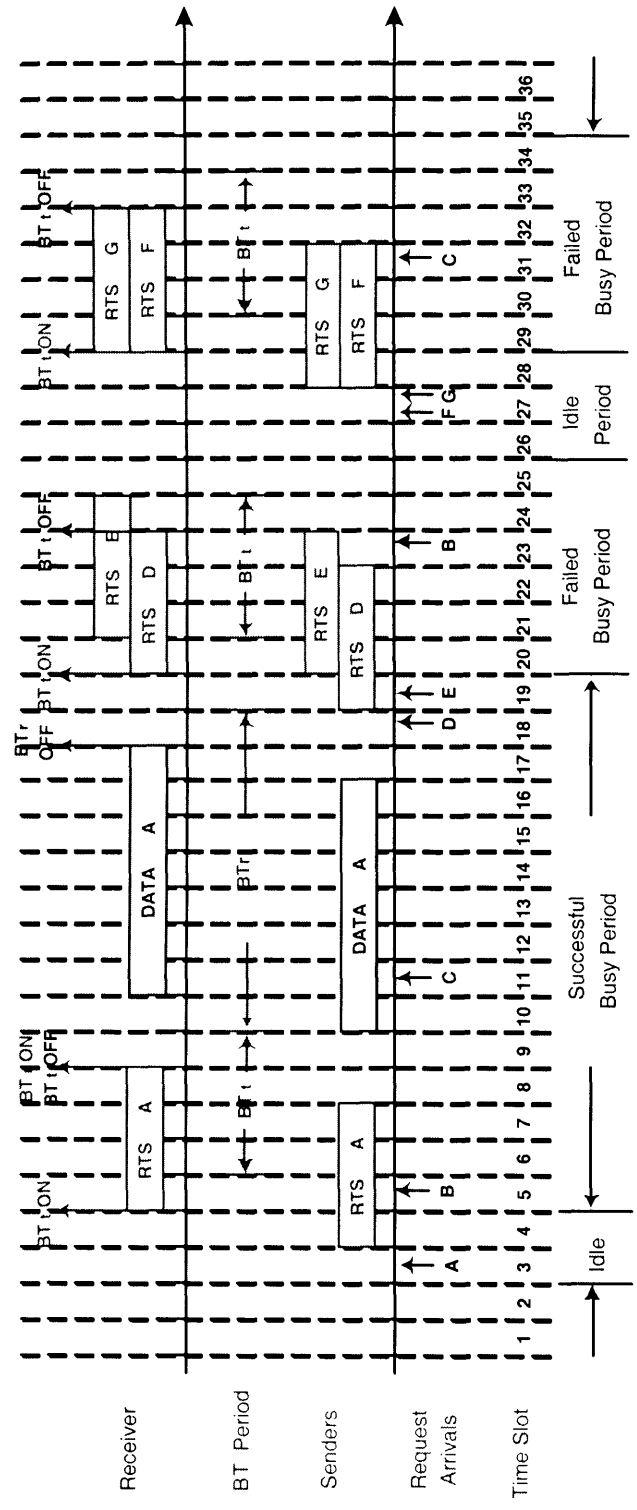

Figure 6.1: Access Mechanism of RSMA

RTS-A. RTS-A arrives at the receiver, router **R**, after a one-slot propagation delay. Upon the arrival of the RTS-A packet, router **R** turns on its BT_t signal, at the beginning of the fifth slot. One slot later, the BT_t signal can definitely sensed by router **R**'s neighboring terminals (the seven transmitters). Thus, the subsequent part of RTS-A transmission is protected. Client **A** completes the transmission of RTS-A by the end of the seventh slot and the whole RTS packet arrives at the receiver by the end of eighth time slot. Since RTS-A is correctly received, router **R** switches off the BT_t signal and turns on the BT_r signal at the beginning of ninth time slot. After sending out the RTS-A, client **A** waits for the notification from the receiver to send its data packets. At the beginning of the 10^{th} time slot, the BT_r signal is sensed by client **A** and at the same time, client **A** sends its data packets, DATA-A. During the "BT_t Period" plus "BT_r Period", clients with their transmission/retransmission attempts scheduled, senses a busy tone signal before transmission and then keep silence. In other words, clients having transmission attempts from the beginning of fifth time slot till the end of 17^{th} time slot are not permitted to send their RTS, e.g. client **B** at the fifth time slot and client **C** at the 11^{th} time slot. They schedule their retransmission attempts after a random backoff delay at 23^{rd} and 31^{st} slots respectively. Clients **D** and **E** have their packet transmission attempts arriving within 18^{th} and 19^{th} slot respectively, while client **F** and **G** with in the 27^{th} slot. They send their RTS packets since there is no busy tone reserve the channel at that time. Unfortunately, RTS-RTS collision occurs at router **R** and all involved RTS packets are failed. As a result, the BT_r signal will not be turned on since no correct RTS packet is received. This vulnerable period of an RTS packet is just a round-trip, two-slot gap, equal to the summation of one slot for RTS arriving and another slot for BT_t signal propagating time.

When collision happens, the transmission (retransmission) attempts are failed and the corresponding clients have to reschedule their retransmissions after a random backoff delay. As the BT_t signal is set up anyway, and the rescheduled transmission from **B** (23^{rd}) and **C** (31^{st}) are both silenced since BT_t is sensed before transmitting their RTS packets.

6.1.2 Pure MAC layer Performance Analysis

In this section, we construct a precise mathematic model to analyze the throughput, delay and blocking probability performance of RSMA.

6.1.2.1 Throughput Analysis

In RSMA, part of RTS transmission is protected by BT_t signal except first two slots, which is a round-trip propagation delay including the RTS sending and BT_t arriving duration. Thus the success probability of a packet transmission attempt p_s is given by:

$$p_s^{RSMA} = \frac{\lambda\tau \cdot e^{-2\lambda\tau}}{1 - e^{-\lambda\tau}} . \tag{6.1}$$

The average length of an Idle period $E[I]^{RSMA}$ is given by:

$$E[I]^{RSMA} = E[I]^{DSMA-S} = E[I]^{DSMA-D} = \frac{e^{-\lambda\tau} \cdot \tau}{1 - e^{-\lambda\tau}} . \tag{6.2}$$

The length of a successful busy period equals to the summation of the transmission times of a RTS packet, a DATA packet and two periods of round-trip propagation delay for turning on and off the BT_r signals, i.e.

$$E[B_s]^{RSMA} = (\gamma + \delta + 4) \cdot \tau . \tag{6.3}$$

The average channel utilization is simply given by:

$$E[U]^{RSMA} = \delta\tau \cdot p_s^{RSMA} . \tag{6.4}$$

Since the BT_t signal is turned on while the first RTS packet arrives at the receiver, the channel is covered by BT_t signal for γ time slots even though a

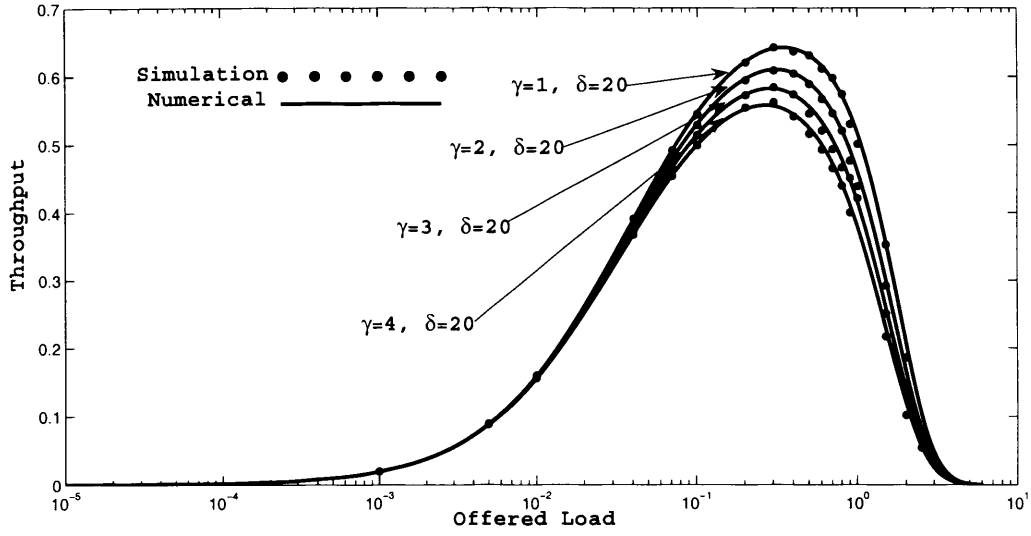

Figure 6.2: Throughput RSMA, $\gamma = 1, 2, 3, 4$, $\delta = 20$.

collision may happen. Therefore, with the round-trip signal propagation delay included, the length of a fail busy period is fixed to γ+2 time slots, i.e.

$$E[B_f]^{RSMA} = (\gamma + 2) \cdot \tau \,. \tag{6.5}$$

Substituting (5.74), (6.2), (6.3), (6.4) and (6.5) into (5.1), we get the system throughput expression as:

$$\begin{aligned} S^{RSMA} &= \frac{\lambda\tau \cdot \delta e^{-2\lambda\tau}}{(\delta+2)\cdot\lambda\tau\cdot e^{-2\lambda\tau} + (\gamma+1)\cdot(1-e^{\lambda\tau}) + 1}\,, \\ &= \frac{\delta \cdot G \cdot e^{-2G}}{(\delta+2)\cdot G\cdot e^{-2G} + (\gamma+1)\cdot(1-e^{-G}) + 1}\,. \end{aligned} \tag{6.6}$$

where $G \triangleq \lambda\tau$ is referred to as "offered traffic".

Fig. 6.2 and Fig. 6.3 illustrate the analytical throughput curves of RSMA plotted according to the equation (??) while the simulation results are shown in markers. RSMA simulation also operates on a C++ platform that describes the random access channel of a receiver when a number of transmission at-

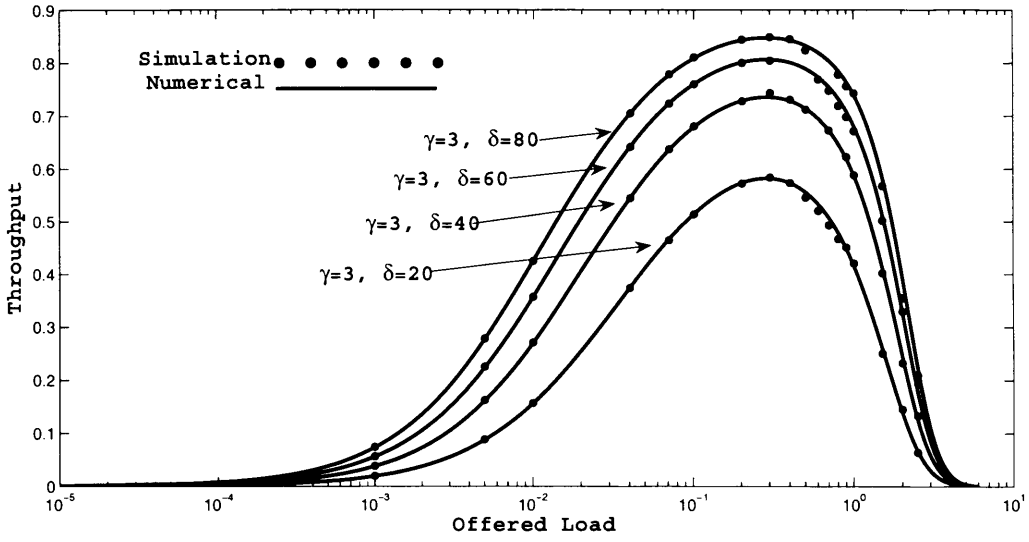

Figure 6.3: Throughput RSMA, $\gamma = 3$, $\delta = 20, 40, 60, 80$.

tempts try to access this channel. Similar with DSMA-D and DSMA-S, the throughput performance has a direct link to the ratio δ/γ.

6.1.2.2 Access Delay and Blocking Probability Analysis

Access Delay Distribution of RSMA.

According to the RSMA algorithm, a transmitter needs to check the status of BT_t and BT_r signals before sending out its RTS packet. Two time slots after the RTS transmission, BT_r is sensed to make further decision of sending DATA or backoff.

CASE I: NO RTS PACKET IS TRANSMITTED.

Within one transmission cycle, the average length of BT_t and BT_r period are $\gamma\tau \cdot p_s^{RSMA}$ and $(\delta+2)\tau \cdot p_s^{RSMA}$ respectively. So the probability that the BT_t or BT_r signal is sensed (hence no RTS packet is transmitted) is given respectively

by:

$$\begin{aligned} p_{11} &= \frac{\gamma\tau \cdot p_s^{RSMA}}{E[I]^{RSMA} + E[Bs]^{RSMA} \cdot p_s^{RSMA} + E[B_f]^{RSMA} \cdot (1 - p_s^{RSMA})}, \\ &= \frac{\gamma \cdot G \cdot e^{(-2G)}}{(\delta+2) \cdot G \cdot e^{-2G} + (\gamma+1) \cdot (1 - e^{-G}) + 1}. \end{aligned} \tag{6.7}$$

$$\begin{aligned} p_{12} &= \frac{(\delta+2)\tau \cdot p_s^{RSMA}}{E[I]^{RSMA} + E[Bs]^{RSMA} \cdot p_s^{RSMA} + E[B_f]^{RSMA} \cdot (1 - p_s^{RSMA})}, \\ &= \frac{(\delta+2) \cdot G \cdot e^{(-2G)}}{(\delta+2) \cdot G \cdot e^{-2G} + (\gamma+1) \cdot (1 - e^{-G}) + 1}. \end{aligned} \tag{6.8}$$

If BT_t is sensed, a DATA transmission may be followed. The corresponding waiting time D_{11} has to be set larger than $(\delta + \gamma + 1)$ slots, i.e.

$$D_{11} = (W + \delta + \gamma + 1) \cdot \tau. \tag{6.9}$$

In order to avoid the transmitter sensing the same BT_r signal again, the corresponding backoff delay D_{12} before the next retransmission attempt should be set longer than $(\delta + 1)$ time slots, i.e.

$$D_{12} = (W + \delta + 1) \cdot \tau. \tag{6.10}$$

CASE II: SUCCESSFUL TRANSMISSION.

This is the successful case for RTS and DATA transmission. In this case, in order to guarantee a successful RTS packet transmission, the transmission attempt inter-arrival time should be no less than two time slots. Thus, the average length $E[I_s]^{RSMA}$ of the idle period is given by:

$$\begin{aligned} E[I_s]^{RSMA} &= \sum_{i=0}^{\infty} (i+1)\tau \cdot P\{I = (2+i)\tau\}, \\ &= \frac{e^{-2 \cdot G} \cdot \tau}{1 - e^{-G}}. \end{aligned} \tag{6.11}$$

The probability of a successful transmission is simply:

$$\begin{aligned} p_{suc}^{RSMA} &= \frac{E[I_s]^{RSMA}}{E[I]^{RSMA} + E[B]^{RSMA}}, \\ &= \frac{e^{(-\gamma G)}}{(\delta+2) \cdot G \cdot e^{-2G} + (\gamma+1) \cdot (1 - e^{-G}) + 1}. \end{aligned} \tag{6.12}$$

The corresponding delay D_2 is equal to the summation of the transmission times of RTS packet, DATA packet and a two time-slot round-trip propagation delay, i.e.

$$D_2 = (\delta + \gamma + 2) \cdot \tau \,. \tag{6.13}$$

CASE III: COLLISION.

A packet collision will be noticed by void sensing result of BT_r signal ($BT_r = 0$) after RTS transmission. In this situation, the client is set to retransmit its RTS after a $(\gamma + 2)$ slots plus a random backoff period, which must ensure has no chance to collide with the same RTS overlapped period. The probability of this case can be simply calculated as

$$p_3 = 1 - p_{11} - p_{12} - p_2, \tag{6.14}$$

and the corresponding delay D_3 is set as

$$D_3 = (W + \gamma + 2) \cdot \tau \,. \tag{6.15}$$

Average Access Delay and Blocking Probability

There are four cases of access delays, D_{11}, D_{12}, D_2 and D_3 with corresponding probabilities p_{11}, p_{12}, p_{suc}^{DSMA-S} and p_3. Let R denote the total number of retransmissions needed before a successful RTS/DATA packet transmission. Conditioning on $R \leq r_{max}$, the retransmission distribution of those successful data packets is given by

$$P\{R = r \mid R \leq r_{max}\} = \frac{p_{suc}(1 - p_{suc})^r}{1 - (1 - p_{suc})^{r_{max}+1}}, \quad r = 0, 1, 2, \ldots, r_{max}, \tag{6.16}$$

and the blocking probability P_B is defined as

$$P_B^{RSMA} = P\{R > r_{max}\} = (1 - p_{suc}^{RSMA})^{r_{max}+1} \,. \tag{6.17}$$

The mean value of R is given by

$$E[R]^{RSMA} = \frac{(1-p_{suc}^{RSMA}) - (p_{suc}^{RSMA} r_{max}+1)(1-p_{suc}^{RSMA})^{r_{max}+1}}{[1-(1-p_{suc}^{RSMA})^{r_{max}+1}] \cdot p_{suc}^{RSMA}}. \tag{6.18}$$

We let M and N denote the numbers of failed transmission attempts due to sensing the BT_t and BT_r in Cases I, wherein $0 \leq M+N \leq R$. The joint distribution of R, M and N is given by:

$$P\{R=r, M=m, N=n\} = \binom{r}{m}\binom{r-m}{n} p_{suc}^{RSMA} p_{11}^{m} p_{12}^{n} p_{3}^{r-n-m}. \tag{6.19}$$

The mean values of M and N can be derived as:

$$E[M]^{RSMA} = \frac{\left(\frac{p_{11}}{p_{11}+p_{suc}^{RSMA}}\right) - \left(\frac{p_{suc}^{RSMA} r_{max}}{p_{11}+p_{suc}^{RSMA}}+1\right)\cdot\left(\frac{p_{11}}{p_{11}+p_{suc}^{RSMA}}\right)^{r_{max}+1}}{\left[1-\left(\frac{p_{11}}{p_{11}+p_{suc}^{RSMA}}\right)^{r_{max}+1}\right]\cdot\frac{p_{suc}^{RSMA}}{p_{11}+p_{suc}^{RSMA}}}, \tag{6.20}$$

and

$$E[N]^{RSMA} = \frac{\left(\frac{p_{12}}{p_{12}+p_{suc}^{RSMA}}\right) - \left(\frac{p_{suc}^{RSMA} r_{max}}{p_{12}+p_{suc}^{RSMA}}+1\right)\cdot\left(\frac{p_{12}}{p_{12}+p_{suc}^{RSMA}}\right)^{r_{max}+1}}{\left[1-\left(\frac{p_{12}}{p_{12}+p_{suc}^{RSMA}}\right)^{r_{max}+1}\right]\cdot\frac{p_{suc}^{RSMA}}{p_{12}+p_{suc}^{RSMA}}}, \tag{6.21}$$

respectively.

Let $D_{11,i}$ and $D_{12,j}$ denote the i^{th} and j^{th} access delay due to sensing the BT_t and BT_r in Cases I; $D_{3,k}$ denotes the access delay due to Case II; D_0 denotes the synchronization delay. The total access delay D and its mean value is given by

$$\begin{aligned} D &= D_0 + D_2 + \sum_{i=1}^{M} D_{11,i} + \sum_{j=1}^{N} D_{12,j} + \sum_{k=M+N+1}^{R} D_{3,k} \\ &= D_0 + (\gamma+\delta+2)\tau + \tau\cdot\sum_{l=1}^{R} W_l + M(\delta+1)\tau \\ &\quad + N(\delta+\gamma+1)\tau + (R-M-N)(2\gamma+1)\tau, \end{aligned} \tag{6.22}$$

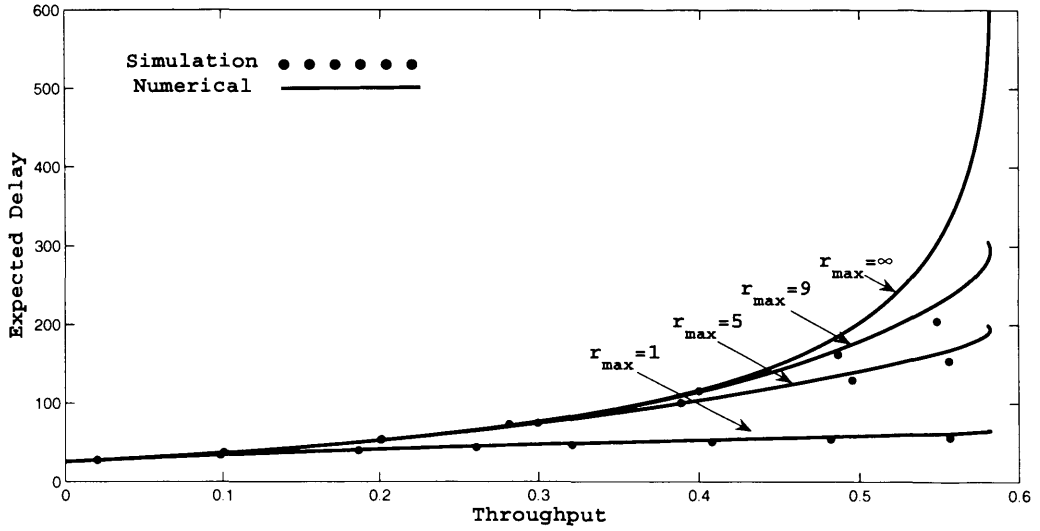

Figure 6.4: Delay RSMA, $\gamma = 3$, $\delta = 20$, $E[W] = 50$.

and

$$\begin{aligned} E[D] = {} & (\gamma + \delta + 3)\tau + E[W]E[R]^{RSMA} \cdot \tau + E[M]^{RSMA}(\delta + 1)\tau \\ & + E[N]^{RSMA}(\delta + \gamma + 1)\tau + (E[R]^{RSMA} - E[M]^{RSMA} \\ & - E[N]^{RSMA})(2\gamma + 1)\tau , \end{aligned} \tag{6.23}$$

respectively.

Fig. 6.4 and Fig. 6.5 illustrate the delay and blocking probability performance of RSMA wherein the analytical curves are calculated according to equation (6.17) and (6.23), respectively. Similar with DSMA-D and DSMA-S, there is tradeoff between the delay and blocking probability with r_{max} as the parameter.

6.1.3 Cross-layer Throughput Analysis of RSMA

The MAC-physical cross-layer throughput analysis refers to the access model on the MAC layer and the radio propagation model, capture model on the

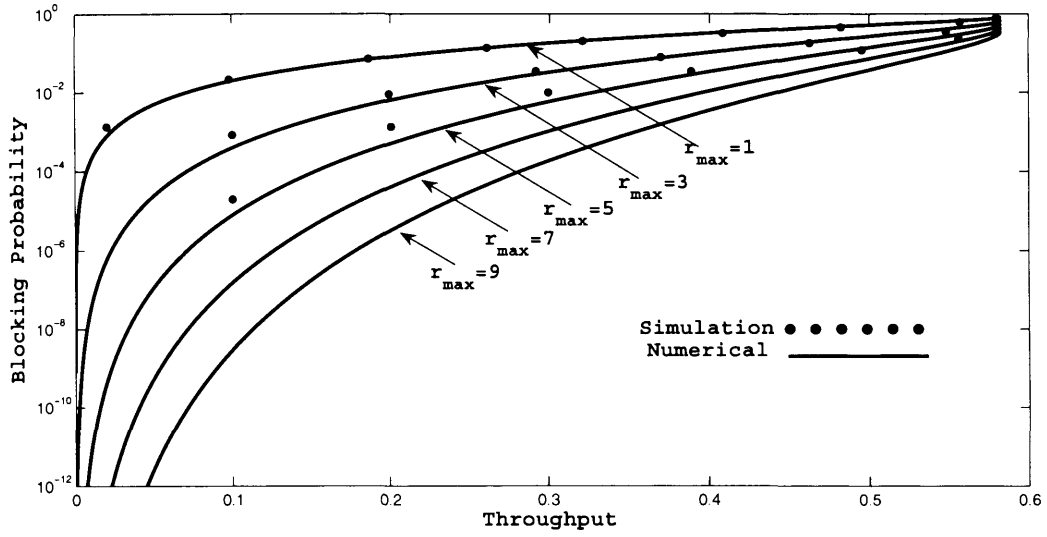

Figure 6.5: Blocking Probability RSMA, $\gamma = 3$, $\delta = 20$, $E[W] = 50$.

physical layer. From the pure MAC layer's perspective, a RTS transmission is able to succeed if there are no contending arrivals during the vulnerable period (2τ) of it. On the other hand, it fails if there are additional RTS arrivals (say n RTS packets). Thus, the MAC layer successful and fail access probabilities are expressed as:

$$p_s^{RSMA(MAC)} = \frac{G \cdot e^{-2G}}{1 - e^{-G}}, \tag{6.24}$$

and

$$p_f^{RSMA(MAC)}\{N = n\} = \frac{G^{(n+1)}e^{-2G}}{(1 - e^{-G})(n+1)!} \qquad n \geq 1, \tag{6.25}$$

respectively, wherein $G = \lambda\tau$ is known as the offered traffic.

The physical layer performance analysis follows the conventional method in [105], [106] and [107]. According to the radio propagation principle described in chapter 3, a RTS packet will encounter three propagation phenom-

ena before reaching the packet receiver: path loss, log-normal shadowing and Rayleigh fast fading. The instantaneous RTS power level transmitted from mesh client i at the mesh router r is a random variable. It is Rayleigh distributed over the local mean power (W_i). The probability density function (pdf) is knows as:

$$f(w_i|W_i) = \frac{1}{W_i} exp\left(-\frac{w_i}{W_i}\right). \tag{6.26}$$

If the ideal power control is enabled, the mean power (local and area mean) of each transmitted packet at the receiver (mesh router) is identical. This value is assumed to μ and the instantaneous power level of mesh clients at the mesh router is rewritten to:

$$f(w_i) = \frac{1}{\mu} exp\left(-\frac{w_i}{\mu}\right). \tag{6.27}$$

From the physical layer's perspective, the access successful probability is highly related to the signal to noise and interference ratio (SINR) at the receiver side. If there is only one RTS arrival, it is still quite possible that the transmission fails because of the background noise. Thus, the successful probability is expressed as:

$$\begin{aligned} p_{s1}^{RSMA(PHY)} &= P\left(\frac{w_i}{n_0} \geq T_c\right) \\ &= \int_{T_c \cdot n_0}^{\infty} \frac{1}{\mu} exp\left(-\frac{w_i}{\mu}\right) dw_i \end{aligned} \tag{6.28}$$

wherein n_0 is the power of the additive white Gaussian noise (AWGN) and T_c is the minimum SINR (signal to noise interference ratio) at the mesh router.

On the other hand, if there are n contending RTS arriving within the vulnerable period of the intended RTS transmission, the successful probability of

the intended RTS is given by:

$$p_{s2}^{RSMA(PHY)}\{N=n\} = P\left(\frac{w_i}{\sum_{j=1}^{n} w_j + n_0} \geq T_c\right) \qquad n \geq 1. \tag{6.29}$$

Wherein the $\sum_{j=1}^{n} w_j$ is the power aggregation of n interfering RTS transmission and n_0 is the power of the background noise. All RTS transmissions are regarded as independent, thus the total received power $\sum_{j=1}^{n} w_j$ has a Gamma distribution [102], and equation (6.29) is rewritten by:

$$\begin{aligned} p_{s2}^{RSMA(PHY)}\{N=n\} &= P\left(\frac{w_i}{\frac{w_j^{n-1}exp\left(-\frac{w_j}{\mu}\right)}{(n-1)!\mu^n} + n_0} \geq T_c\right) \\ &= \int_0^{\infty}\left(\int_{\left(\frac{w_j^{n-1}exp\left(-\frac{w_j}{\mu}\right)}{(n-1)!\mu^n}+n_0\right)}^{\infty}\frac{1}{\mu}e^{\left(-\frac{w_i}{\mu}\right)}dw_i\right)\frac{1}{\mu}e^{\left(-\frac{w_j}{\mu}\right)}dw_j \\ & \qquad n \geq 1. \end{aligned} \tag{6.30}$$

Therefore, we can define the cross-layer successful probability as the aggregation of the MAC and physical layer successful access rate:

$$\begin{aligned} p_s^{RSMA(Cro)} &= p_s^{RSMA(MAC)} \cdot p_{s1}^{RSMA(PHY)} + \sum_{n=1}^{\infty} p_f^{RSMA(MAC)} \cdot p_{s2}^{RSMA(PHY)} \\ &= \frac{G \cdot e^{-2G}}{1-e^{-G}} \cdot \int_{T_c \cdot n_0}^{\infty} \frac{1}{\mu} exp\left(-\frac{w_i}{\mu}\right) dw_i + \sum_{n=1}^{\infty} \frac{G^{(n+1)}e^{-2G}}{(1-e^{-G})(n+1)!} \\ &\cdot \int_0^{\infty}\left(\int_{\left(\frac{w_j^{n-1}exp\left(-\frac{w_j}{\mu}\right)}{(n-1)!\mu^n}+n_0\right)}^{\infty}\frac{1}{\mu}e^{\left(-\frac{w_i}{\mu}\right)}dw_i\right)\frac{1}{\mu}e^{\left(-\frac{w_j}{\mu}\right)}dw_j \end{aligned} \tag{6.31}$$

The throughput of the MAC layer is known to be

$$S^{RSMA(MAC)} = p_s^{RSMA(MAC)} \cdot \frac{\delta\tau}{E[B_f]^{RSMA} \cdot (1 - p_s^{RSMA(MAC)}) + E[B_s]^{RSMA} \cdot p_s^{RSMA(MAC)}} \tag{6.32}$$

while the throughput of the cross-layer is given by

$$S^{RSMA(Cro)} = p_s^{RSMA(Cro)} \cdot \frac{\delta\tau}{E[B_f]^{RSMA} \cdot (1 - p_s^{RSMA(Cro)}) + E[B_s]^{RSMA} \cdot p_s^{RSMA(Cro)}} \tag{6.33}$$

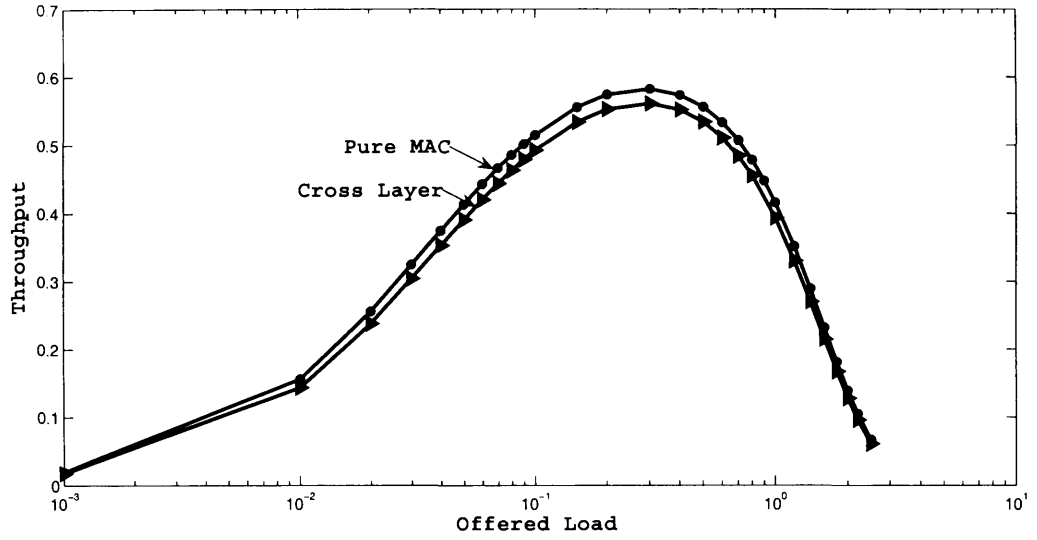

Figure 6.6: Throughput Comparison, Pure MAC and Cross Layer (μ=1 dBm, T_c=1,n_0=0.1 dBm).

Table 6.2: Values of Parameters

Local Mean Power Level μ (dBm)	1
Average Background Noise n_0 (dBm)	0.1, 0.3, 0.5
Power Capture Ratio T_c	1 (0 dB), 3 (4.8 dB), 5 (7.0 dB)

To varify these analytical results, numerical results are generated according to the values given by Tab. 6.2. Fig. 6.6 compares the numerical curves of the pure MAC layer and the cross-layer throughput performance. It is indicated that the pure MAC layer throughput performance is always better than

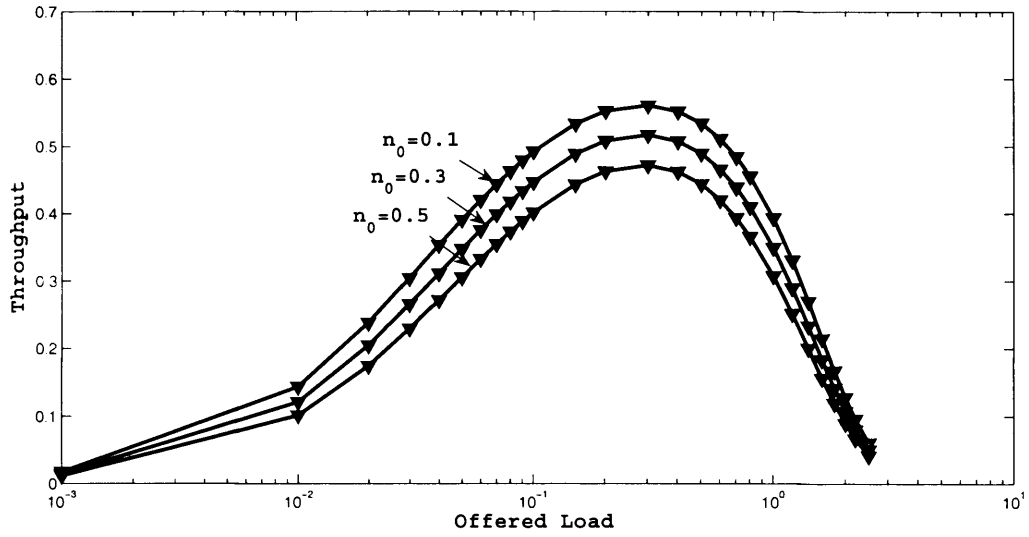

Figure 6.7: Cross-Layer Throughput, μ=1 dBm, T_c=1.

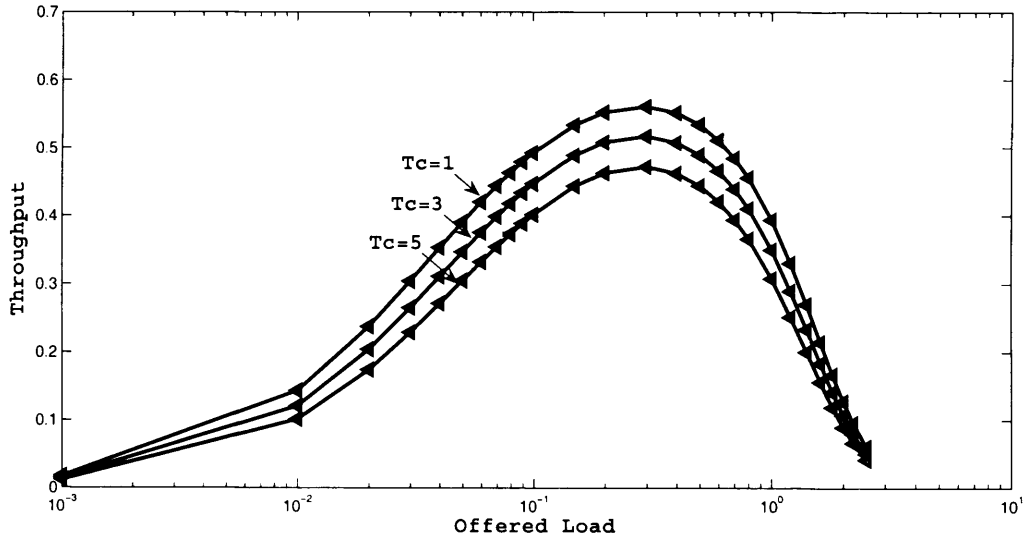

Figure 6.8: Cross-Layer Throughput, μ=1 dBm, n_0=0.1 dBm.

the cross layer throughput performance. When the traffic load is light, data packets have high probability to succeed on MAC layer. However, Rayleigh fading phenomenon on the transmission path decreases the successful probability of these packets. Thus, the cross layer throughput is lower than the pure MAC layer throughput. When the traffic load is heavy, successful transmission on MAC layer will also quite possible to fail because of physical layer propagation loss. However, packets collided on the MAC layer still have chance to be rescued by the capture effect and this improves the successful rate. As a result, in Fig. 6.6, the deviation between the pure MAC and cross layer throughput becomes smaller when traffic load gets heavier. Fig. 6.7 compares the cross layer throughput when the mean value of background noise n_0 varies. Fig. 6.8 compares the cross layer throughput when the capture ratio T_c varies. As expected, the throughput performance becomes worse when the n_0 or T_c get larger. The intended packet is able to be captured if its signal power level is T_c times larger than the interference plus the mean background noise n_0 that totally depends on the environment. The capture ratio T_c indicates the interference resistance ability of the receiver and smaller value means more powerful capture ability. T_c=1 (0dB) is the perfect capture scenario wherein the intended signal power level just has to be equal to the interference plus the noise to be successful received. Unfortunately, in real applications, the capture ratio is usually much larger than this value.

6.2 MAC Protocols Comparison

6.2.1 Comparison Among DSMA-D, DSMA-S and RSMA

Figs. 6.9, 6.10 and 6.11 illustrate the access successful rate, channel throughput and average access delay comparison, respectively, for the DSMA-

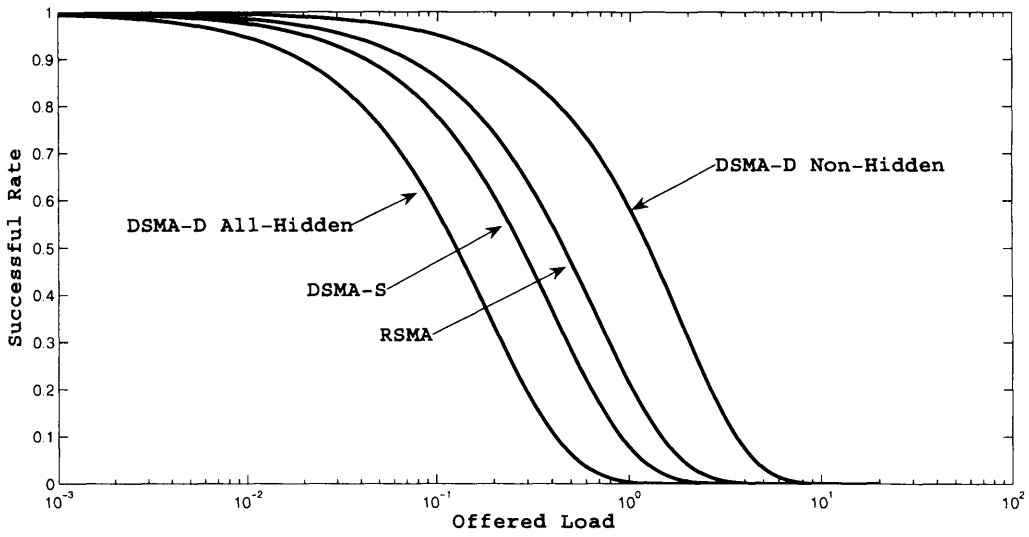

Figure 6.9: Successful Rate, DSMA-D, DSMA-S and RSMA.

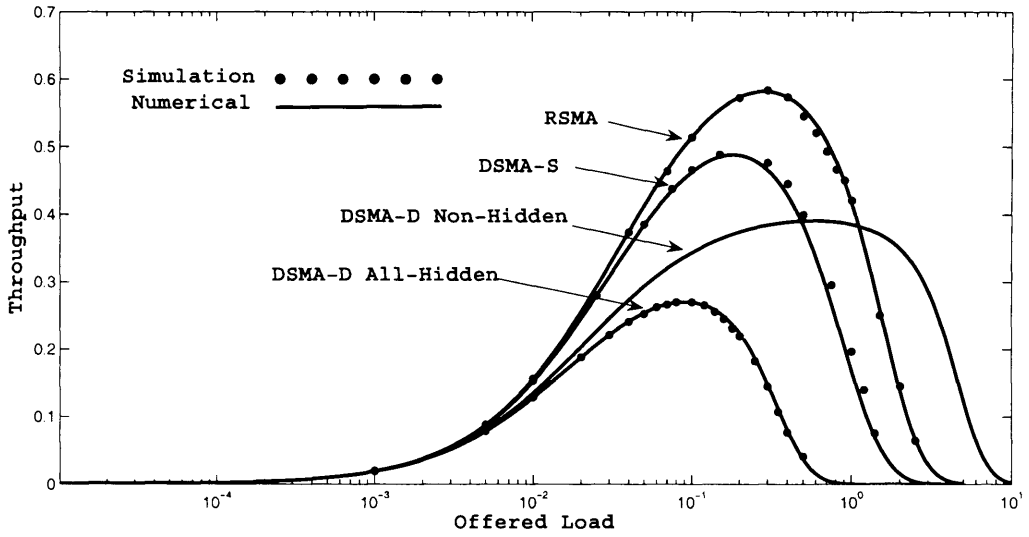

Figure 6.10: Throughput DSMA-D, DSMA-S and RSMA.

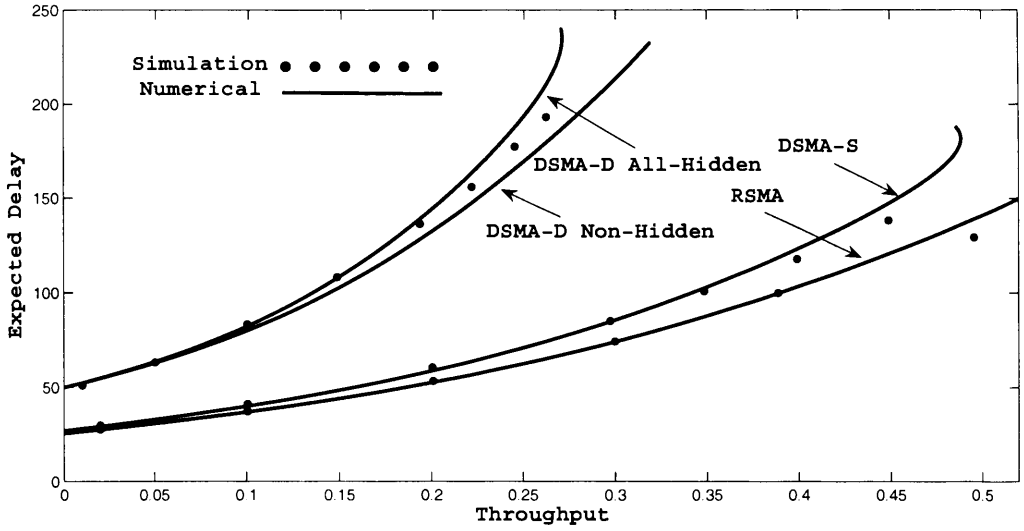

Figure 6.11: Delay DSMA-D, DSMA-S and RSMA.

D, DSMA-S and RSMA protocols. RTS and DATA packet size is set to $\gamma = 3$ and $\delta = 20$, respectively, while the maximum transmission limitation is set to $r_{max} = 5$. Since the channel separation ratio is set to D=0.5 , the RTS and DATA transmission time are $\gamma' = 6$ and $\delta' = 40$ slots in DSMA-D. The curves of access successful rate in Fig. 6.9 are calculated according to equation (5.2) ($p_{s(A)}^{DSMA-D}$), equation (5.11) ($p_{s(N)}^{DSMA-D}$), equation (5.48) (p_s^{DSMA-S}) and equation (6.1) (p_s^{RSMA}). The curves of throughput (Fig. 6.10) and access delay (Fig. 6.11) are cutted from previous figures (Figs. 5.5, 5.6, 5.14, 5.16, 5.19, 5.21, 6.2 and 6.4).

As illustrated in Fig. 6.9, the DSMA-D has the best access successful rate among the three protocols in the non-hidden-sender environment. However, DSMA-D also has the worst successful rate performance in the all-hidden-sender environment. This is because the vulnerable periods (V) of the DSMA-D non-hidden, RSMA, DSMA-S and DSMA-D all-hidden are τ, 2τ,

$\gamma\tau$ and $\gamma'\tau$ respectively, where $V_{DSMA-D(all-hidden)} > V_{DSMA-S} > V_{RSMA} > V_{DSMA-D(non-hidden)}$. In Figs. 6.10 and 6.11, the RSMA and DSMA-S have much better throughput and delay performance than the DSMA-D all-hidden and non-hidden sender environments although the three protocols have the same δ/γ ratio and r_{max} value. This phenomenon indicates clearly that the channel separation collision avoidance mechanism consumes too much channel resource. Extra operation difficulties and latency are induced when the protocol switches among different channels which makes it less attractive and practical for real-life implementation. Theoretically, both RSMA and DSMA-S can achieve collision free DATA transmission as well as alleviate RTS-RTS collision. Figs. 6.10 and 6.11 illustrate that RSMA performs more efficiently by broadcasting BT_t upon receiving RTS. Not only there is no DATA-DATA and DATA-RTS collision, more importantly, RTS-RTS collision probability is efficiently controlled and minimized. However, the immediate BT_t broadcasting may jitter and interrupt other communications which makes the RSMA suitable only for the final hop CR communication. DSMA-S conducts good balance between collision avoidance and resource conservation. By using the "mandatory waiting" mechanism, DATA-RTS collision is avoided; and by using the "mandatory clearance" mechanism, RTS-RTS collision is alleviated. All these solutions can be carried out on single wireless channel. These characteristics make the DSMA-S suitable for resource limited and traffic heavy loaded peer-to-peer communications.

6.2.2 Comparison with DBTMA

When mentioning the busy tone based random access MAC, it is unavoidable to recall the DBTMA (dual busy tone multiple access) [40] protocol. In [40], the authors compare the DBTMA protocol with several existing random access

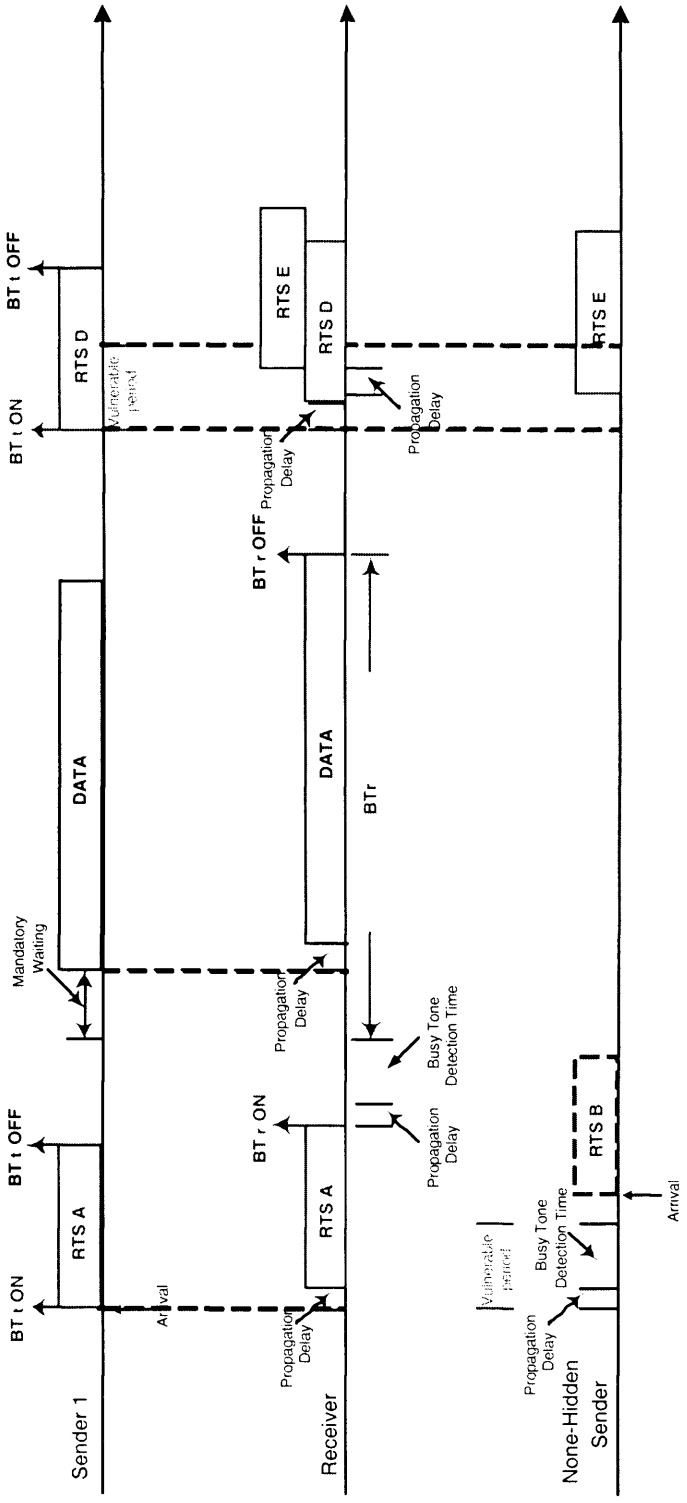

Figure 6.12: DBTMA Access Procedure Non-Hidden-Sender Environment

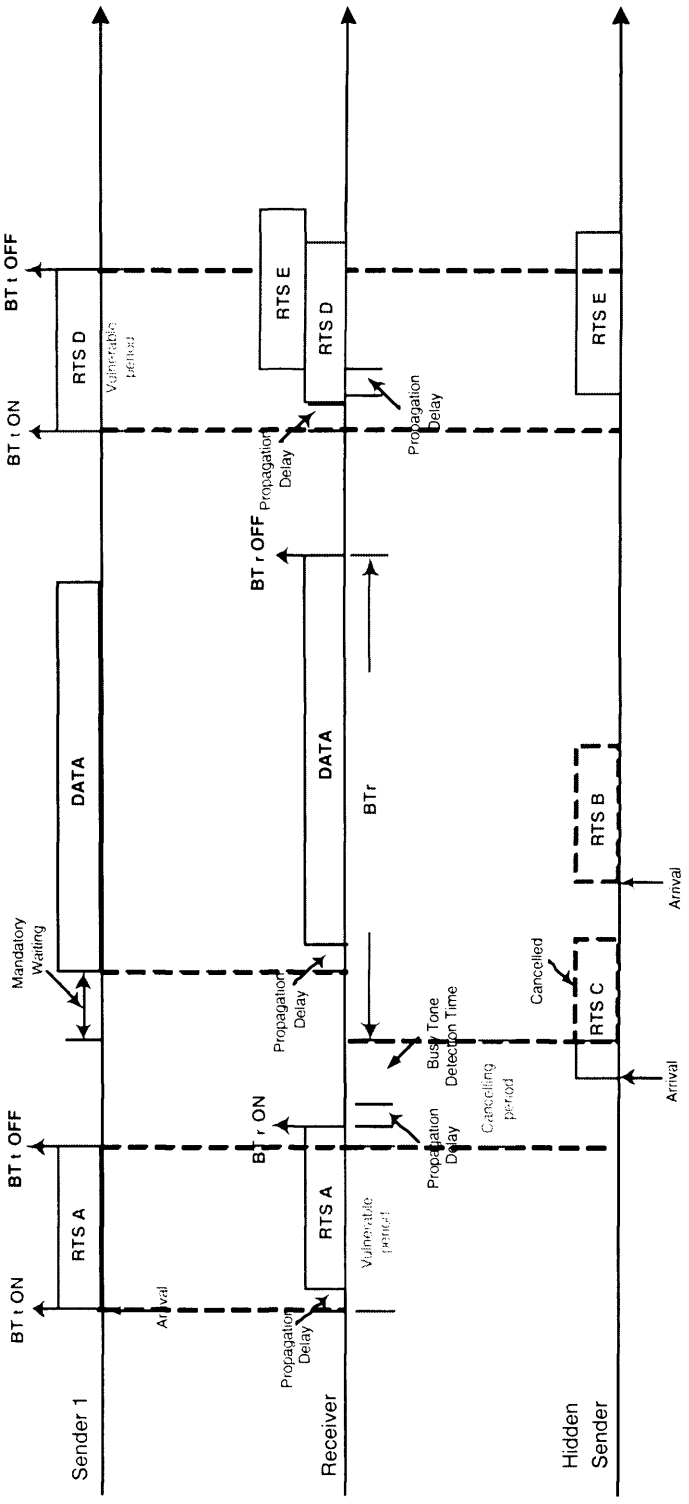

Figure 6.13: DBTMA Access Procedure in All-Hidden-Sender Environment

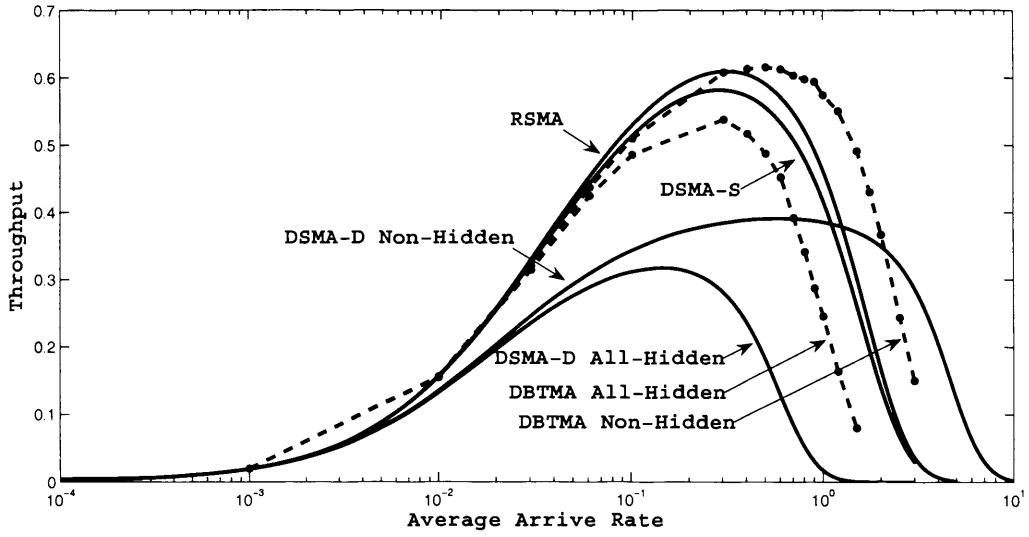

Figure 6.14: Throughput Comparison Among DBTMA, DSMA-D, DSMA-S and RSMA

protocols such as IEEE 802.11 DCF, MACA, FAMA, etc., and illustrate the superior performance of it. As briefly introduced in Chapter 4, the DBTMA protocol targets at resolving the packet collision problem by employing two out of band busy tone signals, BT_t and BT_r, to indicate the status of transmitting a RTS packet and receiving a DATA packet, respectively. Packets are transmitted if both the two busy tone signals are idle. In other words, the transmitter protects the RTS transmission with the BT_t signal and the receiver protects the DATA receiving with the BT_r signal. Because of the hidden terminal problem, the BT_t signal can not sensed by the contending terminals that are hidden from the intended transmitter. As a result, the DBTMA performs quite differently in the all-hidden and non-hidden sender environments.

In the non-hidden-sender environment (Fig. 6.12), the BT_t signal is broadcasted by RTS sender and it can be sensed by contending transmitters. Thus, the vulnerable period of RTS is known as one way propagation delay plus busy

tone detection time (τ+ t_{BT}). Then the subsequent transmission is completely protected by the BT_r signal and collision free. In the all-hidden-sender environment(Fig. 6.13), each contending sender stays out of the busy tone coverage of other senders. Thus the RTS transmission is totally unprotected and the vulnerable period of RTS transmission becomes the entire RTS duration t_{RTS} plus the signal propagation delay τ (τ+ t_{RTS}) which is much longer than (τ+ t_{BT}). For a simple comparison, DBTMA simulation throughput results are illustrated in Fig. 6.14 in comparison with the DSMA-D, DSMA-S and RSMA throughput curves. Since the DBTMA also lets the RTS sender to broadcast a busy tone signal, there are two different throughput performances in all-hidden and non-hidden sender environments like the DSMA-D protocol. They indicates the upper and lower bounds of throughput performance.

There is another major disadvantage with the DBTMA as illustrated in Fig. 6.13. When the RTS transmission is successfully finished, the BT_t is setoff and the BT_r is setup to inform the intended sender to transmit DATA and provide continuous protection on DATA transmission. However, there is a round-trip propagation delay for RTS transmission and BT_r arriving plus the BT_r detection time denoted by "canceling period" in Fig. 6.13. During this period, contending RTS will not collide with existing RTS packet but collide with the subsequent DATA transmission later. The DBTMA introduces a "mandatory canceling and waiting" mechanism to resolve this problem. All RTS transmissions should perform three simultaneous actions: transmit RTS, broadcast BT_t and sense busy tone when transmitting. If a busy tone signal is sensed during the RTS transmission period, this RTS transmission is mandatory cancelled to avoid collisions. The mandatory waiting period at the sender side is used to consume the cancellation duration. As a result, RTS-DATA

collision is resolved at heavy cost: every transmitter has to hold three simultaneous radio signals to perform RTS transmission, BT_t broadcasting and busy tone sensing at the same time. It induces strict hardware requirement which makes this mechanism less practical in real implementations.

Chapter 7

Meshflow Based Monitoring Framework

In the wireless mesh backbone networks, when traffic travels towards the Internet gateways, network resource consumption will be unbalanced. A network bottleneck appears on each mesh router neighboring an Internet gateway. Internet connections can be damaged easily by jamming the limited radio channel resource, exhausting computation ability or simply a flooding attack. In the access network, disruption on critical links (CR link) would totally disable the access network; MAC abusing will reduce probability of successful transmission; and flooding attacks can easily drain the limited energy supply. All these vulnerabilities and security challenges require a comprehensive network-monitoring framework to achieve real-time awareness, immediate response and even traceback to malicious users. Pre-active security design should be investigated to eliminate existing and emerging security vulnerabilities to avoid expensive add-on solutions, thus enhancing the system security.

The concept of network traffic flow has been well researched and implemented by a number of network device providers like Cisco [68] and Ju-

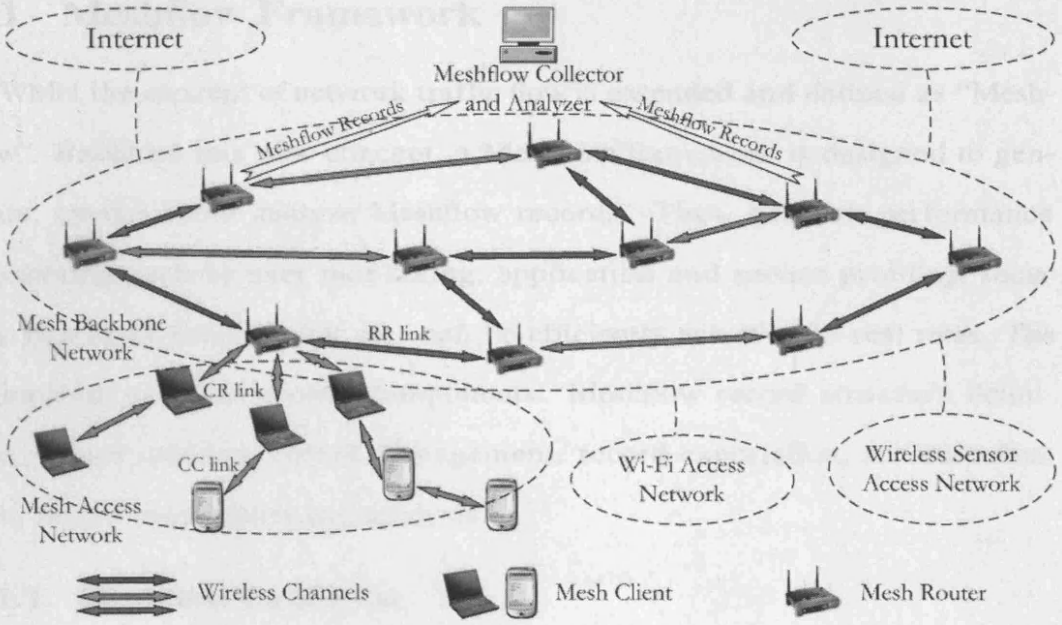

Figure 7.1: Contending Environment

niper [69] in IP networks. Consequently, great improvement of network performance efficiency, as well as comprehensive network securing, monitoring [104] and accounting, can be achieved. Generally speaking, a traffic flow consists of a number of data packets that share common or similar properties, such as source and destination addresses, type of services, port numbers, etc. In this chapter, we extend the traffic flow concept to wireless mesh network and design a comprehensive monitoring framework including user and router monitoring, application and service profiling, network security analysis and protection. A flow based security framework is designed and implemented on a centralized controller (Fig. 7.1) to real-timely monitor the terminals, applications and services in wireless mesh networks.

7.1 Meshflow Framework

In WMN, the concept of network traffic flow is extended and defined as "Meshflow". Based on this new concept, a Meshflow framework is designed to generate, transmit and analyze Meshflow records. Thus, network performance monitoring such as user monitoring, application and service profiling, security guarantee enforcement etc. can be efficiently achieved in real time. The framework includes several components: Meshflow record structure definition, record creation, record management, record exportation, record collection, record aggregation and analysis.

7.1.1 Meshflow Definition

A Meshflow record is a special kind of packet and contains a summary of common properties of data packets passing a mesh router. The fields included in a Meshflow records are source address, destination address, next hop address, number of bytes, number of packets, transport protocols, and previous transmission delay summation. These fields can be flexibly extended to include more information in later Meshflow versions according to specific network requirements. More precise traffic information can be monitored in real time. However, extra performance overhead is introduced at the same time, when generating longer records and holding/transmitting larger packets. Existing record format can also be dynamically shortened to exclude unnecessary fields.

7.1.2 Meshflow Creation

On each mesh router, part of memory size is separated to construct a Meshflow cache dedicated to Meshflow record creation and maintenance. The size of Meshflow cache is flexibly determined by individual mesh routers accord-

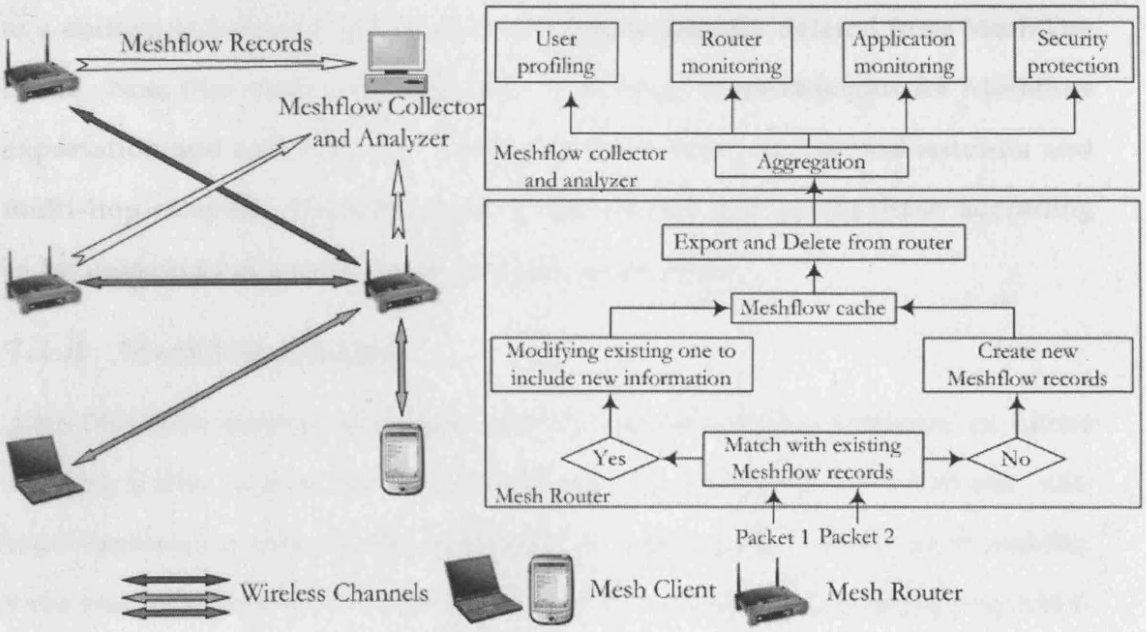

Figure 7.2: Meshflow Framework

ing to available memory or other limitations and requirements. As shown in Fig. 7.2, when a packet travels through a mesh router, its transmission information is extracted and comprises a Meshflow record. If two packets have the same source, destination, next hop address and the same transport protocol, their transmission information can be arranged in one Meshflow record by aggregating the number of packets, bytes and delay duration.

7.1.3 Meshflow Management

As soon as a Meshflow record is created, it is stamped to indicate the starting time of the record. An aging mechanism is then implemented to calculate the overall active duration of the Meshflow record. No additional processing of Meshflow records on mesh routers is suggested, since it will occupy a large part of CPU capability and interfere with basic functionality of mesh routers, e.g. routing, access control, etc. Meshflow records are then exported

to a dedicated collector and analyzer and permanently deleted from Meshflow cache. Note that there are a number of different methodologies for Meshflow exportation and collection, i.e. dedicated cable lines, distributed antenna and multi-hop relaying. Network carriers can choose any one of these according to implementation scenario and network preference.

7.1.4 Meshflow Analysis

After Meshflow records of each router are exported to the collector, an entire network traffic picture can be constructed. By analyzing these records, network application and service performance, bandwidth utilities, user actions, virus and intrusion can be monitored and discovered without deploying hardware sniffers.

7.1.4.1 User Monitoring

When a packet travels through a multi-hop path consists of mesh routers, Meshflow records are created on every one of these routers. By aggregating these records, a complete transportation path of a particular packet can be precisely derived. This path includes the source and destination clients, and every intermediate router. Other parameters such as transport protocol and number of bytes can also be reported. As a result, comprehensive investigation of each traffic flow is achieved, including where it comes from, where to go, what kind of traffic in it and how many packets are transmitted.

7.1.4.2 Router Monitoring

In WMN, mesh routers are responsible for supplying access to clients and relaying packets for other routers. Therefore, there are three kinds of traffic on a mesh router: traffic originated from its own access network, incoming/outgoing traffic from/to other routers. These traffics can be transmitted

simultaneously if there are three separated channels. When Meshflow records are aggregated based on mesh routers, traffic transported on each channel can be illustrated clearly. As a result, access situation of wireless mesh access networks and bandwidth utilization of mesh routers can be mapped on the Meshflow collector and reflected in Meshflow record fields.

With router and client based aggregation mechanisms, a comprehensive traffic structure is constructed for subsequent monitoring and analysis.

7.1.4.3 Security Protection

In WMN, security issues include detecting abnormal traffic, identifying abusing or attacking scenarios and preventing continuous damage to the network. Compared with usual network traffic pattern, abnormal traffic is defined as any kind of traffic that may interrupt, damage or disable network functionalities. As they are usually very different from the general network traffic pattern, detection and identification can be achieved by matching corresponding abnormal/attacking signatures. For example, in a flooding attack, the most obvious characteristic (signature) is a burst traffic towards the same destination; a worm virus will let one user send hundreds and thousands of TCP connection requests within a short time period; MAC abusing or RF jamming in an access network will prohibit successful transmissions for clients and consequently no traffic generated from that access network. All these abnormal situations can be detected by analyzing the Meshflow records and matching with signatures. Then network protection can be achieved with further actions, e.g. letting the flooding generating router block the corresponding attack traffic, or finding the attacker and disabling its connectivity.

7.1.4.4 Application and Service Monitoring

Different network applications and services are usually performed by separate and dedicated transport protocols. Based on the aggregated Meshflow records of each router, performance data of each application on a router can be further fused. Current router resource utilization such as bandwidth, processing capabilities by individual applications and services can be clearly seen. Inappropriate resource utilization is reallocated to balance different applications performed on each mesh router. For example, P2P (peer to peer Protocol) applications usually grab a large share of network bandwidth. If a VoIP (real time transmission Protocol) service is deployed as well which is very sensitive to transmission delay and packet loss, it might be severely affected by the P2P application. The Meshflow records can clearly reflect this situation: large numbers of packets transmitted with peer-to-peer protocol, plus unacceptable transmission delay under real time transport protocol. Then network resource can be reallocated and balanced by preventing the P2P taking too much network bandwidth.

7.2 Implementation Issues

There are many possible ways of implementing the Meshflow framework in real networks. Unavoidably, the Meshflow framework will induce extra performance overheads and influence on several aspects of networks. Carefully designing the implementation details can make Meshflow much more suitable for specific network scenarios and induce little operation cost. If Meshflow is implemented without appropriate original (default) settings and induces unwanted network damage, self-configuration and self-optimization mechanisms will be activated to reset the related parameters.

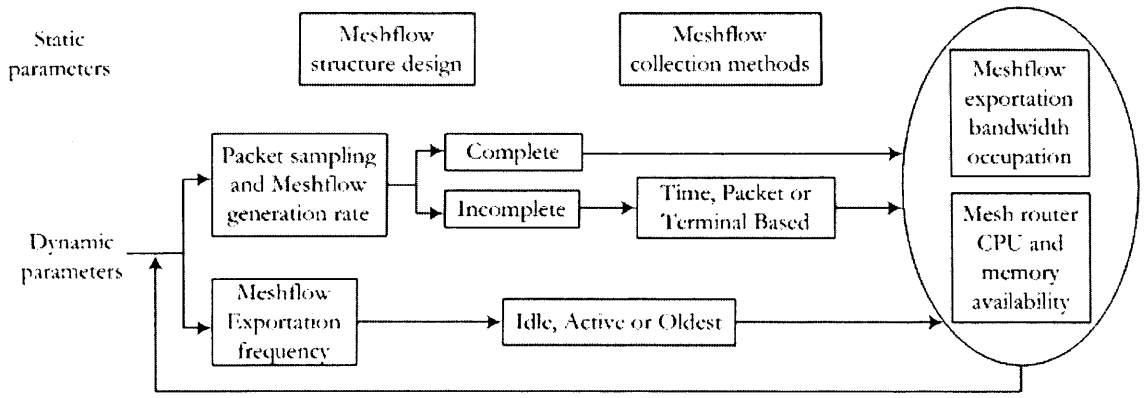

Figure 7.3: Meshflow Implementation Issues

As illustrated in Fig. 7.3, when deploying the Meshflow framework in a WMN, two static settings have first to be determined: Meshflow record structure and Meshflow collection method. As different fields within a Meshflow record are used for different monitoring and analysis purposes, it is not necessary to generate a complete record in each scenario. Unnecessary operation overhead can be efficiently avoided by carefully investigating the network requirement and defining a appropriate Meshflow record structure that includes only necessary fields. During the Meshflow exportation process, records are transmitted to the collector by three different methods:

1. Dedicated cable line: each mesh router has a dedicated cable line for Meshflow record transmission exclusively;

2. Distributed antenna: the Meshflow collector has a number of antennas deployed around the entire backbone network;

3. Multi-hop relaying: Meshflow record exportation is performed as for normal packet transmissions via a multi-hop router-to-router wireless link, finally reaching the collector.

The first two methods guarantee the reliability of Meshflow record transmission but require more strict hardware devices on the Meshflow collector. If the multi-hop relaying method is employed, the collection process might interfere with normal network traffic transport. In this situation, resource has to be carefully allocated to balance the transmission of normal packets and Meshflow records.

There are another two dynamic parameters of the Meshflow framework: packets sampling rate and record exportation time interval. They have standard settings as original values. On each mesh router, when there is an incoming packet, information required by Meshflow is extracted immediately or ignored depending on a predefined sampling rate. Sampling is originally performed on a "complete" mode to collect all incoming packet information. The original methodology may not be suitable for each mesh router depending on CPU and memory availability. By analyzing the Meshflow records generated, the original "complete" sampling method may be replaced by the "incomplete" sampling on some mesh routers to save limited processing resource:

1. Time based: extract information from an incoming packet between a certain time interval;

2. Packet based: sample one packet after ignoring a certain number of them;

3. Terminal based: capture more frequent or complete packets from a number of particular terminals that have bad or "criminal" histories.

After generating more and more Meshflow records, some of them should be exported and erased from the dynamic Meshflow cache. By defining three scenarios, Meshflow records are exported accordingly:

1. Idle: if a Meshflow record is idle for a certain period;

2. Active: if a Meshflow record is active for too long a time;

3. Oldest: oldest record in the Meshflow cache when heavily/fully loaded.

Processing and storage load on each mesh router can be efficiently alleviated by exporting records in a very frequent manner. It can be achieved by setting the "Idle", "Active" and "Oldest" time to a small value so as to prevent the mesh router from holding Meshflow records for too long a period. However, limited wireless bandwidth will be sacrificed to support the over-frequent Meshflow records exportation. Therefore, it is quite critical to investigate balancing these parameters according to the feedback from the Meshflow records under the original settings.

7.3 An Example: Flooding Attack Detection and Traceback

As an example shown in Fig. 7.4, the Meshflow framework is implemented in a network. Considering a UDP flooding attack (from client **A**) launched against client **B**, two mesh routers (1 and 3) are on this 3-hop path. A complete procedure for network monitoring, attack detection and traceback is shown in Fig. 7.5 and described as follows:

Step 1: Real-time Monitoring — Mesh routers 1-5 should export their MeshFlow records to the Meshflow collector and analyzer with default and standard Meshflow settings. The Meshflow collector always aggregates the Meshflow records on a per router basis. Application based Meshflow fusion is then further performed according to the different transport protocols. Then, applications and their resource usage on each mesh router are monitored in

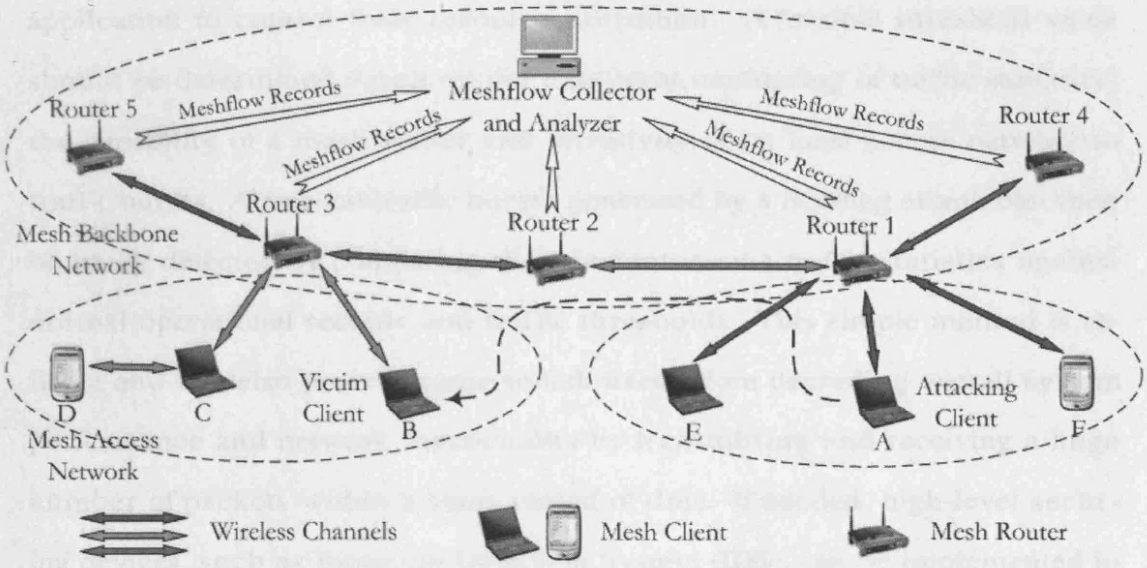

Figure 7.4: An Example: Flooding Attack

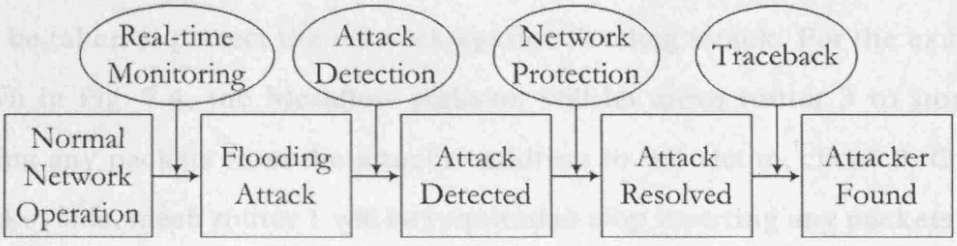

Figure 7.5: Meshflow Working Process

real time.

Step 2: Attack Detection —Thresholds and alarms are specified for each application to control their resource utilization. A feasible threshold value should be determined based on the long-term monitoring of traffic statistics, the capability of a mesh router and sensitivity of its local access network to traffic bursts. Abnormal traffic bursts generated by a flooding attack can then be easily detected by comparing their instantaneous traffic statistics against normal operational records and traffic thresholds. This simple method is reliable and can also prevent some selfish users from degrading overall system performance and network functionality by transmitting and receiving a huge number of packets within a short period of time. If needed, high-level securing devices, such as Intrusion Detection System (IDS), can be implemented to distinguish abnormal traffic bursts caused by a flooding attack from those by selfish users.

Step 3: Network Protection — By detecting and analyzing MeshFlow records of a flooding attack, we can use source and destination addresses in the same Meshflow records to identify the corresponding mesh access subnetworks of the attacker and victim machine. Some protecting actions can then be taken to protect the network against flooding attack. For the example shown in Fig. 7.4, the Meshflow collector will let mesh router 3 to stop delivering any packets from the attacker address to the victim, client B. On the attacker side, mesh router 1 will be required to stop inserting any packets from the attacker address to the mesh backbone network. This can be achieved by executing traffic filtering and rate limiting schemes at the outgoing and the incoming channels of the corresponding routers.

Step 4: Traceback —Experienced attackers can use spoofing techniques

to place incorrect source addresses in their transmitted packets for a flooding attack. This makes it very difficult to traceback and locate the real attacker. With MeshFlow, we can find out the real source of spoofed attacking packets by aggregating the records based on individual users. When a flooding attack is detected, the Meshflow collector can determine the victim (client **B**) address and suspicious (spoofed) addresses without any ambiguity. Meshflow records on each router that related to these two addresses and have the same direction (towards the victim) are extracted and fused. Then the entire traffic path is constructed and the original mesh router that holding the attacker is located. This method can be further utilized to construct a comprehensive profile for each user including basic information such as transport path, protocol and bytes transmitted. By monitoring these profiles, abnormal or selfish actions such as IP spoofing and huge traffic generation can be detected and eliminated from the very beginning.

Chapter 8

Conclusion and Future Work

8.1 Conclusion

The thesis summarizes Feiyi Huang's four-year Ph.D research on MAC protocol analysis and design, and network monitoring framework design in wireless mesh networks. After comprehensively reviewing the problems and existing solutions on MAC layer, three innovative random access MAC protocols, DSMA-S, DSMA-S and RSMA, are proposed and analyzed for wireless mesh access network. Precise mathematic models are constructed to analyze the throughput, delay, blocking probability, energy consumption and MAC-physical cross layer throughput performance. To prove the accuracy of the models, simulation is conducted on a C++ platform. By careful analysis and comparison, conclusion can be made as follows:

1. DSMA-D, DSMA-S and RSMA all utilize two busy tone signals to protect data packets transmissions. DSMA-D lets the sender to broadcast BT_t along with RTS transmission, and receiver to broadcast BT_r along with DATA receiving. DSMA-S lets the receiver to broadcast BT_c when RTS collision happens, and receiver to broadcast BT_r along with DATA receiving. RSMA lets the receiver to broadcast BT_t when start receiving

RTS, and broadcast BT_r along with DATA receiving. As a result, DSMA-D performs quite different in the all-hidden and non-hidden sender environments while DSMA-S and RSMA perform the same in these two environments. This is because DSMA-D lets the sender to broadcast a busy tone signal which usually can not be sensed by hidden terminals. In real applications, there are usually a number of hidden terminals within the system. It is less attractive if a MAC protocol performs well only at the non-hidden-sender environment but the performance degrades dramatically in a scenario where a number of hidden terminals exist. Thus, the busy tone signals are preferred to be broadcasted by packet receivers to achieve their efficient utilization.

2. By comparing the throughput and delay performance of the DSMA-D with the other protocols, it is quite clear that the DSMA-D performs much worse than the others, even in the best scenario, the non-hidden-sender environment. This is because in DSMA-D, in order to avoid the RTS-DATA collision, wireless channel is divided into two separated ones to exclusively transmit RTS and DATA packets. However, the channel division solution will severely decrease the channel utilization efficiency and therefore degrade the system performance. DSMA-S introduces a "mandatory waiting" mechanism to avoid RTS-DATA collision while RSMA does not even have to utilize additional mechanism to avoid the RTS-DATA collision. Thus, we can say the channel division mechanism in DSMA-D protocol costs too much on RTS-DATA collision avoidance and is less attractive for real applications.

3. By comparing the throughput of DSMA-S and RSMA with an existing

DBTMA protocol, it is found that the DSMA-S and RSMA achieve slight performance improvement over DBTMA. Moreover, according to the access mechanism of DBTMA, in order to avoid the RTS-DATA collision, all RTS senders are required to perform three actions simultaneously: RTS transmission, BT_t broadcasting and busy tone sensing. More strict hardware is required in DBTMA to achieve a similar performance in DSMA-S and RSMA. If DBTMA is implemented in the network wherein RTS sender can not perform these three simultaneous transmissions, the RTS transmission may collide with DATA packet, and the network performance will degrade dramatically since DATA packet is usually much larger in size. Therefore, we can conclude that an idea MAC protocol should not require too much on the hardware devices.

4. RTS-RTS collision is usually very difficult to be completely avoided. In RSMA, the RTS-RTS collision is efficiently alleviated as the RTS transmission is partly protected by BT_t broadcasted at the receiver side. However this RTS protecting mechanism may induce a different problem. Since the BT_t is broadcasted as long as a RTS packet arrives, a RTS transmission will trigger several BT_t broadcasting around it. Then several terminals will be silenced because of that and the exposed terminal problem becomes worse. As a result, the RSMA is only suitable for the CR communication wherein the hidden terminal problem and packet collision avoidance is the most critical issue. As a summary, RSMA has excellent ability in dealing with the hidden terminal problem, but induces more serious exposed terminal problem. So we notice that there are tradeoffs between solving the hidden and exposed terminal problems.

Although the MAC protocols in wireless mesh access network is carefully designed to deal with packet collisions, energy wastage, etc., if there are terminals maliciously using the MAC protocols, the network performance will be dramatically harmed. Thus, we design a network performance, application and terminals monitoring framework for wireless mesh backbone network. The conventional network traffic flow concept is extended to the wireless mesh network and "Meshflow" is defined. "Meshflow" is able to collect the information such as source and destination addresses of packets, number of bytes, transport protocols, etc. The abnormal situation can be monitored in real-time by monitoring the "Meshflow" records. When the intrusion, attacking or misusing is detected, the attacker, zombie or selfish client can be located according to information contained in the "Meshflow" records.

8.2 Future Work

1. The transmission in wireless mesh access network is usually operated on a multi-hop basis before reaching the mesh router. So it is more attractive if the multi-hop capability is taken into account in designing and analyzing MAC protocol. The DSMA-D and DSMA-S protocols are designed for the one-hop client-to-client communication while the RSMA protocol is designed for the final hop client-to-router communication. One promising next step work is to comprehensively analyze the multi-hop (including at least a CC and CR link) end-to-end performance, including the throughput, access delay etc., when implementing DSMA on CC link and RSMA on CR link.

2. The MAC-physical cross layer design is having more and more attention in recent years. The DSMA and RSMA protocols can be further improved

if combined with physical layer characteristics to have interference adaptive or rate adaptive capabilities. For example, MAC protocols can be combined with the OFDM technology to simplify the random access procedure. In [108], each OFDM sub-channel state information is defined by channel gain. This information is exchanged between a transmitter and a receiver to help the transmitter make scheduling decisions. To improve our schemes, channel division scheme in DSMA-D can be easily achieved by assigning different OFDM sub-carriers to control and data channels. Moreover, by assigning different number sub-carriers to control/data channel, differentiated quality-of-service is supported to combat with the unstable channel condition. As a result, packet transmission rate is able to be dynamically adapted with the interference.

3. The Meshflow functionality is designed on a strategy level as the initial step. Although the implementation issues are discussed, existing research on this topic provides only the possibility of implementing Meshflow in a real application. To go one step further along the path, Meshflow software should be designed to enable Meshflow record generating, management and analysis. A hypothetic network (test bed) should be constructed with Meshflow software enabled on each mesh router. Then launch an attack (e.g. DoS flooding) to test the functionality and sensitivity of this Meshflow based network monitoring and protection methodology.

Appendix A: Collision Period Analysis

This part provides the collision period analysis of DSMA-D in the All-Hidden Sender Environment. According to the access mechanism of DSMA-D, RTS-DATA collision is avoided because of the channel separation, the DATA-DATA collision is also avoided because of the "double sense" mechanism. Thus, packet collision refers to the RTS-RTS collision. In the All-Hidden-Sender environment, RTS transmissions can not be protected by BT_t signals. As a result, the RTS collision period length ranges between $\gamma\tau$ and ∞.

As illustrated in Fig. A.1, γ slots collision period is induced by more than one RTS transmission attempt arrive within the same time slot, i.e. RTS-A and RTS-B arrive in the 10^{th} slot. The probability of this case is denoted by:

$$P\{B_f = \gamma\tau\} = \frac{e^{-\lambda\tau(\gamma-1)}(1 - e^{-\lambda\tau} - \lambda\tau \cdot e^{-\lambda\tau})}{1 - e^{-\lambda\tau}} \tag{A.1}$$

wherein $e^{-\lambda\tau(\gamma-1)}$ denotes there are no additional RTS arrives from 11^{th} to 13^{th} slot; and $(1 - e^{-\lambda\tau} - \lambda\tau \cdot e^{-\lambda\tau})$ denotes there are at least two RTS arrivals in the 10^{th} slot. For simplicity, we let $e^{-\lambda\tau(\gamma-1)} = \alpha$ and $e^{-\lambda\tau} = \beta$.

Fig. A.2 illustrates a $\gamma + 1$ slots collision period wherein RTS-A arrives in the 10^{th} slot and RTS-B arrives in the 11^{th}. The probability of this case is given by:

$$P\{B_f = (\gamma + 1)\tau\} = \frac{e^{-\lambda\tau(\gamma-1)}(1 - e^{-\lambda\tau})(1 - e^{-\lambda\tau})}{1 - e^{-\lambda\tau}} = \alpha(1 - \beta) \tag{A.2}$$

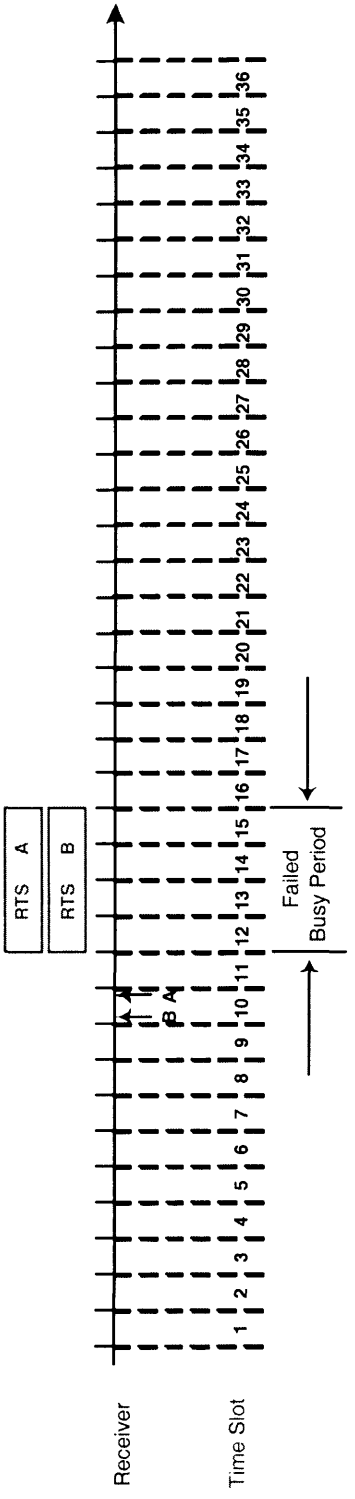

Figure A.1: γ Slots Collision Period.

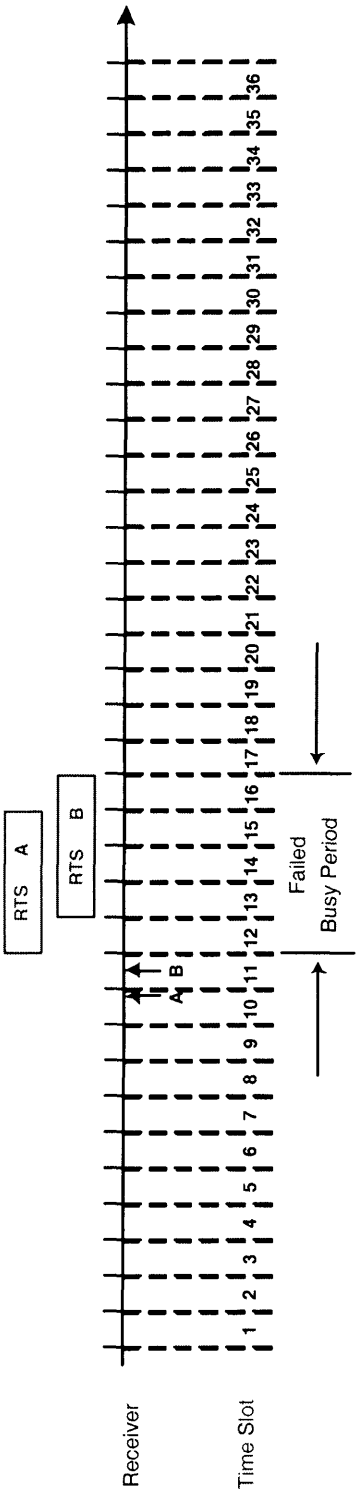

Figure A.2: $\gamma + 1$ Slots Collision Period.

wherein the first $(1 - e^{-\lambda\tau})$ denotes RTS-A arrives within 10^{th} slot, and similarly, the second $(1-e^{-\lambda\tau})$ denotes RTS-B arrives within 11^{th} slot. α $(=e^{-\lambda\tau(\gamma-1)})$ still denotes that there are no additional RTS arrivals to prolong the collision period. Note that the $(1 - \beta)$ $(=1 - e^{-\lambda\tau})$ indicates there is at lease one arrival one slot Thus, the $(1 - \beta)(1 - \beta)$ is able to denote the RTS-A and RTS-B arrive in the $(10^{th}, 11^{th})$, $(10^{th}, 12^{th})$ till $(10^{th}, 13^{th})$ slots. In other words, the equitation A.2 could also illustrate the scenarios of $B_f = (\gamma + 2)\tau$, $B_f = (\gamma + 3)\tau$ till $B_f = (2\gamma - 1)\tau$ shown in Fig. A.3. Thus we have:

$$\begin{aligned} P\{B_f = (\gamma + k)\tau\} &= e^{-\lambda\tau(\gamma-1)}(1 - e^{-\lambda\tau}) \\ &= \alpha \cdot (1 - \beta), \quad 1 \leq k \leq (\gamma - 1) \end{aligned} \tag{A.3}$$

When the length of fail period is prolonged to 2γ time slots, there is a 0 slot gap between RTS-A and RTS-B (Fig. A.4). If we want the fisrt and the last RTS belong to the same collision period, there have to be some other RTS arrivals to overlap with the two RTS, bridge them and make sure the collision peirod is consecutive.

It is shown from Fig. A.4 that the first and the last RTS are end to end, if there is no other RTS signals to bridge them, there will be 0 slot gap between them. We let the P_i denotes the probability of bridging the two i slots' gap. The probability of 2γ slots collision period is known as:

$$P\{B_f = 2\gamma\tau\} = e^{-\lambda\tau(\gamma-1)}(1 - e^{-\lambda\tau}) \cdot P_0 \tag{A.4}$$

We let the situation that no arrival in a slot $(e^{-\lambda\tau} = \beta)$ is denoted by the number "0"; while "1" denotes that at least one arrival arrives in the time slot $(1 - e^{-\lambda\tau} = 1 - \beta)$. The possible cases of bridging are illustrated in Tab. A.1 which actually denotes that there is at least one RTS arrives within the $(\gamma - 1)$ slots. And bridging probability P_0 is given by:

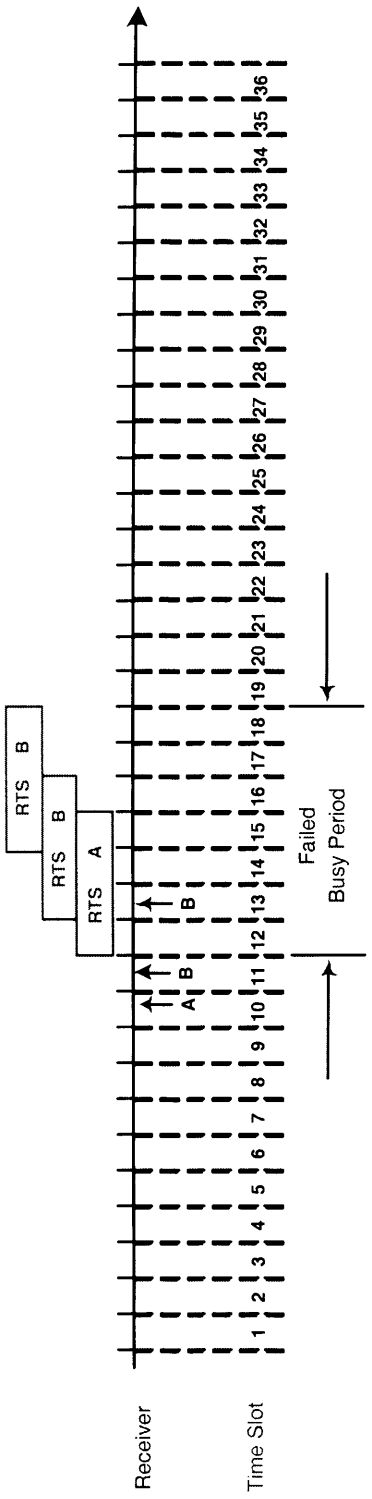

Figure A.3: $(\gamma + 2) \sim (2\gamma - 1)$ Slots Collision Period.

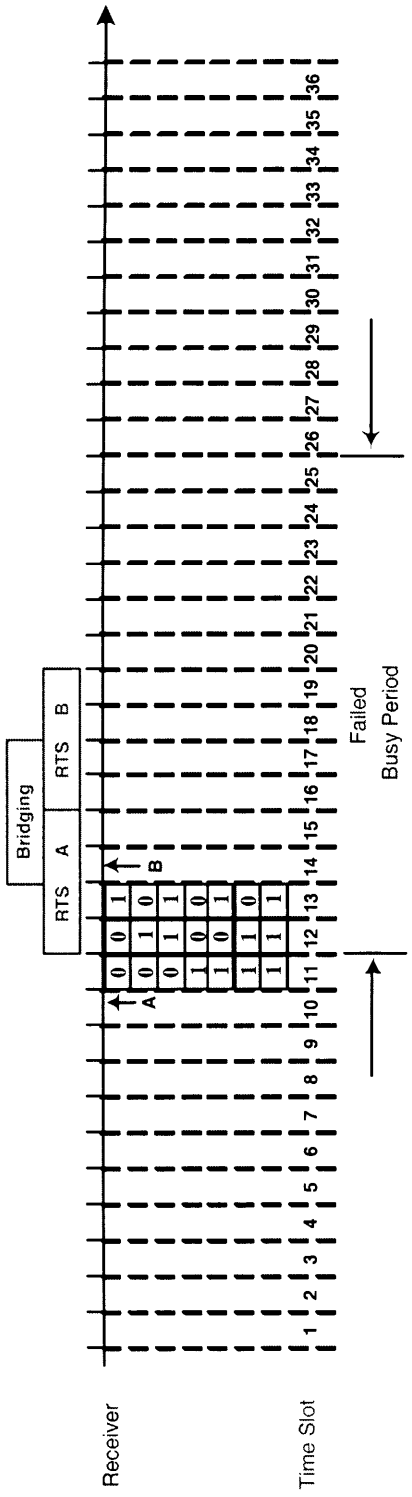

Figure A.4: 2γ Slots Collision Period.

Table A.1: Scenarios of P_0

P_0	Arrival	Arrival	Arrival
P_{01}	0	0	1
P_{02}	0	1	0
P_{03}	0	1	1
P_{04}	1	0	0
P_{05}	1	0	1
P_{06}	1	1	0
P_{07}	1	1	1

$$P_0 = 1 - e^{-\lambda\tau(\gamma-1)} = 1 - \alpha \tag{A.5}$$

When the gap between the first and the last RTS is prolonged to one time slot, the collision period becomes to $(2\gamma + 1)$ slots period. Compared with the 2γ slots scenario, one more time slot has to be bridged as shown in Fig. A.5.

"Case 1" in Fig. A.5 indicates there is at least one RTS arrival during the one more slot conditioned by probability P_0; "Case 2" indicates there is no RTS arrival during that slot conditioned by probability P_0. The combination of P_{04} (in Tab. A.1) and P_0 , i.e. P_{14} in Tab. A.2, will not bridge RTS-A and RTS-B.

And the bridging probability P_1 is given by:

$$\begin{aligned} P_1 &= P_0(1-\beta) + (P_0 - P_{04})\beta \\ &= P_0(1-\beta) + \beta(P_0 - \beta^2(1-\beta)) \\ &= P_0 - \beta^3(1-\beta) \\ &= P_0 - \alpha(1-\beta) \end{aligned} \tag{A.6}$$

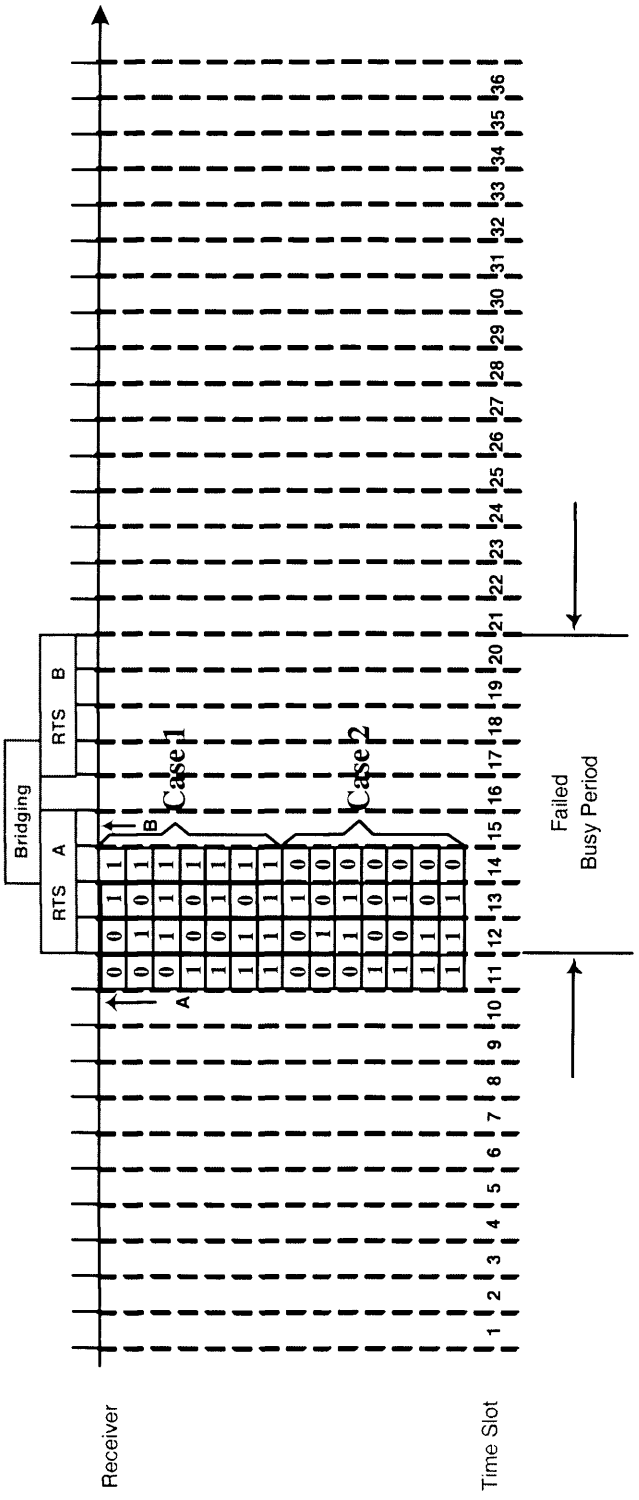

Figure A.5: $2\gamma + 1$ Slots Collision Period.

Table A.2: Scenarios of P_1

P_1	Arrival	Arrival	Arrival	Arrival
P_{11}	0	0	1	0
P_{12}	0	1	0	0
P_{13}	0	1	1	0
P_{14}	1	0	0	0
P_{15}	1	0	1	0
P_{16}	1	1	0	0
P_{17}	1	1	1	0
P_{18}	0	0	1	1
P_{19}	0	1	0	1
P_{110}	0	1	1	1
P_{111}	1	0	0	1
P_{112}	1	0	1	1
P_{113}	1	1	0	1
P_{114}	1	1	1	1

Table A.3: Scenarios of $P_{(\gamma-1)}$

$P_{(\gamma-1)}$	Arrival	Arrival	Arrival	Arrival
$P_{(\gamma-1)1}$	P_0	0	0	1
$P_{(\gamma-1)2}$	P_0	0	1	0
$P_{(\gamma-1)3}$	P_0	0	1	1
$P_{(\gamma-1)4}$	P_0	1	0	0
$P_{(\gamma-1)5}$	P_0	1	0	1
$P_{(\gamma-1)6}$	P_0	1	1	0
$P_{(\gamma-1)7}$	P_0	1	1	1

Similarly, $2\gamma + 2$ slots' collision period requires one more slot be bridged. And the probability of bridging the two slots' gap is given by:

$$\begin{aligned} P_2 &= P_1(1-\beta) + (P_1 - P_{14})\beta \\ &= P_1(1-\beta) + \beta(P_1 - \beta^2(1-\beta)) \\ &= P_1 - \beta^3(1-\beta) \\ &= P_1 - \alpha(1-\beta) \end{aligned} \tag{A.7}$$

Thus, the bridging probability can be summarized as:

$$P_k = P_{k-1} - \alpha(1-\beta) \quad 1 \le k \le (\gamma - 1) \tag{A.8}$$

Tab. A.3 lists the bridging case probability of the critical bridging case: $P_{(\gamma-1)}$ ($B_f = (3\gamma - 1)\tau$). As illustrates in Fig. A.6, the collision period will not be bridged if there is no arrival in the 17_{th} slot together with the $P_{(\gamma-1)4} = P_0 \cdot \beta^2(1-\beta)$ probability. Thus, the bridging probability of bridging γ slots gap is given by:

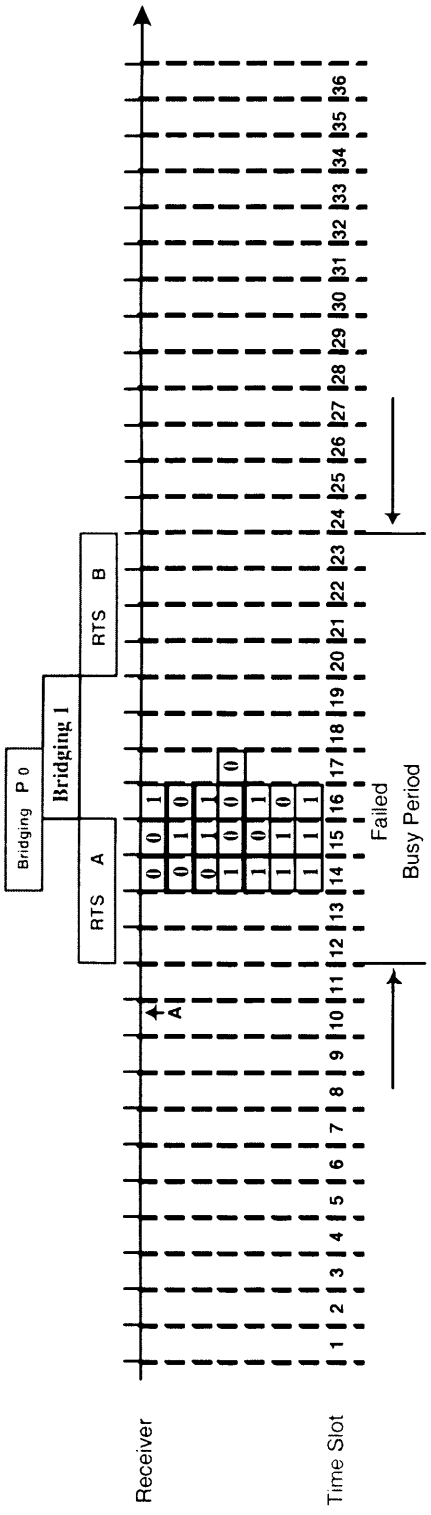

Figure A.6: $(\gamma - 1)$ Slots Gap.

$$\begin{aligned} P_\gamma &= P_{\gamma-1}(1-\beta) + (P_{\gamma-1} - P_0 \cdot P_{(\gamma-1)4})\beta \\ &= P_{\gamma-1}(1-\beta) + \beta(P_{\gamma-1} - \beta^2(1-\beta)P_0) \\ &= P_{\gamma-1} - \beta^3(1-\beta)P_0 \\ &= P_{\gamma-1} - \alpha(1-\beta)P_0 \end{aligned} \tag{A.9}$$

As the collision period is incremental from $3\gamma\tau$, the bridging probability is summarized as:

$$P_k = P_{k-1} - \alpha(1-\beta)P_{k-\gamma} \quad k \geq \gamma \tag{A.10}$$

Together with Equation A.8 and Equation A.5, P_k can be rewriten by:

$$P_k = \begin{cases} 1-\alpha & k = 0; \\ P_{k-1} - \alpha(1-\beta) & 1 \leq k \leq (\gamma-1); \\ P_{k-1} - \alpha(1-\beta)P_{k-\gamma} & k \geq \gamma; \end{cases} \tag{A.11}$$

And the corresponding collision period probability is given by:

$$P\{B_f = (2\gamma + k)\tau\} = \alpha(1-\beta) \cdot P_k \tag{A.12}$$

As a summary, the collision period length distribution is:

$$P\{B_f = (\gamma + i)\tau\} = \begin{cases} \frac{\left(1-e^{-\lambda\tau}-\lambda\tau \cdot e^{-\lambda\tau}\right) \cdot e^{-\lambda\tau(\gamma-1)}}{\left(1-e^{-\lambda\tau}\right)(1-p_s)}, & i = 0; \\ \frac{e^{-\lambda\tau(\gamma-1)} \cdot \left(1-e^{-\lambda\tau}\right) \cdot \alpha_i}{1-p_s}, & i \geq 1; \end{cases} \tag{A.13}$$

where p_s is the RTS successful probability and α_i (i≥1) is an interim variable and is defined as:

$$\alpha_i = \begin{cases} 1, & 1 \le i \le \gamma - 1; \\ 1 - e^{-\lambda\tau(\gamma-1)}, & i = \gamma; \\ \alpha_{i-1} - e^{-\lambda\tau(\gamma-1)} \cdot \left(1 - e^{-\lambda\tau}\right) \cdot \alpha_{i-\gamma}, & i \ge \gamma + 1. \end{cases} \tag{A.14}$$

As a check, $\sum_{i=0}^{\infty} P\{B_f = (\gamma + i)\tau\} = 1$.

Bibliography

[1] S. Toumpis and A. Goldsmith, "Ad Hoc Network Capacity," in *Proceedings of Thirty-Fourth Asilomar Conference on Signals, Systems and Computers*, vol. 2, pp. 1265-1269, 2000.

[2] Chee-Yee Chong, S.P. Kumar and Booz Allen Hamilton, "Sensor Networks: Evolution, Opportunities, and Challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247-1256, Aug. 2003.

[3] K. Rayner, "Mesh Wireless Networking" *IEEE Communications Engineer*, vol. 1, no. 5, pp. 44-47, Oct./Nov. 2003.

[4] T.M. Siep, I.C. Gifford, C. Braley and R.F. Heile, "Paving The Way for Personal Area Network standards: An Overview of the IEEE P802.15 Working Group for Wireless Personal Area Networks," *IEEE Personal Communications*, vol. 7, no. 1, pp. 37-43, Feb. 2000.

[5] B.P. Crow, I. Widjaja, L.G. Kim and P.T. Sakai, "IEEE 802.11 Wireless Local Area Networks," *IEEE Communications Magazine*, vol. 35, no. 9, pp. 116-126, Sept. 1997.

[6] IEEE 802.16 WiMAX Forum, [Online]: "`http://www.wimaxforum.org/home/`" Available Aug. 2007.

[7] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," *Computer Networks Journal (Elsevier)*, vol. 47, pp. 445-487, March 2005.

[8] Ashish Raniwala and Tzi-cker Chiueh, "Architecture and Algorithms for an IEEE 802.11-based Multi-channel Wireless Mesh Network," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, vol. 3, pp. 2223-2234, March 2005.

[9] Jangeun Jun and Sichitiu, M.L., "The Nominal Capacity of Wireless Mesh Networks," *Wireless Communications Magazine*, vol. 10, no. 5, pp. 8-14, Oct. 2003.

[10] A. Jain, A. Pruthi, R.C. Thakur and M.P.S. Bhatia, "TCP Analysis Over Wireless Mobile Ad Hoc Networks," in *Proceedings of IEEE International Conference on Personal Wireless Communications*, pp. 95-99, Dec. 2002.

[11] Nakjung Choi, Yongho Seok and Yanghee, "Choi Multi-channel MAC Protocol for Mobile Ad Hoc Networks," in *Proceedings of IEEE Vehicular Technology Conference*, vol. 2, pp. 1379-1382, Oct. 2003.

[12] A. Adya, P. Bahl, J. Padhye, A. Wolman and L. Zhou, "A Multi-Radio Unification Protocol for IEEE 802.11 Wireless Networks," in *Proceedings of IEEE First International Conference on Broadband Networks*, pp. 344-354, Oct. 2004.

[13] Choi Noun, Patel Maulin and Venkatesan S.,"A Full Duplex Multi-channel MAC Protocol for Multi-hop Cognitive Radio Networks," in *Proceedings of First International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, pp. 1-5, June 2006.

[14] F. Tobagi and L. Kleinrock, "Packet Switching in Radio Channels: Part II–The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution," *IEEE Transactions on Communications*, vol. 23, no. 12, pp. 1417-1433, Dec. 1975.

[15] A. Colvin, "CSMA With Collision Avoidance," *Computer Communication*, vol. 6, no. 5, pp. 227-235, 1983.

[16] IEEE 802.11 Working Group, [Online]: "http://www.ieee802.org/11," Available Aug. 2007.

[17] IEEE 802.11, [Online]: "http://en.wikipedia.org/wiki/802.11," Available Aug. 2007.

[18] IEEE 802.11 Standard, Part 11: Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specification: High-speed Physical Layer in the 5GHz Band, 1999.

[19] IEEE 802.11b Standard, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification: High-Speed Physical Layer Extension in the 2.4 GHz Band, 1999.

[20] IEEE 802.11g Standard, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, Amendment 4: Further Higher Data Rate Extension in the 2.4GHz Band, 2003.

[21] Yiyan Wu and W.Y. Zou, "Orthogonal Frequency Division Multiplexing: A Multi-carrier Modulation Scheme," *IEEE Transactions on Consumer Electronics*, vol. 41, no. 3, pp. 392-399, Aug. 1995.

[22] Theodore S. Rappaport, "Wireless Communications: Principles and Practice (Second Edition)," *Prentice Hall*, Dec. 2001.

[23] Sheldon M. Ross, "Introduction to Probability Models (Fourth Edition)," *Academic Press*, 1989.

[24] R. Scholtz, "The Origins of Spread-Spectrum Communications," *IEEE Transactions on Communications*, vol. 30, no. 5, pp. 822-854, May 1982.

[25] K. Halford, S. Halford, M. Webster and C. Andren, "Complementary Code Keying for RAKE-based Indoor Wireless Communication," in *Proceedings of IEEE International Symposium on Circuits and Systems*, vol. 4, pp. 427-430, July 1999.

[26] M.A. Visser, M. El Zarki, "Voice and Data Transmission Over an 802.11 Wireless Network," in *Proceedings of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, vol. 2, pp. 648-652, Sept. 1995.

[27] J.W. Roberts, "Traffic Theory and the Internet," *IEEE Communications Magazine*, vol. 39, no. 1, pp. 94-99, Jan. 2001.

[28] D. Har, H.H. Xia and H.L. Bertoni, "Path-loss Prediction Model for Microcells," *IEEE Transactions on Vehicular Technology*, vol. 48, no. 5, pp. 1453-1462, Sept. 1999.

[29] A. Saleh and R. Valenzuela, "A Statistical Model for Indoor Multipath Propagation," *IEEE Journal on Selected Areas in Communications*, vol. 5, no. 2, pp. 128-137, Feb. 1987.

[30] Wei Ye, "Radio Propagation Models," Chapter 17, NS Manual, [Online]: "`http://www.isi.edu/~weiye/pub/propagation_ns.pdf`," Available Aug. 2007.

[31] Tzu-Jane Tsai and Ju-Wei Chen, "IEEE 802.11 MAC Protocol Over Wireless Mesh Networks: Problems and Perspectives," in *Proceedings of 19th International Conference on Advanced Information Networking and Applications*, vol. 2, pp. 60-63, March 2005.

[32] P. Karn, "MACA - a New Channel Access Method for Packet Radio," in *Proceedings of ARRL/CRRL Amateur Radio 9th Computer Networking Conference*, pp. 134-140, 1990.

[33] V. Bharghavan, A. Demers and S. Shenker and L. Zhang, "MACAW: a Medium Access Protocol for Wireless LANs," in *Proceedings of ACM Special Interest Group on Data Communication (SIGCOMM) Conference*, vol. 24, no. 4, pp. 212-225, 1994.

[34] C. L. Fullmer and J. J. Garcia-Luna-Aceves, "Floor Acquisition Multiple Access (FAMA) for Packet Radio Networks," in *Proceedings of ACM Special Interest Group on Data Communication (SIGCOMM) Conference*, vol. 25, no. 4, pp. 262-273, 1995.

[35] A. Qayyum, M.U. Saleem, Tauseef-Ul-Islam, M. Ahmad and M.A. Khan, "Performance Increase in CSMA/CA with RTS-CTS," in *Proceedings of 7th International Multi Topic Conference*, pp. 182-185, 2003.

[36] Yang Yang, Feiyi Huang, Xuanye Gu, Mohsen Guizani, and Hsiao-Hwa Chen, "Double Sense Multiple Access for Wireless Ad Hoc Networks," *Computer Networks (Elsevier)*, vol. 51, no. 14, pp. 3978-3988, Oct. 2007.

[37] F. Talucci, M. Gerla and L. Fratta, "MACA-BI (MACA By Invitation)-a receiver Oriented Access Protocol for Wireless Multihop Networks," in *Pro-*

ceedings of The 8th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, vol. 2, pp. 435-439, Sept. 1997.

[38] J. J. Garcia-Luna-Aceves and Asimakis Tzamaloukas, "Receiver-initiated Collision Avoidance in Wireless Networks," *Wireless Networks*, vol. 8, no. 2/3, pp. 249-263, March-May 2002.

[39] A. Tzamaloukas and J.J. Garcia-Luna-Aceves, "A Receiver-initiated Collision-avoidance Protocol for Multi-channel Networks," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM)* vol. 1, pp. 189-198, 2001.

[40] Z. J. Haas and J. Deng, "Dual Busy Tone Multiple Access (DBTMA) – a Multiple Access Control Scheme for Ad hoc Networks," *IEEE Transactions on Communication*, vol. 50, no. 6, pp. 975-985, June 2002.

[41] Supeng Leng, Liren Zhang and Yifan Chen, "IEEE 802.11 MAC Protocol Enhanced by Busy Tones," in *Proceedings IEEE International Conference on Communications*, vol. 5, pp. 2969-2973, May 2005.

[42] Qi He, Lin Cai, Xuemin Shen and Pinhan Ho, "Improving TCP performance over Wireless Ad Hoc Networks with Busy Tone Assisted Scheme," *EURASIP Journal on Wireless Communications and Networking*, vol. 2006, no. 2, pp. 1-11, April 2006.

[43] Wang Ping, Jiang Hai and Zhuang Weihua, "A Dual Busy-Tone MAC Scheme Supporting Voice/Data Traffic in Wireless Ad Hoc Networks," in *Proceedings of IEEE Global Telecommunications Conference*, pp. 1-5, Nov. 2006.

[44] Yang Yang, Feiyi Huang, Xuanye Gu, Mohsen Guizani, and Hsiao-Hwa Chen, "Double Sense Multiple Access for Wireless Ad Hoc Networks," in *Proceedings of The Third International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QShine)*, August 2006.

[45] Ying Li, Minglu Li and Min-You Wu, "An Interference-Aware Busy Tone Based MAC Protocol," in *Proceedings of IEEE 65th Vehicular Technology Conference*, pp. 36-40, April 2007.

[46] M.J. Miller, N.H. Vaidya, "A MAC Protocol Reduce Senseor Network Energy Consumption Using a Wakeup Radio," *IEEE Transactions on Mobile Computing*, vol. 4, no. 3, pp. 228-242, May/June 2005.

[47] Feiyi Huang and Yang Yang, "Energy Aware Collision Avoidance MAC protocol for Hybrid Multi-hop Networks," in *Proceedings of ACM Wireless Communications and Mobile Computing Conference*, August, 2007.

[48] Feiyi Huang and Yang Yang, "Receiver Sense Multiple Access Protocol for Wireless Mesh Access Networks," in *Proceedings of IEEE International Conference on Communications* pp. 3764-3769, June, 2007.

[49] R.L. Borchardt and T.T. Ha, "Power capture ALOHA," in *Proceedings of IEEE Military Communications Conference*, vol. 2, pp. 703-707, Oct. 1988.

[50] M. Stemm and R. H. Katz, "Measuring and Reducing Energy Consumption of Network Interfaces in Hand-held Devices," *IEICE Transactions on Communications*, vol. E80-B, no. 8, pp. 1125-1131, 1997.

[51] Christine E. Jones, Krishna M. Sivalingam, Prathima Agrawal and Jyh-Cheng Chen, "A Survey of Energy Efficient Network Protocols for Wireless Networks," *Wireless Networks*, vol. 7, no. 4, pp. 343-358, 2001.

[52] J.-C. Chen, K.M. Sivalingam and P. Agrawal, "Performance Comparison of Battery Power Consumption in Wireless Multiple Access Protocols, " *Wireless Networks* vol. 5, no. 6, pp. 445-460, 1999.

[53] H. H. Chen and W. T. Tea, "Performance of Hierarchy Schedule Sensing Protocol for Distributed Ad Hoc CDMA Networks under Multiple Packet Collision and Capture Effect," *IEEE/ACM Transactions on Networking*, vol. 12, pp. 1036-1048, Dec. 2004.

[54] Wei Ye, John Heidemann and Deborah Estrin, "An Energy-Efficient MAC protocol for Wireless Sensor Networks," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, pp. 1567-1576, June 2002.

[55] L. Roberts,"ALOHA Packet System with and without Slots and Capture," *ACM SIGCOMM Computer Communication Review*, vol. 5, no. 2, pp. 28-42, 1975.

[56] Suresh Singh and C. S. Raghavendra, "PAMAS – Power Aware Multi-access Protocol with Signalling for Ad Hoc Networks," *ACM SIGCOMM Computer Communication Review*, vol. 28, no. 3, pp. 5-26, 1998.

[57] Eun-Sun Jung and Nitin H. Vaidya, "A Power Control MAC Protocol for Ad Hoc Networks," *Wireless Networks*, vol. 11, no. 1-2, pp. 55-66, Jan. 2005.

[58] Shih-Lin Wu, Yu-Chee Tseng and Jang-Ping Sheu, "Intelligent Medium Access for Mobile Ad Hoc Networks with Busy Tones and Power Control," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 9, pp. 1647-1657, Sept. 2000.

[59] Jung-Won Kim and N. Bambos, "Power-efficient MAC Scheme Using Channel Probing in Multi-rate Wireless Ad Hoc Networks," in *Proceedings of IEEE Vehicular Technology Conference*, vol. 4, pp. 2380-2384, 2002.

[60] Agarwal S., Katz R.H., Krishnamurthy S.V. and Dao, S.K., "Distributed Power Control in Ad Hoc Wireless Networks," in *Proceedings of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, vol. 2, pp. 59-66, Sept/Oct 2001.

[61] Cesana M., Maniezzo D., Bergama P. and Gerla M., " Interference Aware (IA) MAC: an Enhancement to IEEE 802.11 DCF," in *Proceedings of IEEE Vehicular Technology Conference*, vol. 5, pp. 2799-2803, Oct. 2003.

[62] B.S. Kim, Yuquang Fang and T.F. Wong, "Rate-adaptive MAC Protocol in High-rate Personal Area Networks," in *Proceedings of IEEE Wireless Communications and Networking Conference*, vol. 3, pp. 1394-1399, March 2004.

[63] Martin Burkhart, Pascal von Rickenbach, Roger Wattenhofer and Aaron Zollinger, "Does Topology Control Reduce Interference?," in *Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 9-19, 2004.

[64] Tomas Johansson and Lenka Carr-Motykov, "Reducing Interference in Ad Hoc networks Through Topology Control," in *Proceedings of the 2005 joint Workshop on Discrete Algothrithms and Methods for MOBILE Computing and Communications*, pp. 17-23, 2005.

[65] R. Wattenhofer, L. Li, P. Bahl and Y.-M. Wang, "Distributed Topology Control for Power Efficient Operation in Multihop Wireless Ad Hoc Networks,"

in *Proceedings of IEEE Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3, pp. 1388-1397, 2001.

[66] Xiaohua Jia, Deying Li and Dingzhu Du, "QoS Topology Control in Ad Hoc Wireless Networks," in *Proceedings of IEEE Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, vol. 2, pp. 1264-1272, March 2004.

[67] Cheng-Fu Chou and Hsien-Ping Suen, "Topology Control Based QoS Routing (TLQR) in Wireless Ad Hoc Networks," in *Proceedings of IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1-5, Sept. 2006.

[68] Cisco IOS Netflow, [Online]: "http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html" Available Aug. 2007.

[69] Juniper cflowd, [Online]: "http://www.juniper.net/techpubs/software/junos/junos70/swconfig70-policy/html/sampling-summary6.html#1076566" Available Aug. 2007.

[70] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields and E. M. Belding- Royer, "A Secure Routing Protocol for Ad Hoc Networks," in *Proceedings of IEEE International Conference on Network Protocols*, pp. 78-87, 2002.

[71] P. Kyasanur and N. H. Vaidya, "Selfish MAC Layer Misbehavior in Wireless Networks," *IEEE Transactions on Mobile Computing*, vol. 4, no. 5, pp. 502-516, Sept/Oct 2005.

[72] A. Perrig, R. Canetti, D. Tygar, and D. Song, "The TESLA Broadcast

Authentication Protocol," *RSA Cryptobytes*, vol. 5, no. 2, pp. 2-13, Summer/Fall 2002.

[73] Ping Yi, Zhoulin Dai, Shiyong Zhang and Yiping Zhong, "A New Routing Attack in Mobile Ad Hoc Networks," *International Journal of Information Technology*, vol. 11, no. 2, pp. 83-94, 2004.

[74] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Ad Hoc Network Journal (Elsevier), Special Issue on Sensor Network Applications and Protocols*, vol. 1, no. 2-3, pp. 293-315, Sept. 2003.

[75] David B. Johnson, David A. Maltz and Yih-Chun Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," Internet-Draft, [Online]: "`http://www.pataroo.net/ietf/all-ids/draft-ietf-manet-dsr-10.txt`", Available July 2004.

[76] Charles E. Perkins, Elizabeth M. Belding-Royer and Ian D. Chakeres, "Ad Hoc On-Demand Distance Vector (AODV) Routing," Internet-Draft, [Online]: "`http://moment.cs.ucsb.edu/pub/draft-perkins-manet-aodvbis-00.txt`", Available Oct. 2003.

[77] Charles Perkins and Pravin Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," in *Proceedings of ACM Special Interest Group on Data Communication (SIGCOMM) Conference*, pp. 234-244, 1994.

[78] Philippe Jacquet, Pascale Minet, Anis Laouiti, Laurent Viennot, Thomas Clausen and Cedric Adjih, " Multicast Optimized Link State Routing

(OLSR) Protocol," Internet-Draft, [Online]: "http://hipercom.inria.fr/olsr/draft-ietf-manet-olsr-molsr.txt", Available Nov. 2001.

[79] ANSI/IEEE Standard 802.1D, [Online]: "http://standards.ieee.org/getieee802/download/802.1D-2004.pdf", Available 2004.

[80] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking*, pp. 255-265, 2000.

[81] Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Defense Against Wormhole Attacks in Wireless Networks," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, pp. 1976-1986, 2003.

[82] P. Papadimitratos, Z. J. Haas, " Secure Routing for Mobile Ad Hoc Networks," in *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, 2002.

[83] Yhi-Chun Hu, D. Johnson and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," *Ad Hoc Networks*, vol. I, pp. 175-192, 2003.

[84] Yhi-Chun Hu, Adrian. Perrig and D. Johnson, " Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks," in *Proceedings of ACM 8th International Conference on Mobile Computing and Networking*, Sept. 2002.

[85] B. Dahill, B. Levine and E. Royer and C. Shields, " A Secure Routing Protocol for Ad Hoc Networks," Technical Report 01-37, Department of Computer Science, University of Massachusetts, Aug. 2001.

[86] Manel Guerrero Zapata, "Secure Ad Hoc On-demand Distance Vector Routing," *ACM SIGMOBILE Mobile Computing and Communication Review*, vol. 6, no. 3, pp. 106-107, 2002.

[87] Manel Guerrero Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," in *Proceedings of 1st ACM workshop on Wireless Security*, pp. 1-10, 2002.

[88] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Network Magazine*, vol. 13, no. 6, pp. 24-30, November/December 1999.

[89] Felix Lau, Stuart H. Rubin, Michael H. Smith and Ljiljana Trajkovic, "Distributed Denial of Service Attacks," in *Proceedings of IEEE International Conference on Systems, Man, and Cybernetics*, pp. 2275-2280, Oct. 2000.

[90] A. D. Wood and J. A. Stankovic,"Denial of Sevice in Sensor Networks," *IEEE Computer*, vol. 35, no. 10, pp. 54-62, Oct. 2002.

[91] Jelena Mirkovic and Peter Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39-53, 2004.

[92] W. Eddy, "TCP SYN flooding attacks and common mitigations," [Online]: "`http://tools.ietf.org/html/draft-eddy-syn-flood-00`", Available Nov. 2005.

[93] B. Wu, J. Chen, J. Wu and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," Chapter 12, Wireless/Mobile Network Security, Springer, 2006.

[94] A. Yaar, A. Perrig and D. Song, "SIFF: A Stateless Internet Flow to Mitigate

DDoS Flooding Attacks," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 130-143, May 2004.

[95] H. Wang, D. Zhang and K. Shin, "Detecting SYN Flooding Attacks," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, vol. 3, pp. 1530-1539, 2002.

[96] J. L. Hammond and P. J. P. O'Reilly, "Performance Analysis of Local Computer Networks," *Addison-Wesley*, 1986.

[97] R. Rom and M. Sidi, "Multiple Access Protocols: Performance and Analysis," *Springer-Verlag*, 1990.

[98] L. Kleinrock, "Queuing Systems Volume 2: Computer Applications," *Jone Wiley and Sons*, 1976.

[99] Yang Yang and Tak-Shing Peter Yum, "Analysis of Random Access Channel in UTRA-TDD on AWGN Channel," *International Journal of Communication Systems*, vol. 17, pp. 179-192, Apr. 2004.

[100] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordinationfunction," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535-547, Mar. 2000.

[101] C. E. Shannon, "A Mathematical Theory of Communication," *The Bell System Technical Journal*, vol. 27, pp. 379-423, Oct. 1948.

[102] Yang Yang and Tak-Shing Peter Yum, "Analysis of Power Ramping Schemes for UTRA-FDD Random Access Channel," *IEEE Transactions on Wireless Communications*, vol. 4, no. 6, pp. 2688-2693, Nov. 2005.

[103] Yang Yang and Tak-Shing Peter Yum, "Delay Distributions of Slotted ALOHA and CSMA," *IEEE Transactions on Communication*, vol. 51, no. 11, pp. 1846-1857, Nov. 2003.

[104] F. Huang and L. He, "Method and Apparatus for Monitoring a Digital Network," British Telecommunications (BT) patent A30981, 2006, (European patent pending).

[105] J.C. Arnbak and W. van Blitterswijk, "Capacity of Slotted ALOHA in Rayleigh-fading Channels", *IEEE Journal on Selected Areas in Communications*, vol. 5, no. 25, pp. 261-269, Feb. 1987.

[106] D.J. Goodman and A.A.M. Saleh, "The Near/far Effect in Local ALOHA Radio Communications", *IEEE Transactions on Vehicular Technology*, vol. 36, no. 1, pp. 19-27, Feb. 1987.

[107] B. Hajek, A. Krishna and R.O. Lamaire, "On the Capture Probability for a Large Number of Stations", *IEEE Transactions on Communications*, vol. 45, no. 2, pp. 254-260, Feb. 1997.

[108] Taiwen Tang, Ketan Mandke, Chan-Byoung Chae, Heath, R.W. and Nettles S.M., "Multichannel Feedback in OFDM Ad Hoc Networks", *IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, vol. 2, pp. 701-706, Sept. 2006.