EXPLORING QOS AND SECURITY IN WIRELESS AD-HOC NETWORK

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF LE2I
AND THE COMMITTEE ON GRADUATE STUDIES
OF UNIVERSITE DE BOURGOGNE
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

SUN Donglai
February 2013

Abstract

Wireless Ad-hoc Network is an emerging communication technology over the last decade. As this kind of network can be easily implemented without requiring fixed infrastructures, it is considered as one of the most important solutions for building distributed wireless systems. Obviously, the physical channel in wireless ad-hoc network significantly distinguishes itself from the other existing networks. For example, fluctuations caused by unstable wireless channel are more severe. From an ordinary perspective, these characteristics are treated as disadvantages, and have to be eliminated in network design.

Burgeoning technology called physical layer security represents a completely subversive attitude to these issues. Unique physical channel is exploited to provide additional security guarantee. However, new problems are also introduced into the system. Transmission rate of links with physical layer security is largely restricted due to the overhead used for secure mechanism. Network performance (e.g., throughput and delay) is accordingly affected. Thus, QoS turns out to be a major concern in networks with physical layer security.

In this research, the focus is on the problem of how to guarantee QoS and physical layer security simultaneously in wireless ad-hoc networks. Since traditional solutions for QoS are always implemented in upper layers of the network structure, they can hardly provide full support to the new secure physical layer. Furthermore, as services without secure requirement still exist in the network, the coexistence of secure and regular physical layer has to be taken into consideration. These issues have set new demands of corresponding MAC layer scheduling protocols. Therefore, we summarize

the general characteristics of physical layer security technology, based on which SecDCF, a MAC layer scheduling framework is presented. An interface is also designed to enable the integration of different scheduling policies. Furthermore, diversified requirements from different scenarios are studied, and scheduling policies are then derived to be applied with SecDCF.

Corresponding numerical analysis and simulations are also carried out to evaluate our research. As a conclusion, it is illustrated in this dissertation that with elaborately designed MAC layer scheduling schemes, it is possible to exploit the rich physical layer characteristics for achieving both security and QoS in wireless ad-hoc networks.

Résumé

Le réseau sans-fil Ad-hoc est une technologie de communication qui a émergé au cours de la dernière décennie. Ce type de réseau peut être mis en œuvre facilement sans infrastructures fixes, et il est considéré comme l'une des solutions les plus utilisées pour la construction de systèmes distribués. De toute évidence le canal physique du réseau sans-fil ad-hoc se distingue nettement des autres réseaux existants. Par exemple, les fluctuations causées par un canal sans-fil instable sont plus sévères. Du point de vue ordinaire, ces caractéristiques sont considérées comme des inconvénients, et doivent être éliminées dans la conception du réseau.

La technologie appelée "sécurité de la couche physique" représente une attitude tout à fait subversive par rapport à ces questions. L'unique canal physique est exploité pour fournir une garantie de sécurité supplémentaire. Cependant de nouveaux problèmes sont également introduits dans le système. La vitesse de transmission des liens avec la sécurité de la couche physique est limitée en raison de la surcharge utilisée pour le mécanisme sécurisé. Donc les performances du réseau (par exemple le débit et le délai) sont affectées. Ainsi, la qualité de service se révèle être une préoccupation majeure dans les réseaux avec sécurité de la couche physique.

Dans cette recherche, l'accent est mis sur la question de savoir comment garantir la QoS et la sécurité de la couche physique sans fil simultanément dans les réseaux ad-hoc. Comme les solutions traditionnelles de QoS sont toujours mises en œuvre dans les couches supérieures de la structure du réseau, elles ne fonctionnent pas bien avec la nouvelle couche physique sécurisé. En outre, comme il y a les autres services qui ne demandent pas plus de sécurité dans le réseau, la coexistence de la couche physique sécurisée avec la couche physique régulière doit être prise en considération.

Ces questions ont établi de nouvelles exigences de protocoles dans la couche MAC. Par conséquent nous résumons les caractéristiques générales de la technologie sécurité de couche physique, sur la base duquel un cadre de planification de couche MAC est présenté : SecDCF. Une interface est également conçue pour permettre l'intégration de politiques d'ordonnancement différentes. En outre les exigences diversifiées de scénarios différents sont étudiées, et des politiques d'ordonnancement sont ensuite dérivées pour être appliquées avec SecDCF.

Les analyses numérique et les simulations correspondantes sont également menées pour évaluer notre recherche. En conclusion il est illustré dans cette thèse que, avec une ordonnancement special dans la couche MAC, il est possible d'exploiter les caractéristiques riches de la couche physique pour atteindre la sécurité et la qualité de service en même temps dans les réseaux sans-fil ad-hoc.

Acknowledgements

I would like to thank my parents and my grandparents, who gave me life, and have supported me since then. I would like to thank my advisor, Prof. MIKOU Noufissa and Prof. Li Jianhua for their supervising. Many thanks to Prof. SAKHO Ibrahima, Prof. BUSSON Anthony for their kind review. Also many thanks to Prof. WU Yue and Prof. BENABOUD Hafssa for helping me improving my thesis and for being in the jury. My teacher and friends, Xiaole, Alain, Dominique, Thomas, Blandine, Ken, Francois, Jacque, Francoise, Bernard and Martine, I would like to thank you a lot for your support. You treat me like a family member in the past several years, and I truly believe that Dijon is now a second hometown for me in my whole life time. All my teachers and friends in China, Prof. ZHANG Zhigang, GJ, Haijing, and many other people, thank you.

This thesis is under an international cooperative research program of Université de Bourgogne, France and Shanghai Jiao Tong University, China.

The research presented in this thesis is supported by:
"Research on Security and Trust of Vehicular Opportunistic Networks"
From "National Science Foundation of China" (No: 61271220);
"Research on Fundamental Theory of Security Characteristics for Wireless Ad Hoc Networks" From "National Science Foundation of China" (No: 60932003);
"Protocols and Architecture of the Future Internet Communications(PACIFIC)"
From "National Science Foundation of China" and "Le Centre National de la Recherche Scientifique" (NSFC-CNRS) International Cooperation and Exchange Project

(No: 61211130104);
Funding(2010-9201AAO048S06493) from Regional Council of Bourgogne.

Contents

List of Tables

List of Figures

List of Acronyms

QoS	Quality of Service
MAC	Media Access Control
OSI	Open Systems Interconnection
SecDCF	Secure Distributed Controlling Function
QSOS	QoS-Secure-oriented Opportunistic Scheduling
TEOS	Threshold Enabled Opportunistic Scheduling
VANET	Vehicular Ad-hoc Network
IEEE	Institute of Electrical and Electronics Engineers
PRNETs	Packet Radio Networks
SURAN	Survivable Adaptive Network
DARPA	Defense Advanced Research Projects Agency
MANET	Mobile ad-hoc networks
WMN	Wireless mesh networks
WSN	Wireless sensor networks
DSSS	Direct Sequence Spread Spectrum
OFDM	Orthogonal Frequency Division Multiplexing

MIMO	Multi-input Multi-output
RSSI	Received Signal Strength Indication
PHY	Physical Layer
DCF	Distributed Coordination Function
AWGN	Additional White Gaussian Noise
SNR	Signal Noise Ratio
CSMA	Carrier Sensing Multiple Access

Chapter 1

Introduction

Motivation

Wireless Ad-hoc Network Technology was proposed firstly in the 1990s to fulfill the raising demands of distributed wireless communication systems. As it can be constructed rapidly without fixed infrastructures, and also for its wide possibilities in varied applications, e.g., environmental monitoring and emergency rescue, this technology became an attractive topic and has remained a significant research domain since then[1][2].

For the past decade, research community has made great efforts to tap the potential of this technology. Mechanisms, protocols and hardwares have been proposed for constructing practicable wireless ad-hoc systems[3][4]. However, as this technology is required in diversified application scenarios, strong needs exist not only in network construction, but also in providing high service quality. At the time of this writing, we can see that the research community and the industrial companies start to move forward. How to provide high-quality services in these networks becomes an imperative subject[5].

As for the matters of service providing, emphasis is always placed on two major issues: security and QoS. Security has been researched as a vital subject since the initial establishment of network system. In wireless communication, the unstable and open transmission medium complicates the situation. On the other hand, security is

not a simple question, but involves all layers of the network structure[6]. Therefore, literatures concerning messages encryption, authentication mechanism, secure routing protocol and many other research topics have been published, which highly improved the secrecy of wireless ad-hoc networks[7][8].

QoS is another important subject in wireless ad-hoc research. Unpredictable fluctuations of physical channel can severely affect the realtime performance, and multi-hop topology makes the link condition more delicate than that in single-hop networks. However, researchers have worked on solutions by following different models like DiffServ and IntServ. Another example in QoS research in wireless ad-hoc network is to combine QoS with traditional routing protocols, which can be found in studies like [9] and [10].

Apparently, achievements are praiseworthy for solving security and QoS problems in wireless ad-hoc network, but research is becoming trivial since the upper layers of OSI model have been earnestly studied for more than a decade. Then where can we find new growth point to the burgeoning demands? Recent researches, e.g., physical layer security[11] and opportunistic scheduling[12], show us that there exist some kind of potential in physical layer and MAC layer. Our research is carried out in this research domain.

Major Contributions

Our research starts from studying physical layer security technology. After examining this new concept in wireless ad-hoc network, we find that a severe degradation of throughput performance is unavoidable due to the large overhead for guaranteeing security. On the other hand, regular physical layer is still in need for those communications without security requirement, which means links with different physical channels coexist in the network. To adapt to these two alterations, we design a MAC layer scheduling framework to handle the new multi-physical-channel problem; and special opportunistic scheduling policies are then studied to tackle the throughput and QoS issue.

Simply speaking, this literature concludes our research work with four major contributions as follows:

1. **SecDCF: A MAC Layer Scheduling Framework That Can Support Both Physical Layer Security and Opportunistic Scheduling** [1].

   We design a MAC layer scheduling framework called SecDCF (Secure Distributed Controlling Function) in order to support physical layer security and opportunistic scheduling in wireless ad-hoc network. General characteristics of physical layer security technology are summarized, and support for potential secure physical layer is considered. In addition, a special interface for integrating opportunistic scheduling policies into this framework is also designed.

2. **QSOS: Achieving Overall Throughput Optimization and Fairness in Wireless Ad-hoc Networks with Physical Layer Security**[2].

   Considering a network with both secure physical layer and regular physical layer, links with completely different channel condition coexist in the network. QoS is more difficult to be achieved comparing to common wireless networks. Thus, mechanism called QSOS (QoS-Secure-oriented Opportunistic Scheduling) is designed to provide throughput optimization and fairness among different links. Corresponding policy is simulated and verified in SecDCF to show the merits of QSOS over traditional scheduling schemes in this new scenario.

3. **TEOS: Exploiting Multiuser Diversity to Guarantee QoS under Individual Throughput Requirement** [3].

   In a more general scheduling case, individual requirements of each link are also an important factor. To this end, a new scheduling mechanism called TEOS (Threshold Enabled Opportunistic Scheduling) is designed to guarantee the throughput performance for each link. A supplementary mechanism is also invented to judge if a set of throughput requirements can be achieved with

[1] The name SecDCF is derived from a published paper [13], and this part of research have evolved from the idea depicted in paper [13]

[2] This part of research partially appears in paper [14] and [15].

[3] This part of research partially appears in a submitted paper [16].

opportunistic scheduling. Similarly, TEOS can also be integrated to SecDCF framework.

4. **Sparing Channel for Time-critical Communications: using TEOS to improve VANET QoS**[4].

   In VANET, we consider two types of traffic: time-critical traffic and non-time-critical traffic. TEOS is used to reduce the transmission time of non-time-critical traffic, while throughput requirements are still guaranteed. Thus, delay of time-critical traffic is reduced. Numerical results and simulations show that our scheme outperforms the other scheduling schemes in providing better delay performance for time-critical traffic while rarely affecting the performance of non-time-critical traffic.

Organization of Thesis

The Introduction chapter states the motivations of our research. Major contributions are presented to provide a general idea of our research work. Structure of the dissertation is also given in the chapter.

The second chapter demonstrates wider appreciation. Recent developments of related research topics are provided to give a comprehensive understanding of the importance of our research. The fundamental technologies used to support our research, e.g., physical layer security and opportunistic scheduling, are also introduced for further reading.

In the following chapter, our research contributions are demonstrated. The third chapter presents the design of SecDCF; QSOS is discussed in the fourth chapter; in the fifth and sixth chapter, the design and utilization of TEOS is illustrated. Detailed analysis and simulations are carried on in each chapter to evaluate our research work.

The last chapter concludes the whole dissertation.

Chapter 2

Exploiting Physical Layer to Guarantee Wireless Ad-hoc Network Security and QoS: Challenges and Solutions

2.1 A General Introduction of Wireless Ad-hoc Network

2.1.1 The Developing Ad-hoc Network Technology

"Ad-hoc" is a Latin expression that describes a system or an organization established for a special purpose. It was used in the term "wireless ad-hoc network" to show the specificity of the distributed wireless network at the very beginning of its invention. However, similar network structures were applied in many other projects, and this term was then accepted by IEEE (Institute of Electrical and Electronics Engineers) as the name of a whole category of decentralized wireless systems. Unlike the preexisting infrastructures that are used in wired networks (routers) and Wi-Fi networks (access points), all the devices in wireless ad-hoc networks are free to connect or disconnect

to the network system. To support this dynamic topology, nodes in the network have to maintain a real-time link table for routing convergence at any time. Thus, connectivity can be always reestablished immediately after the alteration of topology. In a word, this technology provides possibilities in establishing a robust wireless network for varied applications.

The idea of wireless ad-hoc network was firstly proposed for the military usage. It derived from the PRNETs (Packet Radio Networks) project and SURAN (Survivable Adaptive Network) project[17], which were supported by DARPA(Defense Advanced Research Projects Agency) of USA. As wireless communication technology quickly developed in the late 1990s, wireless ad-hoc network was no longer unattainable for the civil society. Nowadays, applications like environmental sensoring system, wireless backup system and emergency reaction system are implemented all over the world. Wireless ad-hoc network technology becomes a convincing example of the transformation from military technology to civil utilities. An example of cooperate area network is shown in Fig. 2.1.

Although a variety of ad-hoc applications are used in different areas, we can still summarize their common characteristics as follows:

- Self-organized

  All nodes in wireless ad-hoc network are supposed to be able to connect with other nodes, and can form a network system by themselves after any alteration of network topology. This self-organized character can guarantee the system construction in start-up phase, and can also provide system recovery in any other occasion.

- Decentralized

  There is no centric node in wireless ad-hoc network, which means all nodes are equal. Thus, malfunction of some nodes do not affect the functionality of the whole network system. This characteristic provides strong robustness in applications.

- Multi-hop

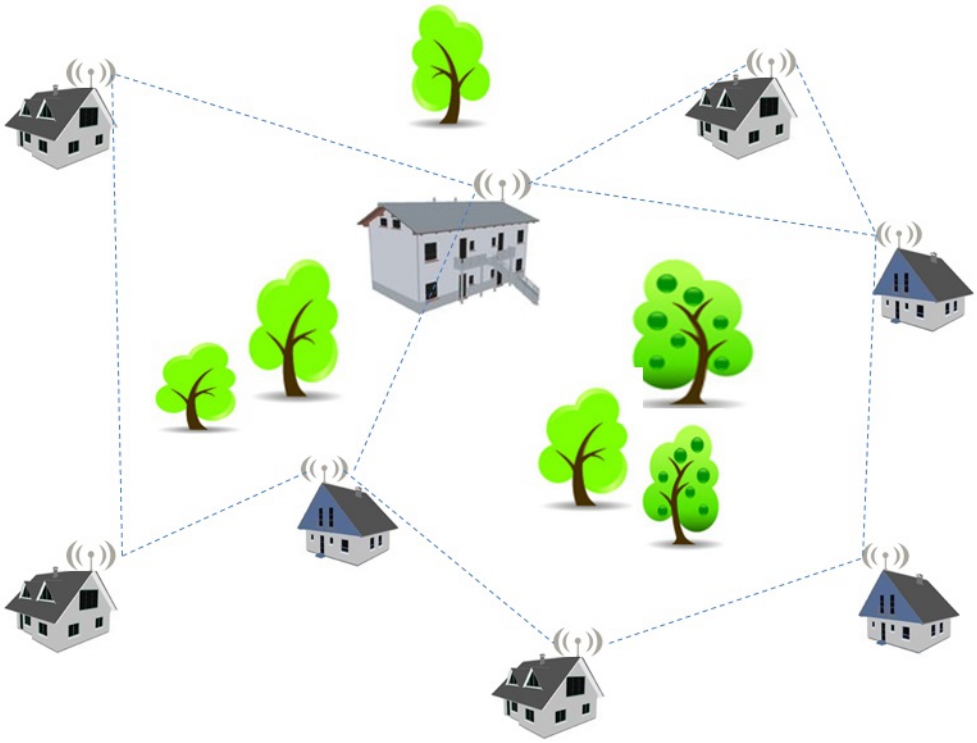

Figure 2.1: Cooperative Area Ad-hoc Network: An Example of Wireless Ad-hoc Network Applications

As the propagation range is limited in wireless communication, a multi-hop transmission is the only solution for a distributed network. A self-organized and decentralized routing protocol is desired. All the devices are capable of forwarding packets in the network. This function provides high connectivity in applications.

According to the application scenarios and features, some of the wireless ad-hoc networks can be further categorized. These special forms of wireless ad-hoc network all share the same basic concept, but has more stringent requirements on certain aspects. We provide the most recognized forms of wireless ad-hoc network as examples:

- **Mobile ad-hoc networks (MANET)** Comparing to traditional concept of wireless ad-hoc network, nodes in MANET are free to move at any direction.

Thus, the topology changes more frequently. Unstable connectivity is the major challenge in MANET. Vehicular Ad-hoc Networks (VANETs) is also a special form of MANET.

- **Wireless mesh networks (WMN)** WMN often has organized and layered structure. Within the layer, nodes and devices are allowed to form a self-organized network, while planned connections are implemented between layers. This structure helps provide dynamic but cost effective connectivity.

- **Wireless sensor networks (WSN)** WSN is always used to describe the sensoring networks used in large area with large quantity of sensors. Large-scale complexity and power efficiency are the major problems which distinguish WSN from the other wireless ad-hoc networks.

2.1.2 Physical Layer of Wireless Ad-hoc Network

Wireless ad-hoc network is a technique for constructing network system, then it can be applied to any kind of wireless devices. That's why there are researches about designing wireless ad-hoc networks with almost all the physical layer realizations, e.g., IEEE 802.11 (Wi-Fi), IEEE 802.15 (Bluetooth and ZigBee), IEEE 802.16 (WiMAX). Some of these researches have already been standardized and can be found in corresponding entries of IEEE standards.

With different physical layer, different frequencies and modulation technologies are used. For example, the frequency channel of 2.4Ghz and 5Ghz are used in Wi-Fi. In the early stage of 802.11b, DSSS (Direct Sequence Spread Spectrum) is applied. The advanced OFDM (Orthogonal Frequency Division Multiplexing) is chosen in 802.11g for providing high-speed wireless communication.

Although diversified physical layer standards may change the implementation methods of wireless ad-hoc applications, the constitution still determines the major characters as depicted in the above section, e.g., open channel and large channel uncertainties. These characteristics are always considered as disadvantages, because they lead to deleterious consequences in the communication procedure. A major task in traditional wireless research is to eliminate these uncertainties. However,

new technology (e.g., physical layer security and opportunistic scheduling) shows the possibility of exploiting it.

2.1.3 MAC Layer of Wireless Ad-hoc Network

MAC Layer is the bottom sub-layer of Data Link layer in OSI Model, as shown in Fig.2.2. In most wireless realizations, shared medium is applied because of the limited frequency resource. Therefore MAC layer plays a key role in connecting physical layer and the other parts of network system. Generally speaking, tasks related to physical channel (i.e., medium resource allocation, intercommunication and interference prevention among all the nodes) are handled in MAC layer. In wireless ad-hoc network, scheduling difficulties aggravate due to the dynamic topology. As a result, designing corresponding MAC layer scheduling schemes is considered important in research of wireless ad-hoc network.

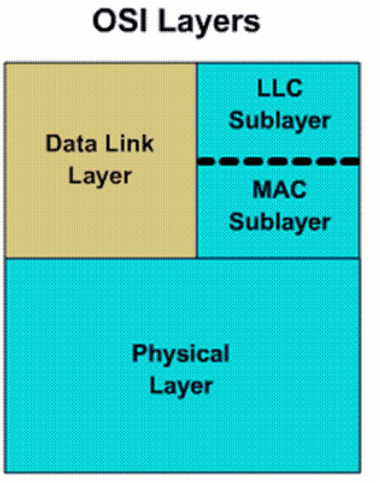

Figure 2.2: Physical Layer and MAC Layer in Wireless Network

In wireless ad-hoc networks, it can be noted that following problems are introduced to MAC layer:

- High Channel Multiplexing

  Wireless ad-hoc networks holds much more links comparing to the traditional wireless technology. The long-distance multi-hop link condition means that

multiple transmission can be carried out simultaneously. It requires a higher channel multiplexing possibility, and the corresponding MAC layer scheduling mechanism is the only solution to achieve the interference management.

- Connection Maintenance

  The dynamic topology means the connections are not fixed in wireless ad-hoc network. Thus, it is difficult to maintain the connectivity among links. As routing and multi-hop link establishment is not the major task of MAC layer, how to provide real-time connection information to the upper layer is of great importance.

- Support for Physical Layer Specialty

  In different applications of wireless ad-hoc network, channel conditions differ from each other because of environment, devices and organization of networks. For example, large-scale and energy-limited wireless sensor networks have to be supported by corresponding energy-efficient MAC layer.

All the above questions originate from the diversity of physical channel. In classical OSI model, physical channel is modelized as a stable and digitalized transmission service provider. However, it becomes diversified in wireless ad-hoc networks. As MAC layer is the only layer connected directly to physical layer, it is the best solution for adapting and exploiting these new physical layer characteristics.

2.2 Approaching Secure Wireless Ad-hoc Networks With Physical Layer Security Technology

As noted in the above section, physical layer in wireless ad-hoc network is special, and is always considered as a trouble maker. However, unless the whole physical layer could be re-designed for the special ad-hoc demand, traditional wireless standards like IEEE 802.11 provide no correlative mechanisms for supporting dynamic physical

channel. Considering the complexity and overhead, the research community shows little interest in remodeling the whole wireless network structure. Instead, solutions for exploiting this physical channel under traditional standards are widely studied, among which physical layer security technology turns out to be one of the best innovations. In the following part of this section, we start with detailed introduction of physical layer security technology, and then present the challenges while applying it in wireless ad-hoc networks.

2.2.1 An Introduction of Physical Layer Security

Physical layer security, as the name suggests, covers varied secure mechanisms using physical layer characteristics. Differed from traditional secure technology, e.g., cryptography, it is hinged tightly with physical layer, and can not be applied to any other layer of OSI model. The most important idea of physical layer security is to find out special physical-layer-related encryption algorithm or secure physical channel between legitimate transmitter and receiver. Thus, diversified particularities of the complex wireless ad-hoc channel can be used to establish new secure mechanisms. Research has been carried on along different paths. We categorize these approaches according to their features, and give an example in each category as follows:

- Key Generation

  One of the most severe problems in wireless ad-hoc physical channel is fluctuation. However, the randomness of the physical parameters can be exploited for generating encryption keys. For example, RSSI (Received Signal Strength Indication) is a common variable in IEEE 802.11 standards. It indicates the quality of physical link between two nodes, and is shared only by these two nodes. As it changes randomly, it can be used to generate a special encryption key for the confidential communication between these two nodes. The duration of every key can be short if the link is unstable enough, so that the eavesdropper can hardly detect it before a new one is generated and used.

- Secure Channel Construction

Naturally, wireless channel lies in the open medium, and anyone can receive the signal in the space. However, special secure channel can be constructed according to information theory. For example, while the wiretap channel of eavesdropper is a degraded version of the main channel, there exists a sub-channel within the main channel in which information transmission is out of detection to the eavesdropper. If this special sub-channel can be used to transmit confidential messages, eavesdropper can never detect the classified content. Research in this category focuses on the problem of how to apply specifically designed mechanism to constructing this kind of secure channel.

- Directional and Smart Antenna Approach

  The development of smart antenna has shown another path for protecting wireless security. By utilizing smart antenna, it is possible to form a private wireless channel between legitimate transmitter and receiver. For example, using beamforming technology, the electromagnetic wave can be restricted in a very limited space along the transmission path. Eavesdroppers are easy to be detected on such an occasion, thus physical layer security can be guaranteed.

Another advantage of physical layer security is that the secrecy is independent from the malicious attackers' capability. Traditional wireless security technology mostly relies on cryptography. A major assumption in cryptography is that malicious attackers have finite computation power [18], and can hardly resolve the encryption keys. Unfortunately, the explosive advancements in microelectronics and ongoing invention of quantum computer have made it easy for anyone to access great computation power. As a result, the above assumptions are becoming weaker and weaker, and the speed for decrypting the confidential message can be really fast even with brutal exhaust algorithm. That's why physical layer security is valued by the research community. Algorithms and schemes are proposed to utilize physical layer security to offer securer wireless system [11][19][20].

2.2.2 The Origin of Physical Layer Security Research

Physical layer security is firstly studied in [21] in the year of 1975. The author has proved that while the wiretap channel of eavesdropper is a degraded version of the main channel, there exists a sub-channel within the main channel in which perfect secrecy can be achieved. If this special sub-channel can be used to transmit confidential messages, eavesdropper can never detect the classified content. The author has also provided the method for calculating the capacity of this secure sub-channel

The key concept in this approach is "perfect secrecy", which is an extension of "shannon secrecy". "shannon secrecy" was invented in Shannon's ground-breaking masterpiece in 1949 [22]. This notion requires *a posteriori* distribution over the message, given the ciphertext, to be equal to *a priori* probability of the message. It can be presented as

$$Pr[X|Y] = Pr[X], \tag{2.1}$$

where X is the source message, and Y is the received cyphertext. Informally, "seeing the ciphertext is only as good as seeing nothing at all" [23] can present the key idea of "shannon secrecy".

Thus, the idea of "perfect secrecy" can be generalized when there exist legitimate receiver and eavesdropper. If one encryption method can guarantee "shannon secrecy" at the eavesdropper's side, it means that none of the confidential message is disclosed. In this way, even the eavesdropper holds infinite computation power, nothing can be decrypted from equivalent "nothing".

A model of wiretap channel is shown in Fig.2.3. A source message s with codebook S^K is coded into message x with the codebook X^N, and is transmitted to the intended receiver over the main channel Q_M. As a message y with the codebook Y^N is observed by the legitimate receiver, an eavesdropper taps the message through an additional wiretap channel Q_W, and harvests a message z with the codebook Z^N.

Under the assumption that the wiretap channel is a degraded version of the main

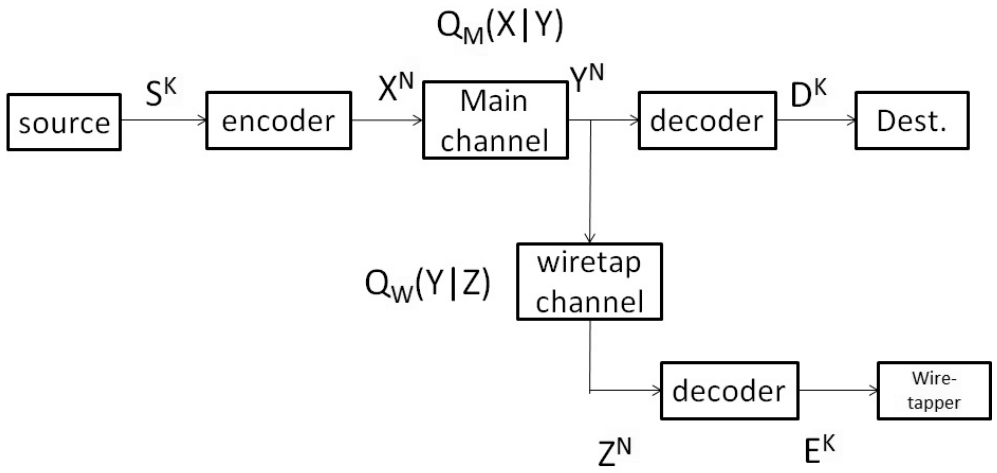

Figure 2.3: System model of Wyner's wire-tap channel

channel, the uncertainty about the secret message at the eavesdropper's side is measured by equivocation per source letter R_e which is given by:

$$R_e = \frac{\mathbf{H}(S^K|Z^N)}{N}, \tag{2.2}$$

where $\mathbf{H}$ is the information entropy. Thus, perfect secure transmission is achievable when $R_e = \mathbf{H}(X)$. In this case, the eavesdropper still has the same uncertainty about the information as the original code book after receiving the message z.

I. Csiszar and J. Korner has studied a more general case of perfect secrecy in [24]. While legitimate channel and eavesdropping channel are independent, a single-letter characterization can be obtained as (R_1, R_e, R_0) such that, in addition to a common message at rate R_0, a private message can be sent reliably at rate R_1, to receiver 1 with equivocation at least R_e per channel use at other receivers. The wiretap channel condition can be treated as a special case with $R_0 = 0$. Secrecy capacity is defined in their article to present the capacity of perfect secure transmission between source and intended destination. As both legitimate channel and eavesdropping channel affect the secrecy capacity, it can be calculated as follows:

$$C_S = \max_{S \to X \to YZ} I(S;Y) - I(S;Z), \tag{2.3}$$

where I is the corresponding mutual information, and S,X,YZ form a Markov chain. It can be further explored according to *Lemma 1* in [21] that the secure capacity has a lower bound as follows:

$$C_S \geq C_L - C_E, \tag{2.4}$$

where C_L and C_E are the channel capacity of legitimate channel and eavesdropping channel, respectively.

Based on these articles, further studies have been carried on in the domain of information theory. Researchers have tried to model the perfect secure network in different environments. [25] has provided an all-around review on articles of these topics, e.g., single-antenna channel, multi-antenna channel, broadcast channel and relay channel.

2.2.3 State-of-the-art

In the approaches depicted in 2.2.2, researchers have proved the existence of "perfect secure channel" under a channel model with eavesdroppers. Most of the researches concerning the topic "secure channel construction" focus on theoretical derivation in the same way with different channel models [26][27]. In the year of 2006, authors of [28] showed that perfect secure capacity exists in general gaussian wireless channel model even if the eavesdropper holds a better channel comparing to the legitimate receiver. This is due to the stochastic nature of the gaussian channel. Namely, during a long period of time, the eavesdropper may suffer a random degradation at some time point when the legitimate receiver is with a good channel condition opportunely, and thus it can seize the opportunity to transmit a packet with perfect secrecy. [11] is another typical example of research in information theory. A fading MIMO (Multi-input Multi-output) channel model is introduced, where the bound of the secure channel is derived. Results show that multi-antenna can lead to a much better secure capacity. These results have largely improved our comprehension of the subject "perfect secure channel".

According to these research, the secure capacity is rather small and unstable.

Thus, mechanisms for enhancing the performance of physical layer security is also studied by the research community, such as "friendly jammer" in [20] and "artificial noise" in [19]. Authors focus on the problem of how to guarantee secure capacity while the channel model is fixed. For the idea of "Friendly jammer", legitimate nodes in the same network are used as friendly jammers. Jamming signals are broadcasted in the network to interfere the eavesdropper, while legitimate receiver can eliminate the jamming signal according to the algorithm. "Artificial noise" is another approach in this area. Assuming that the transmitter and receiver can perfectly estimate the transmission channel, artificial noise which is orthogonal to the channel response matrix can be generated by the transmitter, and is sent with the normal message. As the eavesdropper can not distinguish these two parts, perfect secrecy can be achieved. Further studies are carried on based on this concept. For example, related work like [29] provides some in-depth explorations of how much capacity can be gained, and how to optimize the energy allocation. Performance advancements are achieved in these approaches, though the secure capacity is still much lower comparing to the capacity of regular physical layer.

On the other hand, evolving theoretical results to practical algorithms is a challenging work. Development of applicable mechanisms is still in progress, and far away from implementation. Consequently, studies concerning the other two categories, "key generation" and "directional and smart antenna approach", which specialize more on the practicability, have attracted the research community as a new endeavor.

For the category of "key generation", using which common randomness inherent in reciprocal wireless channels is essential. For example, the phase of the fading coefficients is used in [30] for encryption key generation; multiple independent phases from a multitone communication system is studied in [31] to generate longer keys; RSSI is used in [32] for the same purpose. The problem in these research is that the key generation speed is highly related to the channel uncertainties. If the channel is steady, not only the key generation speed is low, but also it's easier for the eavesdropper to detect the key. On the other hand, severe channel fluctuations may lead to a great loss on performance. This problem becomes a dilemma that has not been well investigated.

The approaches from the antenna design are also interesting. Directional antenna can be used in providing an approximate private wireless channel for legitimate transmitter and receiver. In [33], the authors have provided studies on several critical components of smart antenna design for wireless communication networks. The problem of forming a directional antenna or using eigen-beamforming is studied in [34]. A mathematical derivation concerning how nodes with multiple antennas can improve secure connectivity is presented. Compared with traditional schemes, a large improvement of connectivity possibility can be achieved. However, the major problem in this category relies on the design of corresponding antenna, and is also restricted by the development of this area. By the time of this writing, this kind of antenna is still at the research stage.

2.2.4 Applying Physical Layer Security in Wireless Ad-hoc Networks: Approaches and Challenges

From the above sections, we can find that the research on physical layer security is in its very beginning stage. There is still a big gap between theoretical derivation and applicable realization of secure physical layer. However, if the research community do not start research on corresponding upper layer protocols at this point of time, it will be too late while physical layer security technology burst into applications. To avoid such a situation, we carry on our research concerning this topic. By summarizing the common characters of physical layer security technology, especially the parameters related to MAC layer scheduling, we show that it is possible to initialize the design work of a prototype MAC layer framework.

In traditional wireless standards, e.g., IEEE 802.11, the interface between physical layer and MAC layer is simple. This simple interface approach is due to the design principle of layered structure: the physical layer hides as many realization details as possible from the MAC layer. Thus, MAC layer design can be independent in the largest extent. Primitives used between the MAC layer and the physical layer are listed in Table.2.1 and Table.2.2. While physical layer security is applied to wireless ad-hoc networks, most of these primitives can be inherited directly.

Table 2.1: List of Interface Primitives(1)

primitive name	flow	parameter	value
PHY_TXSTART.request	MAC->PHY	TXVECTOR	PHY depend
PHY_TXSTART.confirm	PHY->MAC	–	N.A.
PHY_TXEND.request	MAC->PHY	–	N.A.
PHY_TXEND.confirm	PHY->MAC	–	N.A.
PHY_DATA.request	MAC->PHY	DATA	X'00'-X'FF' (Octet)
PHY_DATA.confirm	PHY->MAC	–	N.A.
PHY_DATA.indication	PHY->MAC	DATA	X'00'-X'FF' (Octet)
PHY_RXSTART.indication	PHY->MAC	RXVECTOR	PHY depend
PHY_RXEND.indication	PHY->MAC	RXERROR	NE/FV/CL/USR
PHY_CCARESET.request	MAC->PHY	–	N.A.
PHY_CCARESET.confirm	PHY->MAC	–	N.A.
PHY_CCA.indication	PHY->MAC	STATUS	BUSY/IDLE

Table 2.2: List of Interface Primitives(2)

primitive name	description
PHY_TXSTART.request	start the transmission of an MPDU
PHY_TXSTART.confirm	response to PHY_TXSTART.request
PHY_TXEND.request	receive the last PHY_DATA.comfirm
PHY_TXEND.confirm	response to PHY_TXEND.request
PHY_DATA.request	transfer of an octet of data
PHY_DATA.confirm	confirmation of PHY_DATA.request
PHY_DATA.indication	transfer of an octet of data
PHY_RXSTART.indication	receive valid PLCP Header
PHY_RXEND.indication	completed a reception with or without errors
PHY_CCARESET.request	the end of a NAV timer
PHY_CCARESET.confirm	response to PHY_CCARESET.request
PHY_CCA.indication	report of channel state change

However, challenges still exist. The first problem is that overhead largely increases while using secure physical layer. The performance can be rather low due to the additional expense for secure mechanisms. Since traditional scheduling schemes are not designed for this new physical layer and can hardly support this change, we introduce opportunistic scheduling technology to tackle this issue.

Secondly, security is not the only requirement in wireless ad-hoc networks. There

are still a variety of services which have no secure demand. It is clear that secure physical layer can not satisfy these services, then the coexistence of both secure and regular physical layers is a must. As a result, new features have to be designed in the interface to support the switching of different physical layers, and new primitives have to be added.

The third problem is that the physical channel is unstable in wireless ad-hoc networks. Some of the physical layer security mechanisms, especially key generation mechanisms, require even more uncertainties in the channel. This puts a demand of channel probing mechanism in physical layer. As the design of physical layer is out of the scope of this dissertation, we will carry on our research under the assumption that this can be done by the hardware (related research can be found in varieties of research, e.g., [35] and [36]). Thus, the rest of the work lies also in designing corresponding primitives and MAC layer schemes to support this function.

In the following section, we will introduce opportunistic scheduling which is used to solve the first challenging issue. The MAC layer design for the second and third issues will be explained in the third chapter of this dissertation.

2.3 Using Opportunistic Scheduling to Solve Wireless Ad-hoc QoS Problems

In this section, we study the QoS problem of wireless ad-hoc networks. This problem is severe due to the dynamic nature of wireless ad-hoc channel, and can be even more challenging while physical layer security is applied (e.g., severe fluctuation required by key generation). In our solution, the concept of opportunistic scheduling is utilized to tackle the QoS problem. A detailed introduction of this technology and the reasons for using it are depicted in the following part of this section. A discussion concerning opportunities and challenges in applying it is also provided.

2.3.1 Why Opportunistic Scheduling?

QoS is one of the most important domains in wireless research. Mechanisms and algorithms have been proposed from varied aspects within recent decades. Then why do we propose opportunistic scheduling as a new solution? The answer is related to physical layer of wireless ad-hoc networks. Most traditional QoS mechanisms focus on the problem of allocating resources (e.g., bandwidth and time) to different users. On the other hand, they can only provide scheduling function with the resource provided to them, no matter how much it is.

However, channel is unstable in wireless ad-hoc networks. With different approaches, a different amount of resource may be achieved. For example, in an ad-hoc network, throughput per second is not a fixed number. It is determined by the nodes that have transmitted packets in one certain second, and is also affected by the nodes' transmission rate of that second.

Opportunistic scheduling is different from the traditional QoS mechanisms. It is designed to explore the channel condition, and can maximize the quantity of resource. For example, in the case of a wireless ad-hoc network, the overall throughput may be good if the transmitters are with a good channel condition, or it may be bad if the transmitters suffer a channel problem. While opportunistic scheduling is applied, it detects the channel condition of each link. Then the transmission opportunity can be given to the link with good channel condition. Thus, the overall performance can be largely enhanced.

Opportunistic scheduling is considered as one of the best approaches in exploiting channel uncertainties. It is a good choice in solving wireless ad-hoc network performance problem.

2.3.2 The Origin: From Multiuser Diversity to Opportunistic Scheduling

The frequent channel variation is an important characteristic of wireless ad-hoc networks. It is caused by diversified reasons and at multiple time scales. For example, multipath fading can result in small time-scale fluctuations, and long-distance fading

is a reason for large time-scale channel alterations. To adapt these variations of channel condition and harvest stable digital channel for transmission, techniques ranging from coding mechanisms to power controlling algorithms have been developed.

Among all these mechanisms for solving the time-variation problem, diversity is considered as an important breakthrough. The channel efficiency can be multiplied while diversified sub-channels are provided to one or more users simultaneously. There already exist different approaches for exploiting these types of diversity, e.g., FDMA (Frequency-division multiple access) for utilizing multi-frequency diversity, TDMA (Time-division multiple access) for obtaining multi-time-interval diversity, and multi-antenna technology for exploiting multi-space diversity.

Another special form of diversity is called multiuser diversity, which is derived from multiuser wireless environment. The key idea in multiuser diversity can be explained as follows: "Diversity gain arises from the fact that, in a system with many users whose channels vary independently, and there is likely to be a user with a very good channel at any one time. Overall system throughput is maximized by allocating at any time the common channel resource to the user that can best exploit it" [37]. Actually, this idea is firstly discussed in [38], in which authors model a communication system with a base station and multiple users. Almost at the same time, in [39] authors provide a similar result for a network with multiple download links. [37] concludes their research, and renders the name multiuser diversity.

From then on, researchers have proposed varieties of approaches to explore multiuser diversity [40][41][42][43]. Since transmission opportunity coordination is the major task for MAC layer, more delicate scheduling schemes are designed in these research. These schemes share a common concept: exploring the best transmission opportunity opportunistically. Thus, they are categorized as "opportunistic scheduling". Results show that huge performance augmentation can be achieved in wireless environment. Therefore, opportunistic scheduling becomes one of the attractive research domains in recent years.

2.3.3 The-state-of-art

Multiuser diversity exists in all wireless networks that consists of multiple users. After the pathbreaking paper [37] from D. Tse in 2002, research concerning exploiting multiuser diversity has been carried on in different wireless networks. An example can be found in [44], from which a large scale Wi-Fi network is built, and multiuser diversity is used for finding the best route for multi-hop packet transmission.

The term of "opportunistic scheduling" comes from [40]. The usage of multiuser diversity in MAC layer scheduling have been concluded in this literature, and a framework is proposed. The authors show that previous work in this area can fit into or at least relate to their framework. Based on this framework, authors also provide detailed scheduling policy to several scenarios, i.e., temporal fairness scheduling scheme, utilitarian fairness scheduling scheme and minimum-performance guarantee scheduling scheme.

Other detailed issues in scheduling are also studied by the research community. In [42], researchers focus on the uncertainty of measurement in the wireless channel. They consider the gap between measuring and reality, and a special scheduling scheme is developed. Simulation results show that this new scheme can achieve a 35 percent of theoretical delay reduction comparing to other schemes without this consideration. The multiple link category issue is studied in [43]. Authors sort packets from different links into different categories to provide delicate scheduling service. Intuitive analysis is carried on in the literature, and a scheduling scheme similar to the framework in [40] is provided.

It has to be noted that most publications in this area are based on the assumption that there exists an omniscient node which can control every single node in the network. This kind of mechanisms are easy to be implemented in the environment with centric-control. However, in wireless ad-hoc network, distributed scheduling is more valuable.

A recent study [12] has provided an interesting solution to this challenging task. Authors show that it is possible to let each node to make distributed decision for achieving opportunistic scheduling. A mathematical method called optimal stopping theory is used to formulate the optimization problem, based on which a threshold

policy is derived. Nodes in the network are designed to compare their real-time transmission rate with this threshold. Only a positive result can lead to a packet transmission. Numerical results show that this distribute scheduling scheme is efficient in achieving performance optimization. Further studies (e.g., [45]) extend the results of [12]. In [45], a delay constraint is considered, and a similar threshold policy is proved to be applicable for achieving distributed opportunistic scheduling. However, there are still many detailed research topics remaining uninvestigated in this attractive area.

2.3.4 Applying Opportunistic Scheduling in MAC Layer Scheduling

Obviously, opportunistic scheduling is a valuable approach in achieving wireless ad-hoc QoS, especially in the environment with physical layer security. However, there is no interface for integrating opportunistic scheduling policies into existing MAC layer protocols. This explains our motivation in designing a compatible MAC layer protocol. In this subsection, we start from an introduction of DCF (Distributed Coordination Function) in IEEE 802.11 as a paradigm of design, and then present the challenges we may encounter in the design work. These studies lead to our work in the next chapter.

DCF: an Example of MAC Layer Scheduling Protocol

One of the most important mechanisms used in traditional wireless protocols is a distributed transmission opportunity coordination scheme, known as DCF. DCF comprises several essential cornerstones, e.g., random backoff are deployed as the basic policy to reduce collision; network allocation vector (NAV) mechanism is used for estimating the duration of transmission. With these mechanisms, DCF can provide decentralized scheduling to all the nodes in the network. A DCF example is depicted in Fig.2.4 [46].

Here we conclude four basic rules from DCF scheduling scheme[47]:

- When a node has data to transmit. It waits a random backoff time, which is

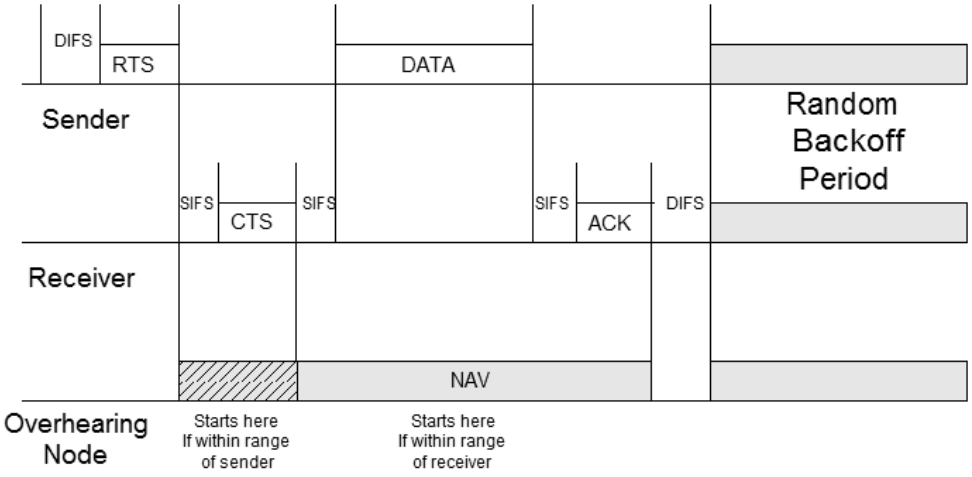

Figure 2.4: An Example of DCF

determined within a contention window. If at any time the node senses that another node is using the channel, it freezes its timer until the other node has finished transmitting.

- When the backoff time has expired, the node detects whether the channel is clear. If yes, it transmits its data.
- A successful transmission compromises the transmission and the ACK. If ACK is not received by the transmitter, the transmission is considered as a failure.
- Unsuccessful transmission may double the contention window, if the contention window do not reach its maximum. If the times of failure reached the pre-fixed maximum value and the transmission is still unsuccessful, the packet is dropped, and the contention window is initialed.

Opportunities and Challenges of Applying Opportunistic Scheduling

To apply opportunistic scheduling in MAC layer protocols, we face both opportunities and challenges. The opportunities lie in the fact that popular protocols (e.g., DCF) are also distributed, a similar structure can be learnt from them. Thus, the design work can be much easier.

However, the scheduling policy is simple in DCF. It can be summarized as: to transmit while the channel is free. In opportunistic scheduling, the optimization efficiency is determined by the scheduling policy. Therefore, much more delicate scheduling policies have to be designed. On the other hand, although performance optimization is valued in opportunistic scheduling, other issues like fairness are also of great importance. This also increases the difficulty of the research.

In the following part of this dissertation, we consider both opportunities and challenges. A MAC layer scheduling framework with different scheduling policies under different scenarios is presented, and simulations show that opportunistic scheduling is an efficient approach.

Chapter 3

SecDCF: A MAC Layer Framework Design

It has been more than thirty years since Wyner's first paper about wiretap channel. However, technologies of that epoch were left far behind this precocious innovation, and not until recent years is the research community ready to investigate applicable solutions. Nowadays, studies from different groups have largely advanced physical layer security technology, and design work of secure physical layer is in progress. However, there is still a soft spot that has not been explored: the design of corresponding protocol in MAC layer. Articles about this topic can hardly be found. Two major issues can be blamed for this condition: 1) the physical layer security technology has not yet been prepared for a real implementation; 2) security problem is not a conventional topic in MAC layer scheduling research.

However, the research on the topic of MAC layer scheduling is essential. Without the support of MAC layer, even if new physical layer security technology will be mature in the near future, the direct implementation may be crude and inefficient. This explains our motivation in this chapter.

To design an assorted MAC layer scheduling protocol, it is important to find out how physical layer security functions. As there is no physical layer design that is mature enough, the only solution is to explore general characteristics according to existing research. Based on these characteristics, A MAC layer scheduling framework

called SecDCF is designed in our research. Furthermore, to handle the performance degradation problem caused by physical layer security, we design an interface to enable opportunistic scheduling policies in our framework. This supports our further research for different scheduling requirements.

3.1 System Model of SecDCF

SecDCF is designed to support the implementation of physical layer security and opportunistic scheduling in wireless ad-hoc networks. To this end, we have to summarize such kind of networks to establish our system model.

3.1.1 Physical Layer Characteristics

As described in chapter 2, both regular and secure service are indispensable in a normal wireless ad-hoc network. In SecDCF, we also have to implement both types of physical layer to support both regular and secure transmissions. For the regular physical layer part, implementation is easy to be found as most standards are open to access. Then in the following, we provide discussion mainly concerning the secure physical layer.

"Artificial Noise": an Example of Secure Physical Layer Functionality

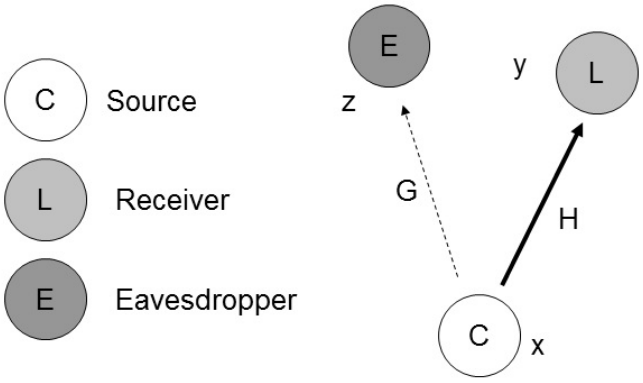

Figure 3.1: System Model for An Eavesdropping Scenario

Basic secure transmission and eavesdropping channels are shown in Fig.3.1. C denotes the transmitter with source message x, which is assumed to be randomly and uniformly distributed over a message set X. The transmitter-receiver channel is denoted by H, and the eavesdropping channel is denoted by G. At time k, the message from the transmitter is defined as x_k, and the channels of transmitter-receiver and transmitter-eavesdropper are defined as H_k and G_k, respectively. Thus, the signal received by the legitimate node is given by:

$$y_k = H_k x_k + n_k \tag{3.1}$$

and the signal received by the eavesdropper is given by:

$$z_k = G_k x_k + e_k \tag{3.2}$$

where n_k and e_k are i.i.d. additive white circularly complex Gaussian noise samples with different variances σ_n^2 and σ_e^2.

In regular cases, normal transmissions take places between source node and the legitimate receiver, and traditional physical layer is applied. The transmission rate of links is given by the Shannon capacity equation for Gaussian AWGN (additional white gaussian noise) channel as follows:

$$R_m = log(1 + \frac{|H_k x_k|^2}{\sigma_n^2}). \tag{3.3}$$

When in secure transmission, secure physical layer is applied. After generating artificial noise signals a_k which lies in the null space of the receiver's channel H_k, the sum of the information signal i_k and artificial noise signal a_k is transmitted as $x_k^* = a_k + i_k$. As $H_k a_k = 0$, the legitimate receiver can easily decode the real information signal i_k, but the eavesdropper can only get mixed information with artificial noise and AWGN which is impossible to decode.

As the eavesdropper can only get corrupted information, the secrecy capacity can be guaranteed. We define Z_k as an orthonormal basis for the null space of H_k, and $Z_k^T Z_k = I$. We also define $p_k = H_k^T / \|H_k\|$. Thus, $i_k = p_k u_k$ where u_k is the

information signal with mean zero and variance σ_u^2, and $a_k = Z_k v_k$ where v_k is i.i.d. complex Gaussian random variable with mean of zero and variance σ_v^2. At the worst condition where the original channel of eavesdropper is noiseless, we still have the following guaranteed capacity[19]:

$$C_{sec,gk} = \left(log\left(1 + \frac{|H_k p_k|^2 \sigma_u^2}{\sigma_n^2}\right) - log\left(1 + \frac{|G_k p_k|^2 \sigma_u^2}{Q_k \sigma_v^2}\right)\right)^+ \tag{3.4}$$

where $Q_k = G_k Z_k Z_k^T G_k^T$. It is clear that is much smaller than R_m.

Performance Analysis of Regular and Secure Physical Layer

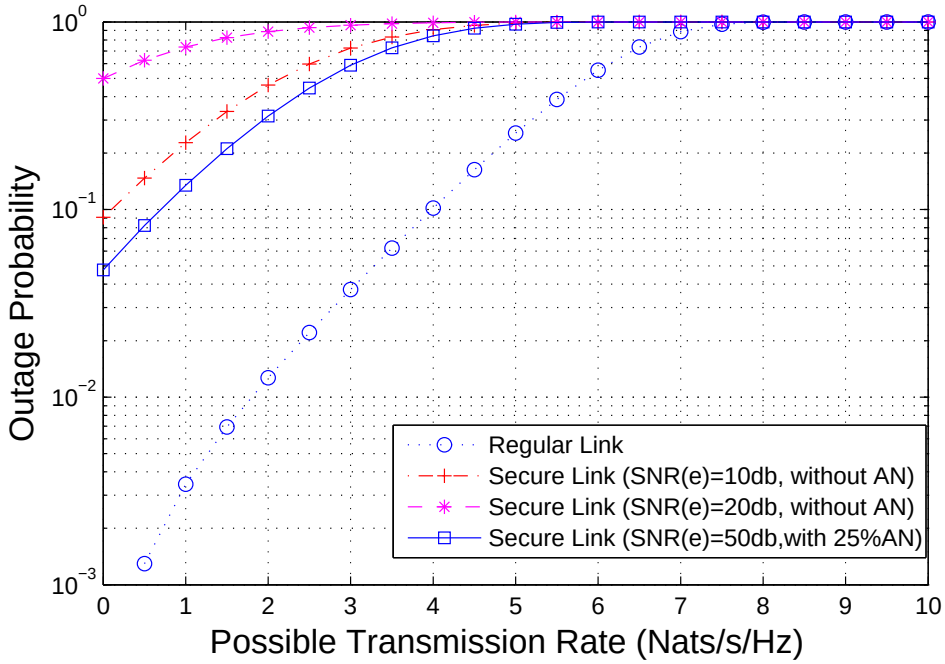

Figure 3.2: Probability of Possible Capacity under Different Condition

The major problem for physical layer security is that it brings enormous overhead. As shown in the above example, the secure capacity is much smaller than the regular one. A comparison of potential capacity among different conditions is shown

in Fig.3.2. Outage probability, which is defined as the probability of a certain capacity can not be supported, i.e., $Pr\{R < C_{outage}\}$, is given under different conditions. Channel functions are all assumed to be complex i.i.d. Gaussian distributed and independent of each other, and receiver's normalized SNR (signal noise ratio) is fixed to $20db$ as an example. The disparity is astonishing.

From Fig.3.2, it can be explored that under about 99% of the conditions, a regular link can achieve a transmission rate of $2M$ Nats/s/Hz. If artificial noise mechanism is not implemented in the system (as shown in the figure as without AN), the user can hardly transmit a secure packet to the legitimate receiver. Under some condition, i.e., the eavesdropper holds a high-quality channel for eavesdropping ($20db$ of SNR), the secure transmission rate is 0 for half of the time. We can also explore from the figure that with artificial noise mechanism, $1M$ Nats/s/Hz of secure transmission rate can be achieved under 90% of time even if the eavesdropper holds a very good channel, i.e., $50db$ of SNR.

3.1.2 Network Topology and System Model

Considering a single-hop ad-hoc network as shown in Fig.3.3, transmitters always have requirements to send confidential messages to legitimate receivers. At the same time, requirements of regular transmission co-exist in the wireless environment. We can see that this network topology can be widely applied in wireless applications, e.g., wireless mesh access networks and wireless sensor networks.

In such a network, connections are established by nodes themselves. Due to the fact that two links holding by one node may have completely different physical propagation paths, nodes can no longer be used as the elementary unit. Instead, scheduling decision have to be made individually by each link. Thus, we model this network with N links presented by $\mathbf{\Omega} = \{1, 2, \ldots, N\}$. p_i denotes the average probability of channel probing attempts of link i, then we can have $P_i = p_i \prod_{j \neq i}(1-p_j)$ as the probability of successful channel contention for link i.. Time-varied channel is modeled into a random variable X with p.d.f $f_X(x)$ and distribution function $F_X(x)$. To this end, the differences between secure and regular physical layer can be presented

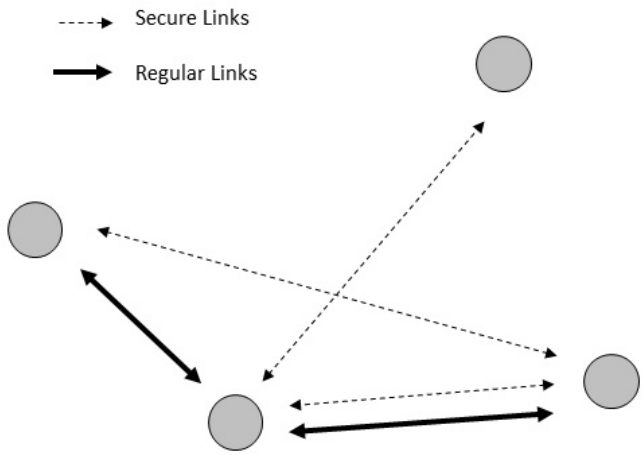

Figure 3.3: Wireless Network Model of Single-hop Ad-hoc Network with Physical Layer Security

easily by using different distribution functions.

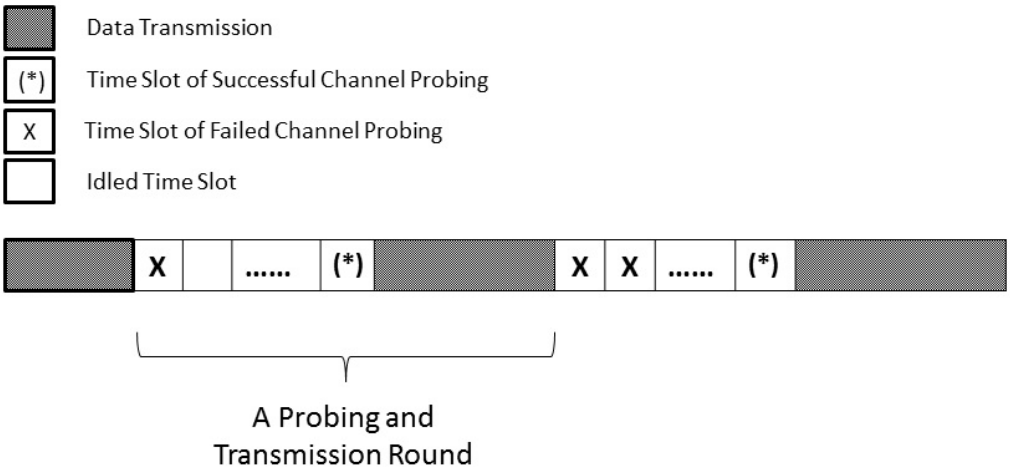

Figure 3.4: An example of random access channel-aware scheduling in wireless ad-hoc network

Furthermore, we apply a slotted scheduling model in our research. A joint channel

probing and packet scheduling procedure is shown in Fig.3.4. In any time slot, if the channel is not taken by data transmission, links are allowed to probe the channel with a probing packet. More than one channel probing attempts lead to a collision, and if there is only one link tries to probe the channel, it succeeds in the channel contention. In a regular random access scheduling scheme, this link is allowed to transmit a packet immediately after the successful contention. For the convenience of presentation, the period of time for an intact channel probing and packet transmission procedure is called a contention round. We assume that the duration of a time slot is t, and the data transmission duration t_p is no greater than the channel coherence time.

3.2 SecDCF: A Compatible Design of MAC Layer Framework

As depicted in the above section, a compatible MAC layer design is urgently required for tackling the special scheduling requirements from physical layer security and opportunistic scheduling. Hereby, we present our new MAC layer scheduling framework called SecDCF for this problem.

3.2.1 New Problems with Physical Layer Security and Opportunistic Scheduling

DCF is a practical scheme for distributed medium resources coordination in wireless networks. However, problems are brought in by secure physical layer and the needs for resource allocation between two different types of transmissions. Amendments have to be designed to fulfill three critical requirements.

- Primitives have to be designed to communicate MAC layer and physical layer for switching the two physical layer according to the real-time requirement.
- Opportunistic scheduling needs the knowledge of current channel condition. Thus, channel probing is required. To save the limited channel resource, probing is carried out on demand. Primitives have to be designed for this function.

- Scheduling policies are important in achieving QoS. Thus, interface has to be designed for quick implementation.

3.2.2 Primitive Design

The first two problems listed in last paragraph require new primitives. Thus, additional primitives are designed as shown in Table.3.1 and Table.3.2. These new primitives can guarantee enough information exchange for achieving the functionality of SecDCF.

Table 3.1: List of Additional Interface Primitives(1)

primitive name	flow	parameter	value
PHY_ChToS.request	MAC->PHY	–	N.A.
PHY_ChToS.confirm	PHY->MAC	–	N.A.
PHY_ChToR.request	MAC->PHY	–	N.A.
PHY_ChToR.confirm	PHY->MAC	–	N.A.
PHY_Probing.request	MAC->PHY	–	N.A.
PHY_Probing.confirm	PHY->MAC	–	N.A.
PHY_ChaCon.indication	PHY->MAC	DATA	X'00'-X'FF' (Octet)
PHY_ChaCon.confirm	MAC->PHY	–	N.A.

Table 3.2: List of Additional Interface Primitives(2)

primitive name	description
PHY_ChToS.request	request for changing to secure physical layer
PHY_ChToS.confirm	response to PHY_ChToS.request
PHY_ChToR.request	request for changing to regular physical layer
PHY_ChToR.confirm	response to PHY_ChToR.request
PHY_Probing.request	request for channel probing
PHY_Probing.confirm	response to PHY_Probing.request
PHY_ChaCon.indication	indicate the channel condition
PHY_ChaCon.confirm	confirmation to PHY_ChaCon.indication

"PHY_ChToS" and "PHY_ChToR" are designed to change the physical layer to secure physical layer and regular physical layer. "PHY_Probing" is used to initial a probing procedure in physical layer. All these three primitives are started by MAC

layer. If the request is carried out, a confirm message is given back from the physical layer. "PHY_ChaCon" is used by the physical layer to report the current channel condition after a successful probing. A confirmation primitive of "PHY_ChaCon" is also designed for MAC layer after receiving the information.

3.2.3 SecDCF Scheduling Rules

A new set of scheduling rules is also applied in SecDCF. The major difference between SecDCF scheduling and traditional random access scheduling is that after a successful channel contention, a certain policy should be implemented to make a judgement. The packet transmission only starts if the judgement result is positive. For the convenience of presentation, the period of time for an intact channel probing and packet transmission procedure is still called a contention round.

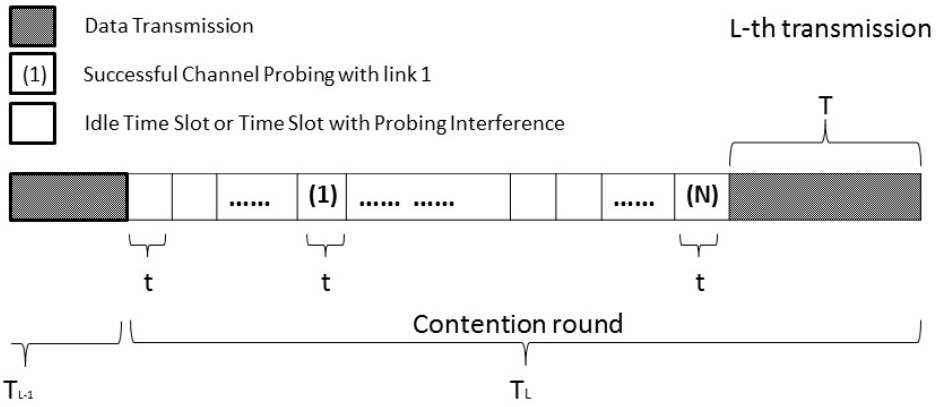

Figure 3.5: An Example of A Contention Round in SecDCF

As shown in Fig.3.5, link 1 has won the channel contention in the middle of a contention round. However due to the judgement, it has to skip the transmission opportunity. Not until a link N has won both the channel contention and the judgement of the scheduling policy is a transmission carried out.

Thus, the scheduling rules of SecDCF framework can be presented as follows:

1. **Channel Probing**. Channel probing is combined with channel contention, and is carried out before each transmission. If multiple nodes probe channel at

the same time, an interference occurs, and all of them fail to claim the channel resource. If only one node probes, it successfully contends the channel and probes the channel state information of that link. Then this information will be used in scheduling policy to make further scheduling decision.

2. **Link Establishment**. Probing packet is also used to establish links. While probing packet from one new node is broadcasted in the network, all the existing nodes memorize the information of this node and a potential link can be established according to the broadcasted information.

3. **Scheduling Policy**. According to the current scheduling policy, transmission decisions are made. In random access, the link who wins the channel contention is allowed to transmit its packet immediately. **(This rule can be replaced according to the research in the following chapter.)**

4. **Regular Transmission**. If the pending transmission is a regular one, transmission is carried out with regular physical layer with regular transmission rate. A successful transmission is ended by an ACK packet.

5. **Secure Transmission**. If the pending transmission is a secure one, secure packet is transmitted under the secure transmission rate by the secure physical layer. A successful transmission is ended by an ACK packet.

6. **Backoff Policy**. If ACK is not received in transmission phase, the attempt is considered failure. It then follows a random backoff policy. A random period of time has to be waited before next attempt as in DCF. The attempt counter for this specific link increases by 1.

7. **Packet Dropping**. A pre-defined parameter is used to control packet dropping according to the wireless environment. If the attempt counter passes the parameter, the packet is dropped, and further packet transmission to this node is banned until a new establishment of the link with a channel probing packet.

3.3 Simulations and Conclusion

3.3.1 Simulation scenario

In our simulations, a one-hop ad-hoc network with N links is implemented. An AWGN channel model considering both propagation loss and shadowing is employed. Based on such a channel model, normalized SNR ρ is calculated according to [48]. Therefore the transmission rates of links are given by the Shannon capacity equation for Gaussian AWGN channel as follows:

$$R_m = log(1 + \rho|H_m|^2) \text{ nats/s/Hz}, m \in L_n, \tag{3.5}$$

where H_m denotes the random channel gain with a complex Gaussian distribution. Then we can get the distribution function of transmission rate for one link as:

$$F(r) = 1 - exp(-\frac{exp(r) - 1}{\rho}). \tag{3.6}$$

In SecDCF, secure and regular links can be easily distinguished by their transmission rate as we have shown in Fig.2.4. Therefore, we use different ρ to present different kinds of links in our simulations.

Our simulator is developed in MATLAB with a slotted CSMA model. Physical layer characteristics are implemented as depicted above. A packet transmission duration is fixed as t_p. For the MAC layer realization, a structure following the scheduling rules of SecDCF is applied. To communicate the physical layer and the MAC layer, primitives are designed in the simulator.

As the probing part is not a major concern in our research on scheduling scheme, we abstracted the probing phase with the channel contention. Thus, there would be no channel probing if there is no waiting packet. Channel information can be detected after a successful probing in the physical layer, and this information is transmitted to MAC layer by primitives. Thus, there is no more probing overhead in this simulator.

Three more parameters are designed in the MAC layer. For adjusting the backoff window and limit the retry times, denoted as t_{window} and c_{drop}. Algorithm is applied

to double the backoff window while transmission is not successful. A finite buffer is also designed for each link for storing waiting packets with a size of n_{buffer}. Initial values are set as $t_{window} = 8$, $c_{drop} = 5$ and $n_{buffer} = 20$. t_{window} and c_{drop} are chosen as half of the value in DCF, for a probing mechanism is already employed for collision avoidance. Buffer size is set according to general case. Needless to say, these parameters play important characters in the simulation results. Interested readers can refer to papers like [49] for further exploration.

Generally, a poisson distribution is used for presenting the arrival rate of packet in designing network simulator. It is also followed in ours. For link i, the number of slots between the arrival time of two packets is denoted by a poisson random variable D_i, with the expectation δ_i. Then we can have the probability of a packet generating in a time slot as $\frac{1}{\delta_i}$. Approximately, we use $P_i = \frac{t_p}{\delta_i}$ to present the individual traffic load, and we have the overall traffic load as follows $\frac{N \cdot t_p}{\delta_i}$. To adapt the system model we use for calculation, a probing probability for each link P_i is also derived from the individual traffic load.

3.3.2 Results and Analysis

In our simulation, we use different $\rho_s = 5$ and $\rho_r = 30$ to present secure and regular links respectively. We also try to test our algorithm in a busy network, so 10 links with 5 secure links and 5 regular links are implemented. t_p is designed to be 30 time slots.

First, we examine the overall channel performance under SecDCF framework. We assume that all the links are with the same packet arrival rate. By changing δ_i, we can have different traffic load. For example, in the network we presented above with 10 links, we can have an overall traffic load of 0.01 when $\delta_i = 30000$. We can also have a very heavy overall traffic load of 1.5 when $\delta_i = 200$.

In Fig.3.6, a comparison between secure and regular throughput is presented. It is clear that the secure throughput is much smaller than the regular one. It is due to the overhead used for guaranteeing secure transmission.

Delay performance is shown in Fig.3.7. In SecDCF framework, there is no obvious

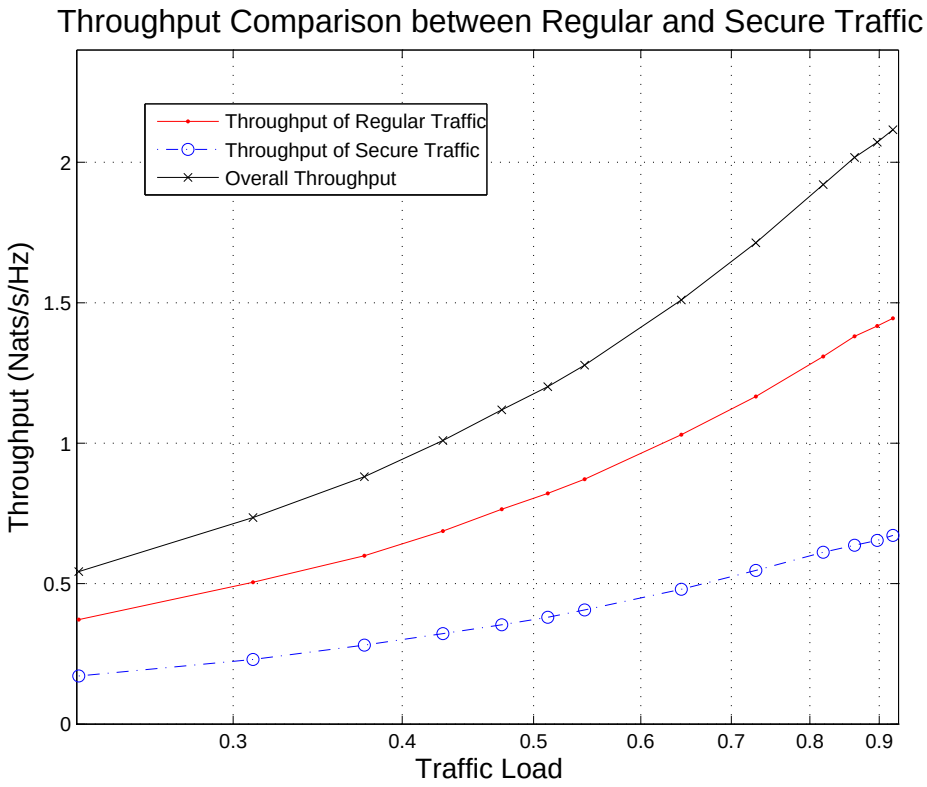

Figure 3.6: Throughput Comparison of Secure and Regular Traffic

difference between delay performance of secure and regular traffic. As a conclusion, we can see that transmission opportunities are coordinated fairly among different links. If we want to transmit more packets with secure links, scheduling policy has to be adjusted based on SecDCF framework.

3.3.3 Conclusion

In this chapter, we have studied the alterations caused by physical layer security and opportunistic scheduling. To adapt to these changes, a framework called SecDCF is constructed for MAC layer scheduling. Simulations are also carried out under the normal random access scheduling condition. From the results, it is easy to find out that the channel efficiency is highly affected while achieving high secrecy level. Performance in such a network can really be a problem. QoS is also hard to be guaranteed.

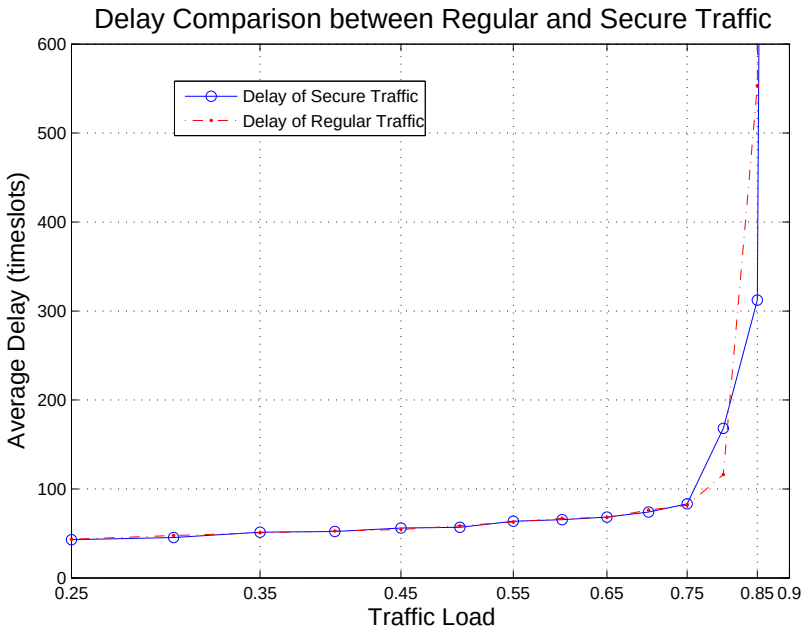

Figure 3.7: Delay Comparisons of Secure and Regular Traffic

Fortunately, interface has already been designed in SecDCF for integrating opportunistic scheduling policies. In the following chapters, we will present our approaches to achieve better performance and QoS under diversified scenarios and requirements.

Chapter 4

QSOS: A MAC Layer Scheduling mechanism Considering both Security and QoS

In the above chapters, we show that secure transmissions can be protected by physical layer security technology, in which real-time physical channel characteristics is used to achieve perfect secrecy. Accordingly, a compatible MAC layer scheduling framework called SecDCF is designed to support the implementation of secure physical layer.

We also explore that physical layer security brings new problems into the network while improving secrecy level, within which, QoS is definitely one of the most critical issues. Wireless ad-hoc networks hold links with time-varying channel, and the transmission rate is unstable originally. If new secure technology is applied to the network, necessary overhead leads to even worse performance. Low transmission rate can cause not only throughput degradation, but also congestion and delay issues. To solve these problems, we design interface in SecDCF to integrate opportunistic scheduling policies which have to be studied indeed in the following.

In this chapter, we focus mainly on two problems: **1) throughput has to be optimized in order to provide better network capacity for not only each link, but also overall network; 2) as secure and regular links coexist in the network, a solution for fairness has to be considered.** Then a scheduling

scheme called QSOS (QoS-Secure-Oriented Opportunistic Scheduling) is designed by us.

The rest of the chapter is organized as follows: motivation and general solution are provided in the first section; in the second section, problem is formulated, an idea of scaled transmission rate is introduced to solve the fairness problem. We describe in the third section the mathematical approach for opportunistic scheduling with scaled transmission rate. A further exploration with weighted scaled transmission rate is shown in section four, more flexibility is provided with this scheme; in the fifth section, the scheduling scheme is studied, and the integration with SecDCF is presented. The last section is with the simulation and analysis of QSOS.

4.1 Motivation and a Solution of Scaling Function

In this section, we first present some simulations using traditional scheduling scheme, e.g., random access and DOS (Distributed Opportunistic Scheduling). We show that a severe performance loss, and also fairness problem exist in wireless ad-hoc networks with both regular and secure physical layer. This explains our motivation of developing QSOS. It then follows a discussion of scaling function which is our approach for solving these service quality problems.

4.1.1 An Analysis on Existing Scheduling Schemes

The utilization of physical layer security can lead to severe service quality problems. This has been addressed in chapter 2 of this dissertation. We also show that the idea of opportunistic scheduling can be introduced to solve these problems. However, existing distributed opportunistic scheduling schemes, e.g., DOS, has not been adjusted for this special situation. DOS is proposed in recent publication [12]. In this paper, authors have applied optimal stopping theory [50] to derive distributed policy for wireless ad-hoc networks. A shared threshold can be calculated at every link's side, and is used to judge whether the current transmission rate is large enough for performing a transmission. If the current transmission rate is smaller than

the threshold, the transmission opportunity has to be dropped and another round of channel contention starts in the following time slot. Lucid illustrations show that this threshold policy is sufficient for achieving optimized overall network capacity.

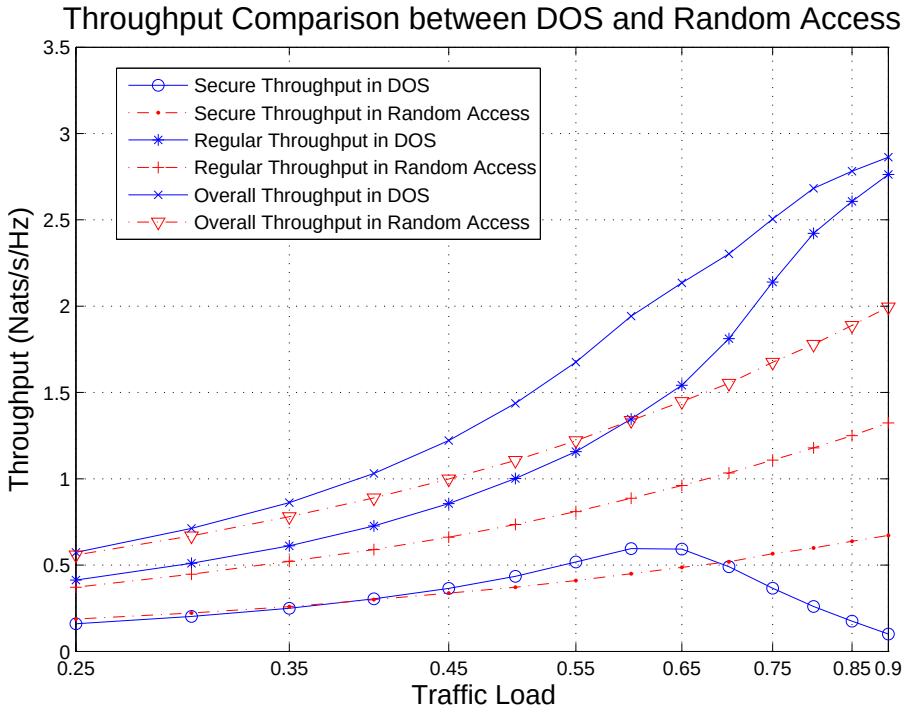

Figure 4.1: An example of DOS and random access performance with regular and secure links

However, DOS has not yet been applied to the ad-hoc networks with both regular and physical layer security. Little work has been done for coordinating transmission opportunities for multiple categories of traffic. In Fig.4.1, we show a simulation result of a one-hop ad-hoc network with 10 links (detailed simulation scenario is described in the simulation section). Physical layer security is implemented in 5 of the links with smaller transmission rate. It is easy to explore from the figure that random access scheduling suffers a big loss of overall throughput comparing to DOS scheme. DOS can largely improve the overall throughput with a rather low secure link throughput, even worse than the random access scheduling scheme while the network traffic load

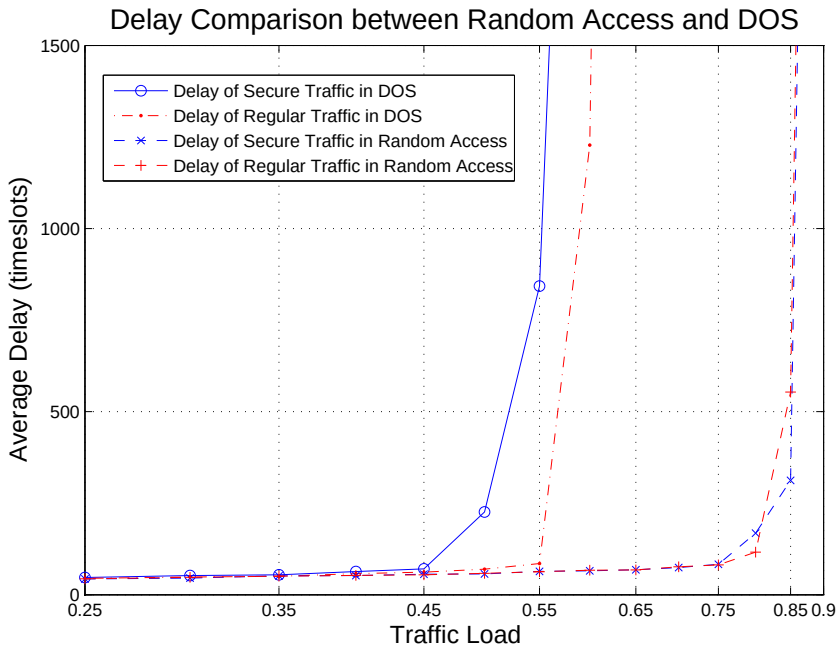

Figure 4.2: Delay Performance Comparison between DOS and Random Access

is heavy. Delay performance is very bad in DOS, as shown in Fig.4.2. It is due to the fact that packets are always delayed for a better transmission rate. Clearly, these two scheduling schemes have their own advantages and disadvantages.

As a conclusion, the introduction of physical layer security can cause severe throughput problem. Although performance of overall throughput can be improved by DOS, a new problem of fairness appears. To benefit the high secrecy level provided by physical layer, two QoS requirements have to be tackled in the new scheduling scheme: fairness and throughput optimization. Moreover, considering the throughput requirements of different link categories, it is better to provide a mechanism which can fine-tune the throughput for each link. These are subjected to the following research.

4.1.2 A Design with Scaling Function

Considering the threshold policy used in DOS, links with bad performance suffer a great loss of transmission opportunity. It is because that these links are more

likely to have a smaller transmission rate comparing to the same shared threshold. Accordingly, those links with good performance have larger probability to seize the transmission opportunities. This explains how the overall capacity can be improved. The extreme condition is terrible in DOS, if a link with a rather small transmission rate exists in the network. It may lose its access to the channel while its maximal transmission rate is smaller than the threshold.

To this end, we propose a scaling function as a solution. It is used to scale the transmission rate of each link to a similar extent, e.g., the same expectation. A scaled threshold can be derived based on the scaled transmission rate. We use this new threshold to judge whether current scaled transmission rate is good enough. From a certain perspective, the scaled threshold is approximately in the middle place of the scaled transmission rate for each link. Thus, a necessary amount of transmission opportunity can always be guaranteed for each link.

Furthermore, a weight function is applied to the scaling function to provide more flexibility. While a large weight is designated to a link, this link can win more transmission opportunities. Notably, the weight chosen procedure can be a distributed one. Thus, the selection of the weights may be used in a selfish way. To solve this problem, we investigate the corresponding Nash equilibrium for this non-cooperated game, and we prove that no link can benefit from changing only its own weight at the Nash equilibrium point.

4.2 Problem Formulation of QSOS

4.2.1 System Model

The system model used in the development of QSOS is as same as the model that is depicted in chapter 3. For the convenience of readers, we re-present the network topology figure in chapter 3 here as Fig.4.3. A single-hop wireless ad-hoc network with support for both secure and regular transmissions is still considered. This network is with N links presented by $\mathbf{\Omega} = \{1, 2, \ldots, N\}$. p_i denotes the average probability of channel probing attempts of link i, then we can have $P_i = p_i \prod_{j \neq i}(1 - p_j)$ as the

probability of successful channel contention for link i. Time-varied channel is modeled into a random variable X with p.d.f $f_X(x)$ and distribution function $F_X(x)$. To this end, the differences between secure and regular physical layers can be presented easily by using different distribution functions.

Optimal stopping theory is used as the major mathematical tool for exploring QSOS scheme in our research. That is why the system model is similar to that is used in [12] and [45]. However, differences still exist between the models, for we introduce multiple categories of link, i.e., secure links and regular links in our derivation.

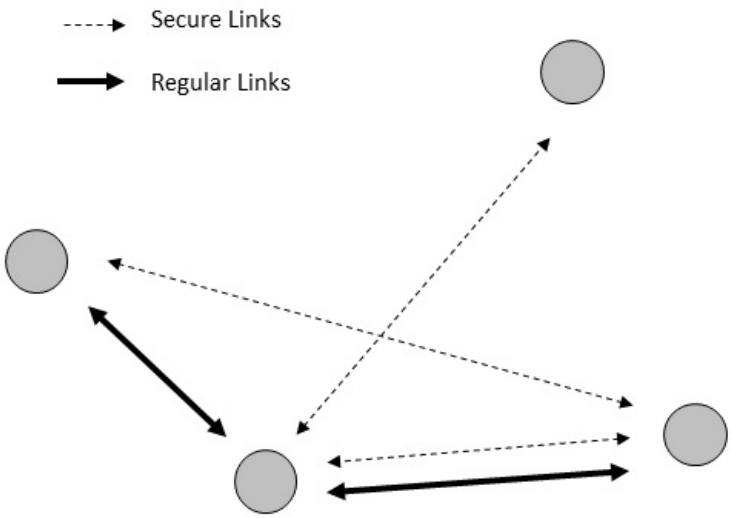

Figure 4.3: Wireless Network Model of Single-hop Ad-hoc Network with Physical Layer Security

4.2.2 Scaled Transmission Rate

We assume that for link i, the transmission rate R_i is with expectation λ_i. In the scaling function, the transmission rate is scaled over its average, and is called STR (scaled transmission rate). At a certain time slot, S_i can be presented as follows:

$$S_i = \frac{R_i}{\lambda_i} \tag{4.1}$$

We assume that the new random variable S_i is modeled with p.d.f $\ell_i(s)$ and distribution function $\mathcal{F}_i(s)$. Thus, different rate distributions are scaled to new distributions with the same average, e.g., 1. The rate heterogeneity between regular and secure links is no longer a dominant factor impacting the throughput unfairness.

According to opportunistic scheduling, each time a link successfully contends the channel, a rule is followed to determine whether it is allowed to transmit (for example, the transmission rate is large enough). Here, we use scaled transmission rate to derive a scaled threshold for establishing this rule. The detailed study is presented in the following sections.

4.3 Opportunistic Scheduling with Scaled Transmission Rate

4.3.1 Optimal Stopping Rule with Scaled Transmission Rate

The opportunistic scheduling problem is formulated as a problem of maximizing the profit over cost. The cost here is the time used for a contention round. The profit is the scaled information quantity transmitted in the contention round, here, denoted by current STR multiplying the transmission time t_p. For each time slot, we use a stopping rule V to decide whether a link can carry out data transmission. Thus, we use T_V to denote the time duration of a contention round with channel probing and transmission, and S_V is the scaled transmission rate in this transmission. The profit of the whole problem can be represented as $E[S_V t_p]/E[T_V]$.

Define Q as the set of all the stopping rule as follows:

$$Q \triangleq \{V : V \geqslant 1, E[T_V] \leq \infty\}, \tag{4.2}$$

the problem of maximizing the profit can be presented as:

$$V^* \triangleq \underset{V \in Q}{argmax} \frac{E[S_V t_p]}{E[T_V]}, s^* \triangleq \underset{V \in Q}{sup} \frac{E[S_V t_p]}{E[T_V]}. \tag{4.3}$$

If we can prove that the optimal stopping rule V^* exists, the problem is solved. To this end, we have the following proposition:

Proposition 4.1 *The optimal stopping rule V^* for QSOS exists, and is given as follows,*

$$V^* = min\{n \geqslant 1 : S_n \geqslant s^*\}. \tag{4.4}$$

The maximal scaled throughput s^* is also the scaled threshold, and is the unique solution to

$$E(S_n - s)^+ = \frac{st}{t_p \sum_{i=1}^{N} P_i} \tag{4.5}$$

Proof: The proof is very similar to Appendix A of [12], and is presented in Appendix A.1.

Remarks: 1) *proposition* 4.1 shows that the optimal rule is a single threshold policy. After a successful channel contention, current STR of the link is compared to the scaled threshold s^*. If the current STR is larger than the threshold, the transmission is proceeded. Otherwise, the opportunity is skipped, and channel contention continues.

2) As STR of each link are with the same average, the threshold policy implies that the transmission opportunities are assigned more or less equally over the network. This can improve the system fairness. The optimal stopping rule ensures that the system still achieves a better throughput comparing to random access, due to the fact that during the relevant "low rate" period of each link, packet transmission is not carried out.

3) The nonlinear equation in 4.5 can not be resolved easily in a formula mode. However, by using a fix-point iterative method, the optimized threshold s^* can be calculated. First, following the definition of s^*, we can have

$$s^* = \sum_{i=1}^{N} \frac{\frac{\int_{s^*}^{\infty} r \mathrm{d}\mathcal{F}_i(r)}{1-\mathcal{F}_i(s^*)} t_p}{\frac{t+\sum_{j\neq i} P_j(1-\mathcal{F}_j(s^*))t_p}{P_i(1-\mathcal{F}_i(s^*))} + t_p}. \tag{4.6}$$

The content of the sum formula is $E[S_V t_p]/E[T_V]$ for each link. The numerator is the expected throughput for link m, and the denominator is the expectation of channel

contention time plus the transmission time t_p.

It can be rewritten as follows:

$$\mathcal{K}(s^*) = \frac{\sum_{i=1}^{N} P_i \int_{s^*}^{\infty} r \mathrm{d}\mathcal{F}_i(r)}{\frac{t}{t_p} + \sum_{i=1}^{N} P_i(1 - \mathcal{F}_i(s^*))}, \tag{4.7}$$

and

$$s = \mathcal{K}(s). \tag{4.8}$$

Thus, we can have the iterative algorithm as $s_{k+1} = \mathcal{K}(s_k), k = 0, 1, 2, ...$ Proposition 3.4 in [12] proves the convergence of this algorithm for any non-negative initial value s_0, i.e., $s_0 = 0$. It means that the optimal threshold s^* can be always achieved with this iterative algorithm.

4.3.2 Analysis of the Opportunistic Scheduling with Scaled Transmission Rate

Using Scaled transmission rate is a simple way for achieving throughput optimization and fairness simultaneously. Optimal stopping theory can be directly applied. The links in different categories are almost treated equivalently, thus transmission opportunities are assigned to them fairly.

However, the throughput of each link is determined as soon as the current scaled threshold s^* is calculated. It is because that threshold is the only factor in a scheduling decision. According to (4.1), the real threshold of normal transmission rate for link i can be presented as $\lambda_i s^*$. Then from (4.7), we define the real throughput of link i as:

$$\mathcal{Z}_i = \frac{P_i \int_{\lambda_i s^*}^{\infty} r \mathrm{d}F_i(r)}{\frac{t}{t_p} + \sum_{j=1}^{N} P_j(1 - F_j(\lambda_j s^*))}. \tag{4.9}$$

The major concern of using scaled transmission rate is that it can only provide a fixed fairness to the system. When more delicate scheduling is required in the network, this scheme is not able to provide fine-tuning. These problems have put forward the demand of a more elaborate scheduling scheme.

4.4 Opportunistic Scheduling with Weighted Threshold

In this section, we introduce a weighted mechanism to enhance the scaled opportunistic scheduling policy proposed in the last section. With this mechanism, links are able to fine-tune its throughput according to requirements. However, while distributed weight selection is applied, selfish behavior can lead to disastrous result in the network. To tackle this problem, we treat the weight selection as a non-cooperative game, and useful results are derived with game theory.

4.4.1 Weighted Threshold and Weighted Throughput

From (4.9), it is easy to find out that the only way to adjust individual throughput is to modify the shared threshold. Thus, we introduce a weight parameter w to the threshold. For link i, the weighted scaled threshold ω_i can be calculated as follows:

$$\omega_i = w_i s^*. \tag{4.10}$$

First, we assume that the weight w_i for link i is pre-fixed, and it can be selected according to the requirements of the network independently. With different weight w_i, throughput of each link is no longer fixed, the demand of fine-tuning among different links can be achieved. If requirements are changed, weights can also be adjusted.

4.4.2 Analysis of Weight Selection

However, a random selected weight is impossible to guarantee the delicate scheduling purpose. Then the following problem is to find out how to determine these weights for achieving throughput improvement. Following (4.9), we use $\mathcal{Z}_i$ to present the real throughput of link i as follows:

Definition 4.1 *The current throughput for link i under a set of weight $\{w_1, w_2, \ldots, w_N\}$ is denoted by $\mathcal{Z}_i$ as:*

$$\mathcal{Z}_i(w_1, w_2, \ldots, w_N) = \frac{P_i \int_{\lambda_i w_i s^*}^{\infty} r \mathrm{d}F_i(r)}{\frac{t}{t_p} + \sum_{j=1}^{N} P_j(1 - F_j(\lambda_j w_j s^*))}. \tag{4.11}$$

According to (4.11), the individual throughput is only affected by the weight set if the channel condition remains the same. To see through the characteristics of weight selection, we define $w_{-v} \triangleq [w_1, \ldots, w_{v-1}, w_{v+1}, \ldots, w_N]$. Assuming that w_{-v} is fixed, in what follows we can have this proposition:

Proposition 4.2 *For a certain link v, there exists an optimal throughput $Z_v^*(w_v^*, w_{-v})$. The optimal weight w_v^* used to achieve this optimal throughput can be calculated with the following iterative algorithm:*

$$w_{v,k+1}^* = \frac{\mathcal{Z}_v(w_{v,k}^* w_{-v})}{\lambda_i s^*}, k = 0, 1, 2, ... \tag{4.12}$$

and

$$w_{v,0}^* = 0. \tag{4.13}$$

The proof of *Proposition* 4.2 can be found in Appendix A.2.

Remarks: 1) Proposition 4.2 shows that a weight mechanism can be used to improve links' performance. While an optimal weight is applied to one link, the throughput of this link can be better.

2) However, this mechanism may affect the throughput of other links. Fig.4.4 shows a pictorial illustration for this problem. While there are two links in the network, link 1 can achieve a better throughput with a smaller w_1, while link 2 suffers a loss of throughput.

4.4.3 A Non-Cooperative Game for Weight Selection

In a wireless ad-hoc network, the distributed nature requires decentralized management. However, the weight selection procedure presented in the last section is a pre-fixed one. It is interesting to discuss if the weight selection can be carried out in a distributed way.

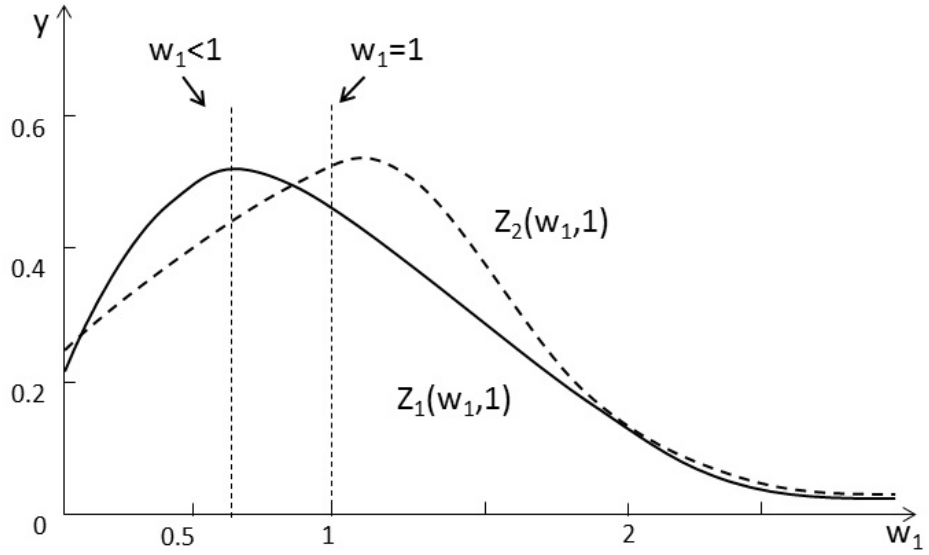

Figure 4.4: A pictorial illustration of the influence of selfish behavior

One big problem for an independent weight selection is that selfish decision exists. If all the links use the optimal weight to improve its own throughput, significant improvement is no longer achievable for any individual link. This problem can be treated as a non-cooperative game in the network.

We assume that each link wants to maximize its throughput by changing the weight. Thus, all the links are the players in a non-cooperative weight selection game. We use $\mathcal{A}_i = [\{w_i | 0 < w_i < \infty\}, i = 1, 2, \ldots, N]$ to denote the action set of each link, and $\mathcal{P} = [1, 2, \ldots, N]$ to denote the player set of the game. The payoff function is denoted by $\mathcal{U}_i = [\mathcal{Z}_i, i = 1, 2, \ldots, N]$. Let $G = [\mathcal{P}, \{\mathcal{A}_i, i \in \mathcal{P}\}, \{\mathcal{U}_i, i \in \mathcal{P}\}]$, then the non-cooperative game can be casted as:

$$(G) \max_{w_i \in \mathcal{A}_i} \mathcal{Z}_i(w_1, w_2, \ldots, w_N), \forall i = 1, 2, \ldots, N. \tag{4.14}$$

One of the interesting topics in this game is whether there exists Pareto Optimality. The study can be started from a two-link scenario. Assuming that there are two links in the network, both of the links can choose its weight independently. Thus, we can have the following proposition:

Proposition 4.3 *There exists Pareto Optimality in the weight selection game G of two links. To achieve Pareto Optimality, the weights have to be chosen so that:*

$$w_1 s^* \lambda_1 = w_2 s^* \lambda_2. \tag{4.15}$$

The proof of *Proposition* 4.3 can be found in Appendix A.3.

Remarks: 1) Under Pareto Optimality, there is no possible pareto improvement in the network. No one can achieve a better performance without affecting the other one. It is interesting that the threshold derived in [12] is the pareto optimality. To understand this, we can assume that if this overall maximal point derived in [12] is not the pareto optimality, which means the overall performance can be further improved without performance loss from any link. This is obviously a contradiction.

2) The scenario can be easily extended to multiple-link scenario. An equal threshold (without scaling) can be always proved to be the pareto optimality. To avoid the worthless repeat of the same derivation, it is not included in this literature.

Obviously, the Nash equilibrium is also an interesting topic in this weight selection game. It represents the condition that nodes can not negotiate to accept the overall optimization, but only a balance under compromise can be achieved. This Nash equilibrium problem in weight selection game is similar to the Nash equilibrium problem discussed in [12]. The readers can refer to this article for further explorations.

4.5 Scheduling Policy Design for QSOS

4.5.1 New Problems with QSOS

With QSOS, problems are brought in by the needs for performance optimization and fairness concerns. Amendments have to be designed to fulfill two more critical requirements.

- The calculation of optimized threshold is based on the channel states of the entire network. Procedures of both channel states distribution and threshold calculation should be specified at the nodes' end.

- The scaled threshold policy has to be applied in the scheduling scheme for both regular and secure links.

4.5.2 Scheduling Policy

According to above rules, the QSOS scheduling policy is designed. The "Scheduling Policy" rule in SecDCF can be replaced by the following three rules:

1. **Threshold Calculation**. Scaled threshold is calculated locally using channel states information. The link information of other nodes are collected from their successful transmissions.

2. **QSOS Scheduling Policy**. In the case of a successful channel contention, current scaled transmission rate for this link is calculated. A comparison between this scaled transmission rate and current scaled threshold is carried out by the scheduling policy. A positive result leads to a procedure of packet transmission. If the scaled transmission rate is smaller than the threshold, the transmission opportunity is skipped, and the channel probing and contention continues.

3. **Physical Channel Adaption**. If a packet is allowed to be transmitted by the QSOS scheduling policy, the physical channel has to be adjusted according to the packet category. "PHY_ChToS.request" and "PHY_ChToR.request" have to be sent to the physical layer. It then follows the data transmission. Channel state information is also required to be broadcast as the first part of a successful transmission.

With the new SecDCF scheduling rules, QSOS can be utilized. In the following section, we provide simulations and analysis according to SecDCF implementation.

4.6 Simulations and Analysis

4.6.1 Simulation scenario

The simulation scenario is similar comparing to the simulator we used in chapter 3. We generally present it here again for the convenience of readers. We use an AWGN channel model with normalized SNR ρ. Therefore the transmission rates of links is given by the Shannon capacity equation for Gaussian AWGN channel as presented in (3.5):

$$R_m = log(1 + \rho|H_m|^2) \text{ nats/s/Hz}, m \in L_n, \tag{4.16}$$

where H_m denotes the random channel gain with a complex Gaussian distribution.

Initial values are set as $t_{window} = 8$, $c_{drop} = 5$ and $n_{buffer} = 20$. For link i, the number of slots between the arrival time of two packets is denoted by a poisson random variable D_i, with the expectation δ_i. Then we can have the probability of a packet generating in a time slot as $\frac{1}{\delta_i}$. Approximately, we use $P_i = \frac{1}{\delta_i}$ to present the traffic load, and we have the traffic load as follows $\frac{N \cdot t_p}{\delta_i}$.

4.6.2 Simulations for QSOS with Secure and Regular Traffic

As analyzed in last chapter, the packet generation speed is essential for the throughput and delay. Here, we use the same model as we used in last chapter. $\rho_s = 5$ and $\rho_r = 30$ are used to present secure and regular links respectively. A network of 10 links with 5 secure links and 5 regular links are implemented. We still assume that all the links are with the same packet arrival rate. By changing δ_i, we have different traffic load.

A throughput comparison between random access, DOS and QSOS is presented in Fig.4.5, Fig.4.6 and Fig.4.7. Since there is no other research concerning the same subject so far, the only way to show the value of our research is to compare it with existing schemes in the similar research domains. It is easy to find out that when the channel is not busy, the differences are not clear. However, when packets arrive more frequently in channel, these three scheduling schemes distinguish with each other.

With QSOS, a balanced and optimized performance is offered. The security throughput is much better than it is in the other two scheduling schemes. Clearly,

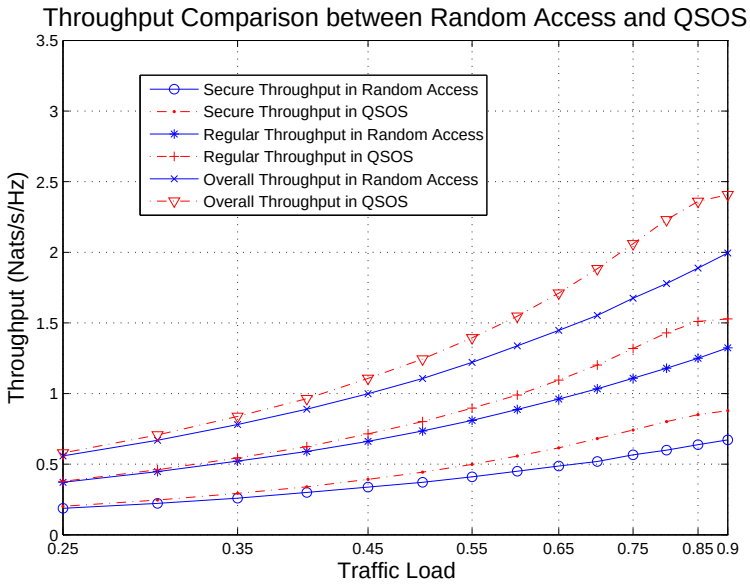

Figure 4.5: Throughput Comparisons between QSOS and Random Access

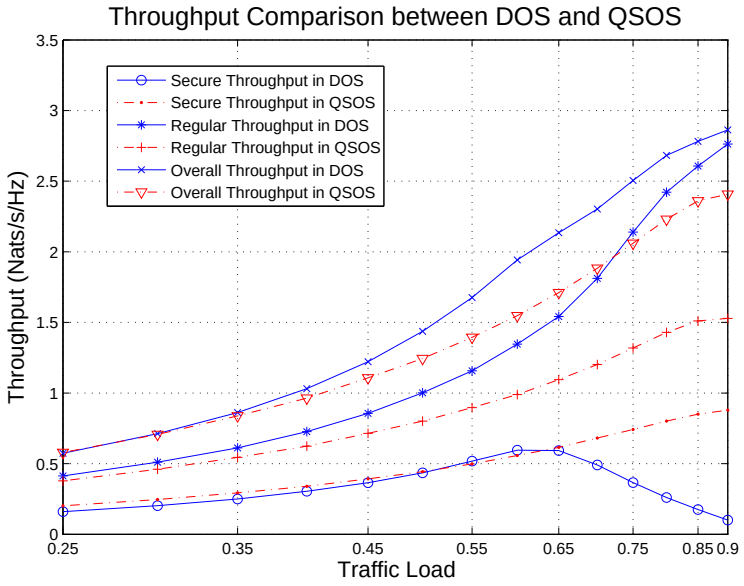

Figure 4.6: Throughput Comparisons between QSOS and DOS

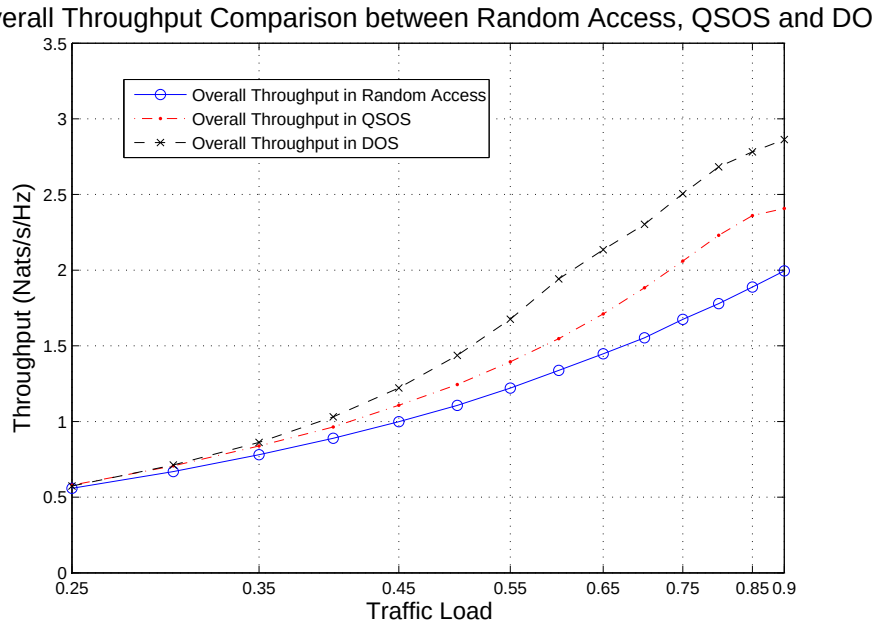

Figure 4.7: Overall Throughput Comparisons between QSOS, DOS and Random Access

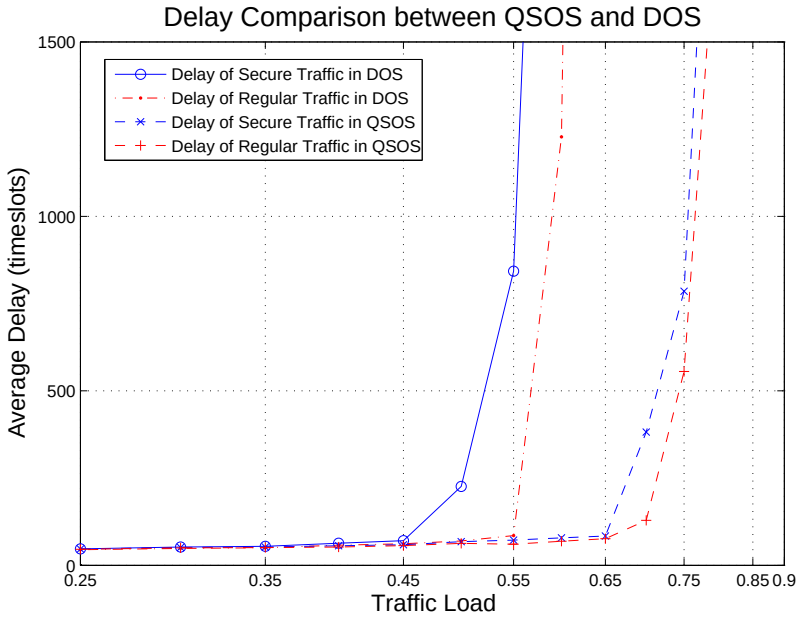

Figure 4.8: Delay Performance Comparison between DOS and QSOS

both opportunistic scheduling schemes improve the overall throughput. By sacrificing secure traffic, DOS scheduling is capable to transmit the most regular packets, and also achieve the best overall throughput. By equivalently treating secure and regular packet transmission, QSOS achieves the fairness between different link types. Due to the difference between transmitting a secure packet and a normal packet, the throughput improvement for secure traffic is smaller than the loss in regular traffic. Thus, the overall throughput of QSOS is smaller than DOS.

Furthermore, we compare the delay performance in Fig.4.8. The delay performance for both secure and regular traffic are similar in QSOS. The fairness is quite obvious with the implementation of scaled threshold. A further balance between throughput optimization and delay performance is also achieved.

4.6.3 The Impact of Weight Selection

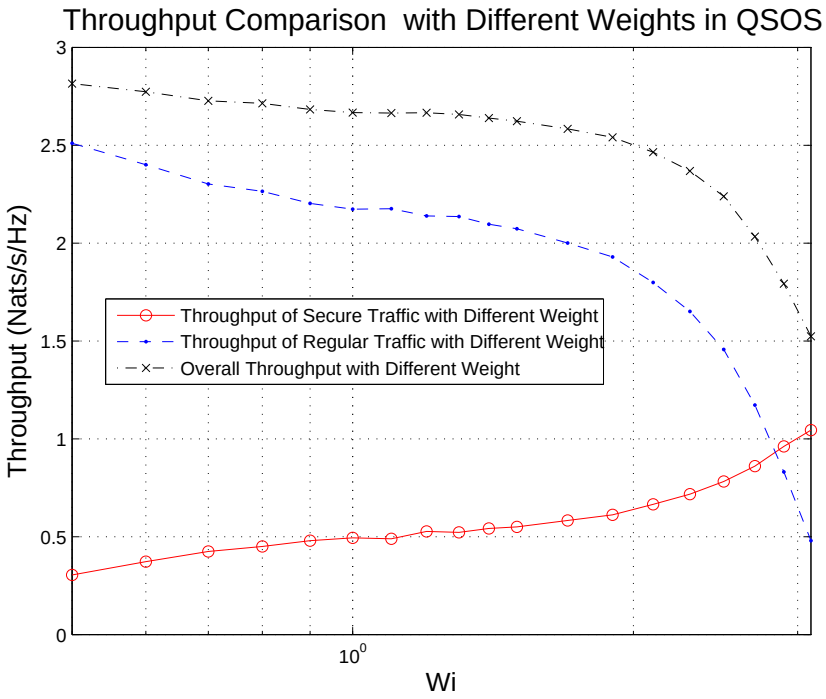

Figure 4.9: Throughput Comparison with Different Weights in QSOS

In this section, we present a series of simulations to show the impact of weight

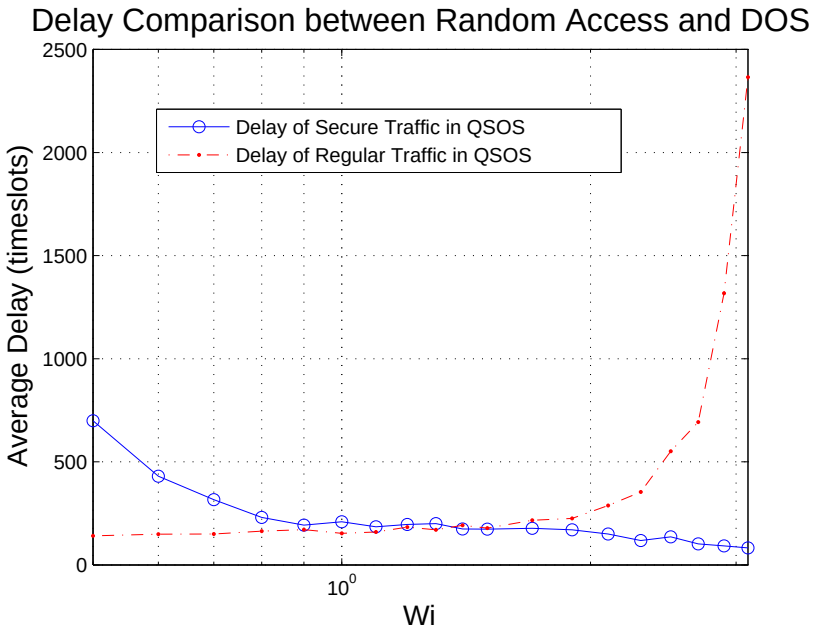

Figure 4.10: Delay Comparison with Different Weights in QSOS

selection. A total of 3 links coexist in the network, in which two are regular links and one is secure link. The normalized SNR is rendered the value of $\rho_s = 5$ and $\rho_r = 40$, respectively. The traffic load is fixed as 0.8. The weight for those two regular links are fixed as 1. Thus, by changing the weight of the secure link, we show how this parameter affects the network performance.

In Fig.4.9, a throughput comparison is presented. Even with a very low normalized SNR, the secure link can finally achieve a throughput of more than $1 Nats/s/Hz$ when the weight is 3.1. However, the cost reveals in the performance of the regular links. They suffer a great loss to provide better performance to the secure link. Overall throughput is also affected.

A delay comparison is shown in Fig.4.10. The final delay of regular traffic is large when the weight of secure link reaches 3.1. The problem here is that the changing weight affects the scaled threshold, and most of the transmission opportunities for the regular links are dropped according to the large threshold. In this way, a better throughput can be achieved with the secure link. This is definitely the selfish problem

we discussed in the sections above.

4.6.4 Conclusion

The loss of throughput is a huge problem in wireless ad-hoc networks with physical layer security. When opportunistic scheduling is applied to the network, although overall throughput is improved, the fairness issue becomes even more critical. In this chapter, we want to explore the balance between throughput optimization and fairness.

That's why Qos-Secure-oriented Opportunistic Scheduling (named as QSOS) is developed by our research group. By using scaled transmission rate and scaled threshold, our mechanism achieves two goals simultaneously: 1) better network capacity for the whole network; 2) better fairness between secure and regular links. With the integration of SecDCF framework, QSOS shows its potential in providing high-quality performance in wireless ad-hoc network with physical layer security.

Chapter 5

TEOS: Using Threshold Enabled Opportunistic Scheduling to Guarantee QoS under Individual Throughput Requirement

In this chapter, we focus on the problem of individual throughput, which is also an essential factor in wireless QoS. A variety of research including ours has shown that opportunistic scheduling can be used to provide an optimized overall capacity. However, the case under individual throughput requirement has not yet been well investigated. To explore this unsolved problem, scheduling scheme with individual threshold is studied by us. As a result, TEOS (Threshold Enabled Opportunistic Scheduling) is proposed.

The rest of this chapter is organized as follows: background and system model is provided in the first section; individual throughput requirement is introduced in the second section, with the analysis of traditional scheduling scheme; a derivation of applicable threshold policy and a corresponding iterative algorithm is presented in the third section; MAC layer protocol design is then described in the fourth section; numerical results and conclusions are included in the last section.

5.1 Individual Throughput Requirement: Unsolved Problem in Distributed Opportunistic Scheduling

5.1.1 Limitation of Traditional Capacity-oriented Opportunistic Scheduling

Traditional opportunistic scheduling research mostly focus on the subject of capacity optimization. Our research in last chapter is a good example of these capacity-oriented opportunistic scheduling studies. Threshold policy is derived with mathematical approach, and performance results in simulation show that an optimization in throughput capacity can be achieved.

However, there is a missing point in the former research, that individual requirements are not taken into account. For example, in a network with regular link A and secure link B, we assume that A has better performance than B. A fixed thresholds can be easily calculated for the opportunistic scheduling problem in this case. We can achieve an optimized capacity by transmitting comparatively more packets with link A, and less packets with link B. If there is a real-time requirement with link B for transmitting a certain amount of packets, this optimized capacity and corresponding threshold can provide little help in network realization. It can be treated as a kind of fairness problem as we studied in chapter 4. However, the results are not explicit enough.

The aim of capacity-oriented opportunistic scheduling is to find out the upper bound of a certain scenario. This derivation is important for system design. However, the system does not function under full loads all the time. If a set of individual throughput requirement is given, there lacks a special solution to derive thresholds to achieve opportunistic scheduling. How to do the scheduling work remains challenging.

5.1.2 Opportunistic Scheduling under Throughput Constraint

For a wireless ad-hoc network, individual throughput requirement certainly exists, and is determined by network layer protocols and upper layer applications of each link. Hence, the judgement of whether these requirements can be achieved and how they can be achieved are important in MAC layer scheduling. **If requirements that can not be achieved by traditional scheduling scheme (e.g., random access scheduling), are possible to be accomplished with opportunistic scheduling, opportunistic scheduling is certainly a valuable solution in applications.**

If the above proposition is true, we can have the following deduction. Considering a scenario with individual throughput requirement, we can categorize the requirements into three different classes based on the final scheduling results. The first class of requirements can be achieved by random access scheduling, thus there is no need to apply new opportunistic scheduling scheme. The second class lies out of the upper bound of random access scheduling. Only new opportunistic scheduling scheme can solve the scheduling problem. In the third category, requirements are out of the channel capability. Even new scheme can not coordinate the transmission opportunity without causing congestion.

Thus, our objective in this study is clear. The proposition has to be proved, and a new scheduling scheme, which we call TEOS has to be designed. Furthermore, an effective region of TEOS has to be defined. For the requirements that can be accomplished by TEOS, a corresponding scheduling policy is necessary. For the requirements that can not be accomplished by TEOS, an algorithm for making the judgement is also dispensable.

5.1.3 System Model

Comparing to the system model that is depicted in chapter 3, the only change is to add the requirement. The network topology, channel contention model and physical layer design are all the same.

A single-hop ad-hoc network with N links presented by $\mathbf{\Omega} = \{1, 2, \ldots, N\}$ is

still used. p_i denotes the average probability of channel probing attempts of link i. Due to the dynamics of wireless environment, we model the time-varied channel into a random variable X with p.d.f $f_X(x)$ and distribution function $F_X(x)$. Here we assume X has a finite range $[\underline{X}, \overline{X}]$. For the convenience of derivation, we denote t as the duration of a time slot. We also assume that t_p is the data transmission duration and is no greater than the channel coherence time.

To present the real demand in the network, we denote $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_N\}$ as the throughput requirement for each link in a certain period of time. It has to be noted that $\boldsymbol{\mu}$ can be defined in any time scale. If a small time duration is used in the derivation, e.g., millisecond level, delicate real-time scheduling can be achieved. Without loss of originality, we use one second to define this requirement in this literature. Thus, $\boldsymbol{\mu}$ can also present the required transmission rate of each link approximately.

5.2 MAC Layer Scheduling Problem under Individual Link Requirement

5.2.1 Limitation of Random Access Scheduling

Following the system model we presented in the above section, it is easy to derive the upper bound of individual transmission rate in random access scheduling. Apparently, the probability of successful channel probing for link i can be given by

$$P_i = p_i \prod_{j \neq i} (1 - p_j). \tag{5.1}$$

Then, the overall successful channel probing probability P_{succ} is given by

$$P_{succ} = \sum_{i=1}^{N} P_i = \sum_{i=1}^{N} p_i \prod_{j \neq i} (1 - p_j). \tag{5.2}$$

Therefore for all the links, the average waiting time before a transmission is given by

$$t_r = \frac{t}{P_{succ}} = \frac{t}{\sum_{i=1}^{N} p_i \prod_{j \neq i}(1-p_j)}. \tag{5.3}$$

To calculate the effective transmission rate for each link, it is also important to calculate the average time for link i to wait before a transmission. It can be given by

$$t_r^i = \frac{t}{P_i} = \frac{t}{p_i \prod_{j \neq i}(1-p_j)}. \tag{5.4}$$

However, while link i waits for the next transmission opportunity, some other links may succeed in channel contention and transmit. User i needs to back-off and freeze its timer for these transmission, e.g., timer frozen mechanism in IEEE 802.11 DCF. To this end, the waiting time experienced by each single user is larger than t_r^i, and from a long-term aspect of view, it can be approximately presented as:

$$\tilde{t_r^i} = t_r^i + \frac{t_r^i - t_r}{t_r} \cdot t_p, \tag{5.5}$$

in which the second part is the expectation of potential transmission time for other links during the waiting period. Thus, we can have the effective transmission rate for link i as

$$S_{ran}^i = \frac{t_p}{t_p + \tilde{t_r^i}} \int_{\underline{X}}^{\overline{X}} x \cdot f_X(x) dx. \tag{5.6}$$

If we use X_{mean} to present the expectation of transmission rate as: $X_{mean} = \int_{\underline{X}}^{\overline{X}} x \cdot f_X(x) dx$, it is easy to have the following proposition:

Proposition 5.1 *For any scenario with giving individual requirement μ, it is impossible to use random access scheduling to satisfy the demand if and only if the following inequations can not be satisfied:*

$$\frac{p_i \prod_{j \neq i}(1-p_j)}{\frac{t}{t_p} + \sum_{i=1}^{N} p_i \prod_{j \neq i}(1-p_j)} \cdot X_{mean} \geq \mu_i, \quad \forall i \in \Omega. \tag{5.7}$$

Remark: In a given wireless ad-hoc network scenario, the effective transmission

rate for all the links can be statistically calculated as presented above. If any of the individual requirements can not be satisfied, this requirement is out of the capability of random access scheduling.

5.2.2 Using Thresholds to Improve Individual Throughput

According to multi-user diversity, channel potential is not well exploited with random access scheduling. It has also been proved in [12] that thresholds can provide overall capacity optimization for wireless ad-hoc networks. However, the improvement is based on the fact that transmission opportunities are re-coordinated to links with better performance. Whether thresholds can also be used for improving individual throughput without sacrificing performance of other links in the network remains an unsolved problem.

While individual requirements exist in the network, the problem is different. The objective is to satisfy everyone's requirement. Overall capacity optimization is still critical, but not with first priority. Thus, if we can prove that better individual throughput for one link can be achieved without causing other users' performance fall below their requirement threshold, problem is solved.

To this end, we provide the following threshold policy. Considering a threshold set denoted as $\mathbf{T} = T_1, T_2, \ldots, T_N$, when a link i gets the transmission opportunity after a successful channel probing at time τ, the channel condition X_τ can be explored and is compared with threshold T_i. If X_τ is larger than T_i, the user will proceed to transmit; while if X_τ is smaller thanT_i, the user will release the channel and another round of channel probing starts.

Thus, with threshold policy, it is possible to skip the transmission opportunity even with a successful channel contention. Then the probability of a successful transmission can be given by

$$P_{teos,succ} = \sum_{i=1}^{N} P_i \cdot (1 - F_X(T_i)). \tag{5.8}$$

Therefore an average waiting time before a transmission is given by

$$t_w = \frac{t}{P_{teos,succ}}. \tag{5.9}$$

Thus, in a time period of $t_p + t_w$, a packet transmission takes place. The average transmission rate can be denoted by

$$S_{ave} = \sum_{i=1}^{N} \frac{P_i \cdot (1 - F_X(T_i))}{P_{teos,succ}} \cdot \frac{\int_{T_i}^{\overline{X}} x \cdot f_X(x)dx}{1 - F_X(T_i)} = \frac{1}{P_{teos,succ}} \sum_{i=1}^{N} P_i \int_{T_i}^{\overline{X}} x \cdot f_X(x)dx \tag{5.10}$$

For the average throughput of each user under threshold T_s, it can be derived following the same steps. As the probability of a successful transmission for user i is given by $P_i \cdot (1 - F_X(T_i))$, the real average time for user i to wait can be derived as

$$t_w^i = \frac{t}{P_i \cdot (1 - F_X(T_i))}. \tag{5.11}$$

However, it is similar to the condition in the random access scheduling. Back-off is needed. The real waiting time for link i becomes

$$\tilde{t_w^i} = t_w^i + \frac{t_w^i - t_w}{t_w} \cdot t_p, \tag{5.12}$$

in which the second part is the expected transmission time of other links during the waiting period. Therefore the average throughput for user i is that

$$S_{ave}^i = \frac{t_p}{t_p + \tilde{t_w^i}} \frac{\int_{T_i}^{\overline{X}} x \cdot f_X(x)dx}{1 - F_X(T_i)}. \tag{5.13}$$

In this way, we have the following proposition:

Proposition 5.2 *For any giving scenario with individual requirement μ, there exists a set of thresholds $\mathbf{T_o} = \{T_1, T_2, \ldots, T_N\}$, with which better individual throughput for all the links can be achieved comparing to random access scheduling:*

$$S_{ave}^i(\mathbf{T_o}) \geq S_{ran}^i, \qquad \forall i \in \mathbf{\Omega}. \tag{5.14}$$

The proof can be found in Appendix A.4.

Remarks: 1) It is shown in Proposition 5.2 that optimized thresholds set $\mathbf{T_o}$ exists. Thus, threshold enabled opportunistic scheduling can be used to solve the scheduling problem established by individual requirements. The problem now is how to derive the corresponding thresholds for each link.

2) From the proof, it is easy to find out that the equality is true when and only when for all i we have $S^i_{ave} < \underline{X}$. Namely, all the probing probability p_i is extremely small. Even under this terrible condition, all the thresholds can be taken as $\underline{X}$ which makes the scheduling policy equivalent to pure random access. In all, there is no loss induced by TEOS. As this condition is negligible and trivial, it is not included in the further discussion.

5.3 TEOS: Solution for Exploiting Channel Potential under Individual Throughput Requirement

With proposition 5.1, it is easy to find out whether a certain set of requirements can be achieved with random access scheduling. Also, we have proved that better individual throughput performance can be provided if we use thresholds in scheduling, based on which we can propose TEOS for solving the scheduling problem.

Obviously, a random threshold set can not guarantee the required functionality. Delicately selected thresholds are a must for the scheduling conundrum. Hereby, we define the major task in TEOS, is to find out a threshold set that can make a certain requirement set achievable. Also, as TEOS can not exceed the limitation of channel capacity, another task in TEOS research is to explore the requirement that can never be achieved even with TEOS.

5.3.1 Threshold Derivation for TEOS

We now explore the threshold derivation for TEOS. It is clear that for link i, the effective transmission rate can be derived from (5.13) as:

$$S^i_{ave}(\mathbf{T}) = \frac{p_i \prod_{j\neq i}(1-p_j)}{\frac{t}{t_p} + \sum_{k=1}^{N}(1-F_X(T_k))p_k \prod_{j\neq i}(1-p_j)} \int_{T_i}^{\overline{X}} x \cdot f_X(x)dx, \tag{5.15}$$

where $\mathbf{T}$ is the current threshold set.

Thus, to have a set of thresholds for satisfying the individual requirement, it is obliged to have:

$$S^i_{ave}(\mathbf{T}) \geq \mu_i, \qquad \forall i \in \Omega. \tag{5.16}$$

As a result, the problem of threshold derivation can be treated as solving multiple nonlinear inequations. If we can characterize the solution set for (5.16), efficient thresholds for achieving the requirement can be derived spontaneously. Furthermore, if we can prove the system of inequalities unsolvable under a requirement set, it can be treated as a mechanism for distinguishing un-achievable requirement.

The uniqueness of solution is another interesting subject in this problem. Unfortunately, in general, the solution is not necessarily unique as a result of the complicate condition of F_X. It is possible to provide some sufficient condition, with which unique solution can be established to the scheduling problem. However, this kind of special cases are not interesting considering the real application requirement. In the following sections, we focus on a general iterative algorithm for deriving one of the possible solution under individual requirement.

5.3.2 Iterative Algorithm

Based on the structure of (5.15), we propose the following iterative algorithm for deriving the thresholds. Two scales of iteration are used in the algorithm. In the large scale, we try to approach a possible threshold set step by step, hereby, defined as step k. In the small scale, we derive the threshold for link i with the thresholds that have already been calculated in the current step k, i.e., $T_1^{(k)} \dots T_{i-1}^{(k)}$, and the

thresholds that have not yet been renewed in the current step, i.e., $T_{i+1}^{(k-1)} \dots T_N^{(k-1)}$. While $k = 0$, we have the initial value for all the links as $T_1^{(0)} = T_2^{(0)} = \cdots = T_N^{(0)} = \overline{X}$.

In step k, we have the following iteration for link i:

1. First, we denote $T_{-i} = \{T_1^{(k)}, T_2^{(k)}, \dots, T_{i-1}^{(k)}, T_{i+1}^{(k-1)}, \dots, T_N^{(k-1)}\}$. Derived from (A.18), we define:

$$g(T_i^*, T_{-i}) = -T_i^* t - T_i^* P_{teos,succ} t_p + P_i t_p \int_{T_i^*}^{\overline{X}} x \cdot f_X(x) dx. \tag{5.17}$$

   Then it is possible to have the optimized threshold T_i^* under the condition $g(T_i^*, T_{-i}) = 0$.

2. As presented in the proof of proposition 5.2, the unique solution T_i^* of $g(T_i^*, T_{-i}) = 0$ exists and is the optimized threshold for having the best S_{ave}^i under T_{-i}. Then we can calculate the current S_{ave}^i with (5.13).

3. Based on the comparison between current S_{ave}^i and μ_i, we can have the following judgement:

   (a) if $S_{ave}^i < \mu_i$, iteration terminated, no solution;

   (b) if $S_{ave}^i = \mu_i$, update $T_i^{(k)} = T_i^*$;

   (c) if $S_{ave}^i > \mu_i$, find the maximal solution for $S_{ave}^i(T_i^{(k)}, T_{-i}) = \mu_i$.

4. If the algorithm does not terminate, continue with the same procedure to calculate for the link $i + 1$ in step k. If it is already the last link in step k, move on to the step $k + 1$. If fixed points have arrived for all thresholds in $\mathbf{T^k}$, the algorithm stops, and the current $\mathbf{T^k}$ is a solution to the scheduling problem.

Then we have the following proposition:

Proposition 5.3 *For a giving set of requirement $\boldsymbol{\mu}$, when there exist solutions for the scheduling problem, the iterative algorithm will come to a fixed point $\mathbf{T}^* = \{T_1^*, T_2^*, \dots, T_N^*\}$, so that $S_{ave}^i = \mu_i$, for all i.*

Proof: The proof can be found in Appendix A.5.

Remark: 1) The convergence of the iterative algorithm is shown in Proposition 5.3. It is interesting that the convergence only appears when there exist solutions for the scheduling problem. To this end, if a threshold set can be derived from this algorithm, it is clear that the corresponding requirement set is achievable.

2) The times to achieve the fixed-point is also important for the algorithm. Unfortunately, the iterative number to achieve convergence is not always finite. However, as the transmission rate is always digitalized in wireless ad-hoc network, a certain level of accuracy that can be finished with limited iteration is more practicable. To show the performance of this part, experiments are carried on in the numerical results part. It is clear that with limited iteration, the solution set can be achieved. Theoretical analysis remains to be our future research.

3) Unachievable requirement set leads to a termination in the iterative algorithm. Thus, it is possible to use this rule to distinguish them.

5.3.3 Unachievable Requirement in TEOS

By applying opportunistic scheduling, threshold policy can be used to achieve better individual throughput for links in wireless ad-hoc network. However, there is certainly a limitation. Extreme conditions can never be satisfied with limited channel resource. Thus, problem turns out to be how to distinguish achievable requirements from immoderate ones.

Surprisingly, we have explored that our iterative algorithm presented in the above section can be used directly for this problem. Here by, we have the following proposition:

Proposition 5.4 *For a giving set of requirement $\boldsymbol{\mu}$, if the iterative algorithm terminates during the iteration, i.e., in step 1, step 2, ..., step k, there is no solution set $\mathbf{T}^*$ to satisfy requirement set $\boldsymbol{\mu_i}$.*

Proof: The proof can be found in Appendix A.6.

Remark: The proof show that there is no possibility to find out another solution pair if the iterative algorithm terminates. Thus, for all the conditions provided to our

scheduling scheme, one iterative algorithm is enough to fulfill both tasks of threshold derivation and the judgement of impossible cases.

5.4 Scheduling Policy Design for TEOS

5.4.1 New Problems with TEOS

TEOS can also be used in SecDCF to provide individual throughput guarantee for secure and regular links. Problems are brought in by the needs for exchanging channel state information, as well as the scheduling policy. Amendments have to be designed to fulfill the following requirements.

- The calculation of individual threshold is based on the channel states of the entire network. Procedures of both channel states distribution and threshold calculation should be specified at the nodes' end.
- Individual threshold has to be applied in the scheduling scheme for each link.

5.4.2 Scheduling Policy

According to above rules, TEOS scheduling policy is designed. The "Scheduling Policy" rule in SecDCF can be replaced by the following three rules:

1. **Threshold Calculation**. Scaled threshold is calculated locally using channel states information. The link information of other nodes are collected from their successful transmissions.
2. **TEOS Scheduling Policy**. In the case of a successful channel contention, current transmission rate for this link is calculated. A comparison between this rate and current threshold of this link is carried out by the scheduling policy. A positive result leads to a procedure of packet transmission. If current transmission rate is smaller than the threshold, the transmission opportunity is skipped, and the channel probing and contention continues.

3. **Physical Channel Adaption**. If a packet is allowed to be transmitted by the TEOS scheduling policy, the physical channel has to be adjusted according to the packet category. "PHY_ChToS.request" and "PHY_ChToR.request" have to be sent to the physical layer. It then follows the data transmission. Channel state information are also required to be broadcast as the first part of a successful transmission.

With the new SecDCF scheduling rules, QSOS can be utilized. In the following section, we provide simulations and analysis according to SecDCF implementation.

5.4.3 New Problems with TEOS

- The calculation of optimized threshold is based on the channel states of the entire network. Procedure should be specified for the derivation at the nodes' end.

5.4.4 TEOS Scheduling Policy

Following the above rules, the SecDCF protocol is designed as follows:

1. **Threshold Calculation**. Threshold is calculated using the channel states information which is broadcast by nodes within the propagation range.

2. **Scheduling Policy**. In the case of successful channel probing, the transmission only starts when the current transmission rate exceeds the threshold of this link. Each links hold its own threshold, no matter it is a secure link or a regular link. The transmission opportunity is dropped when it does not exceed the threshold. A successful transmission is ended by an ACK packet.

5.5 Numerical Results, Simulation and Conclusion

5.5.1 Numerical Results

TEOS is not used to optimize the network capacity. The major task for TEOS is to judge whether and how to achieve a set of thresholds. Thus, we first provide the numerical results to characterize the property of TEOS.

Obviously, times of iteration to achieve the fixed point is important in an iterative algorithm. We present an example of the iteration in Table 5.1. The accuracy level is four decimal places. One secure link as link 1 and two regular links as link 2 and 3 are denoted with the normalized SNR $\rho_s = 5$ and $\rho_s = 40$, respectively. $\overline{X}$ is assumed to be 20. The probing probability p_i is taken as 0.1. The required throughput is set as $\mu = \{0.5, 0.5\}$. Thus, we have found that after 5 rounds of iteration, the threshold set arrives the fixed point.

Table 5.1: Convergence behavior of TEOS algorithm

Link	s_0	s_1	s_2	s_3	s_4	s_5	s^*
link 1	20	2.5821	2.4677	2.4535	2.4522	2.4518	2.4518
link 2	20	4.7623	4.7004	4.6941	4.6933	4.6933	4.6933
link 3	20	4.7238	4.6972	4.6933	4.6933	4.6933	4.6933

To see the effective area of TEOS, we present a figure with numerical results as Fig.5.1. In the calculation, One secure link as link 1 and another regular links as link 2 are denoted with the normalized SNR $\rho_s = 5$ and $\rho_s = 40$, respectively. X_{max} is assumed to be 20. The probing probability p_i is taken as 0.5. By changing the required throughput, we can find out whether it can be achieved by TEOS.

Area A is the effective area of random access. According to the calculation result, the upper bound capacity of random access is at the point $\{1.5075, 0.75\}$. No more throughput requirement can be achieved in this area. Area C contains the requirements fail TEOS. It is out of the channel potential. Area B is the area where TEOS can provide its function.

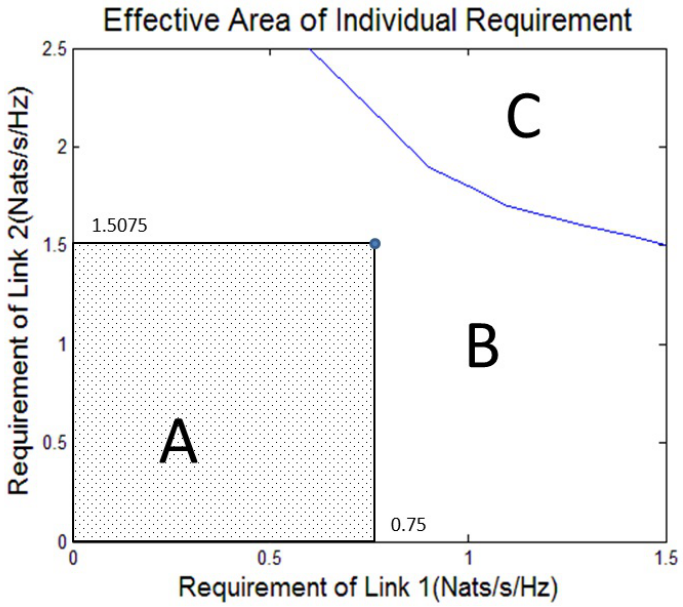

Figure 5.1: The Effective Area of TEOS

5.5.2 Simulation Results and Analysis

With the same condition we used in the numerical results, we simulate the scheduling scheme in our simulator. Similar to the simulation scenario in the other chapter, a one-hop ad-hoc network is implemented. We assume that 2 links exist in the network. An AWGN channel model with normalized SNR $\rho_1 = 5$ and $\rho_2 = 40$ are used for link 1 and link 2. A packet transmission duration is fixed as $t_p = 30$ time slots. Thus, we have the following results.

Threshold of link 1 is plotted in Fig.5.2. With these thresholds, link 1 can achieve its required throughput, as shown in Fig.5.4. When the requirement is too large to be handled in TEOS, i.e., in the area C of Fig.5.1, threshold does not exist, and the throughput is zero. For the requirement that can be satisfied with TEOS, the required throughput is achieved. Similar results are also shown in Fig.5.3 and Fig.5.5 for link 2.

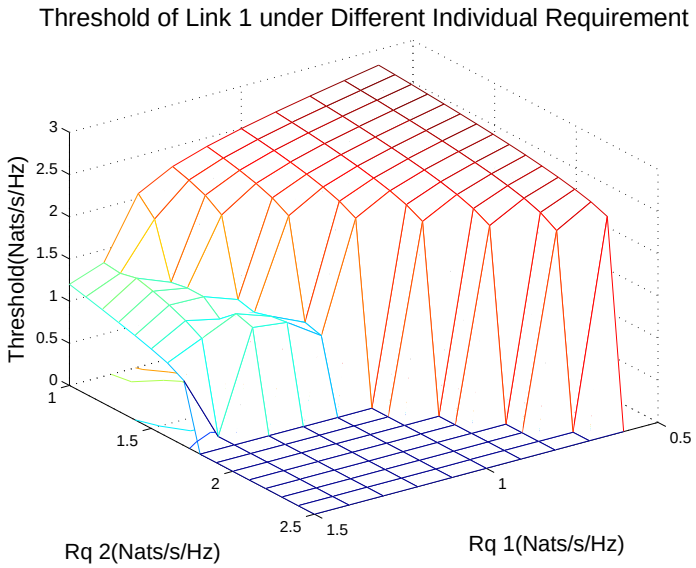

Figure 5.2: The threshold of link 1 under different individual requirements

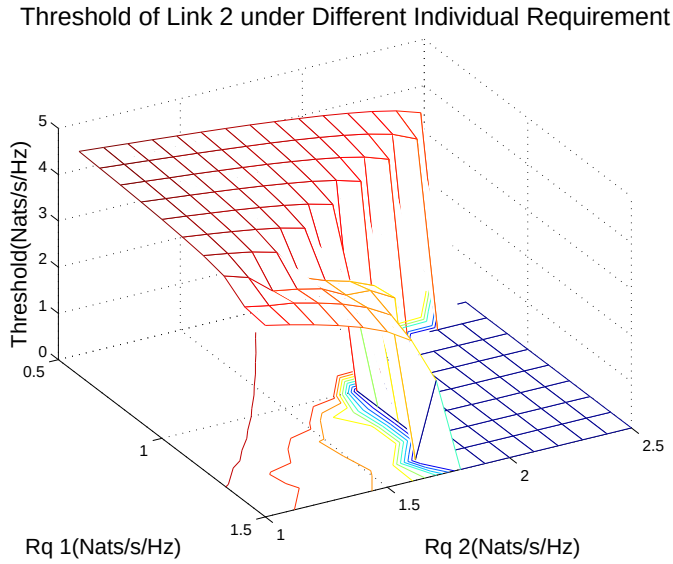

Figure 5.3: The threshold of link 2 under different individual requirements

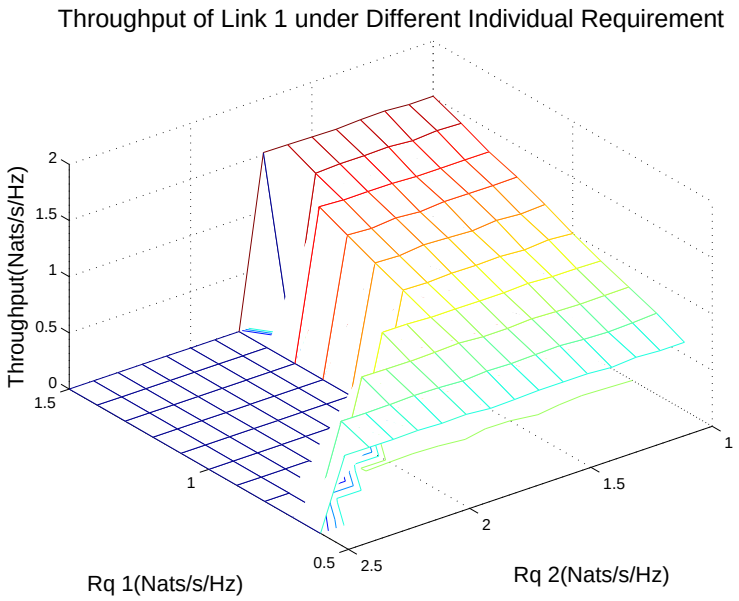

Figure 5.4: The throughput of link 1 under different individual requirements

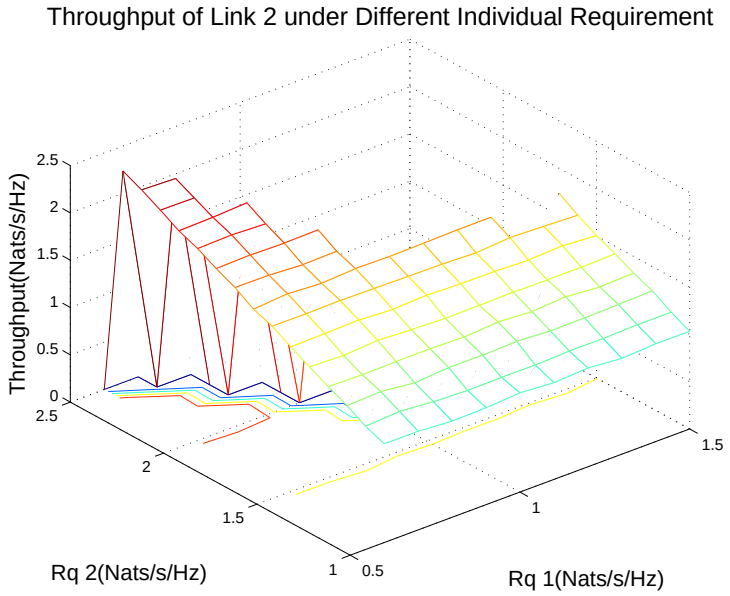

Figure 5.5: The throughput of link 2 under different individual requirements

5.5.3 conclusion

In this chapter, we have researched on the scheduling problem under the constraint of individual requirements. Capacity optimization is no longer our objective in this research. We try to find out whether it is possible to achieve a certain requirement with threshold enabled opportunistic scheduling, while random access cannot accomplish the scheduling task without causing congestion. This problem is more related to a common scheduling problem for a wireless ad-hoc network. We show that with an iterative algorithm, it is possible to accomplish more requirements with our TEOS comparing to random access. We also note that for those requirements that can never be achieved with limited channel resource, our mechanism can easily distinguish them by terminating the iteration in calculation.

After a long period of researches on the capacity optimization problems, the research in this chapter show that there still exist a lot of unsolved problem in real applications. We hope this initial research can provide the community an interesting topic.

Chapter 6

Sparing channel for time-critical Communications: using TEOS to Improve VANET QoS

In this dissertation, we have already covered a variety of network performance, i.e., security, throughput and individual requirement. However, delay performance has not been taken into consideration. In this chapter, we try to extend our research of TEOS to a more specific application scenario: the delay performance of time-critical traffic in a VANET (vehicular ad-hoc network) network. This extension is an initial attempt in VANET. Considering the special characteristics of VANET, it can not provide all-sided solution, but only a special application scenario in VANET.

To ensure the functionality of intelligent transportation, time-critical messages are of great importance in VANET. Meanwhile, non-time-critical traffic still exists in the network, with which regular services, e.g., orientation and navigation are provided. A key problem in VANET is to achieve best effort delay performance for time-critical traffic.

To achieve this object, a threshold policy derived from TEOS is used to reduce the transmission time of non-time-critical traffic. For randomly generated time-critical traffic, delay performance is ensured by providing the first transmission opportunity to it. Numerical results and simulations show that this approach can provide low-delay

time-critical transmissions for VANET.

6.1 Problem Formulation and System Model

6.1.1 Special Problem in VANET Network

Vehicular Ad-hoc Network which is also known as VANET, is an emerging branch of wireless ad-hoc network research. Due to the large requirement of intelligent transportation systems, it has attracted tremendous attentions from both research community and industries. Former researches like [51, 52, 53] have provided varied approaches to achieve better QoS in VANET. However, all these studies are focused on the higher layers of network structures in VANET. Little work has been done with MAC layer scheduling. As we have presented in the above chapters, opportunistic scheduling can be used to solve this kind of performance problem.

Comparing to the other wireless networks, links in VANET suffer a more frequent and wider-range of fluctuations due to the mobility of the nodes. It is a challenging problem, but also means that the uncertainty is rich, and larger improvements can be exploited. However, existing opportunistic scheduling schemes can not be applied to VANET directly. A major differences have to be addressed: throughput optimization is no longer the only goal in the design of VANET scheduling scheme. Balance among different traffic and performance requirements are also of great importance.

In our approach, a DiffServ model is applied. Obviously, throughput and delay are two most important parameters in VANET, and traffic with differential delay requirements and throughput requirements are always classified. For example, most of the communications are used to maintain the connections and report the vehicle conditions. This type of traffic is considered to be with stable throughput requirement, and is not time-critical. Emergency report is another type of traffic in VANET which is hard to predict and is time-critical. To this end, our goal is to provide optimized delay performance to time-critical traffic, while guaranteeing the throughput requirement of non-time-critical traffic at the same time.

In a distributed network, due to the lack of centralized control, transmission opportunity cannot be assigned voluntarily to the link with time-critical traffic. Thus, if the channel is congested, not only non-time-critical transmissions are affected, time-critical packet can hardly contend the channel as well. The only way for this problem is to improve the channel efficiency. When an optimized MAC layer scheduling scheme is applied, the congestion can be avoided for most of the time. Improvement of delay performance for time-critical traffic can be achieved. We have to note that our scheme can not provide efficient functionality if the throughput requirement of non-time-critical traffic is beyond the limitation of the channel capacity. Congestion controlling technology has to be deployed for this kind of conditions. It is beyond the scope of this study.

6.1.2 System model

In a VANET, there are multiple mobile nodes in the network. We assume that by implementing the power control technology, nodes can restrict the propagation of the communication signal within the range of their neighbors. Thus, only one-hop links between each pair of neighbor nodes are required. An AODV protocol [54] is deployed to form the multi-hop routing table. Furthermore, we assume that this network takes place in a high-speed freeway, and all the vehicles are with a similar speed. A demonstration of the network can be seen in Fig.6.1.

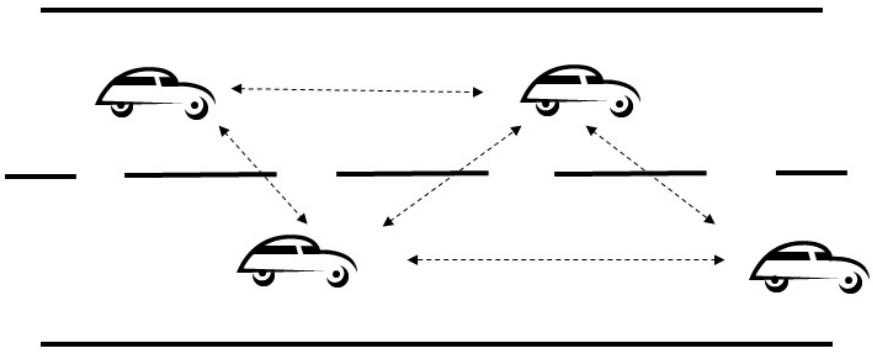

Figure 6.1: A demonstration of a VANET

For the convenience of mathematical derivation, we use the similar system model as used in the above chapters. N links presented by $\mathbf{\Omega} = \{1, 2, \ldots, N\}$ are assumed existed in the network. p_i denotes the average probability of channel probing attempts of link i. Due to the dynamics of wireless environment, we model the time-varied channel into a random variable X with p.d.f $f_X(x)$ and distribution function $F_X(x)$. We also assume that t_p is the data transmission duration and is no greater than the channel coherence time. To present the demand of non-time-critical traffic, we denote $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_N\}$ as the throughput requirement for each link in a certain period of time.

6.2 Mechanism to Spare Channel for Time-critical Traffic in VANET

Though the scheduling scheme of existing opportunistic scheduling is not suitable for VANET, the threshold policy still offers a solution for controlling the delay performance. Considering a VANET scenario with a regular requirement of non-time-critical transmissions, a majority of channel resource is used for transmitting these packets. While emergent time-critical packets arrive, they may be delayed due to the busy channel which is occupied by the non-time-critical transmissions or congestion. Thus, if the transmission time for non-time-critical transmissions can be reduced as much as possible, the delay performance of time-critical traffic can be boosted. In this section, the concept of TEOS is used for this purpose, and a corresponding scheduling policy is presented.

6.2.1 Delay Performance of Time-critical Packet Transmission

In VANET, time-critical transmissions are always used to handle emergency. As emergent situations can never be foretold, the arrival rate of time-critical traffic is stochastic. Obviously, when a time-critical packet arrives at MAC layer, the physical channel condition and the scheduling scheme are the only factors that matter the

delay performance. According to the statistics of regular non-time-critical traffic, the potential delay of an emergent time-critical packet can be estimated as follows.

When a time-critical packet arrives, the medium is for sure under either of three conditions: 1) packet transmission; 2) channel contention; 3) idle. If the channel is idle, the time-critical packet can be transmitted immediately. Thus, The major problems lie among the other two conditions.

As we denote the probability for each link i to probe for a non-time-critical packet as p_i, we have the probability for link i to successfully contend the channel as:

$$P_i = p_i \prod_{j \neq i} (1 - p_j). \tag{6.1}$$

Then we can have the overall probability for a successful channel contention as:

$$P_{succ} = \sum_{i}^{N} p_i \prod_{j \neq i} (1 - p_j). \tag{6.2}$$

Obviously, the number of slots for achieving a successful channel contention is a geometric random variable with the expectation of $1/P_{succ}$. It then follows that the expectation of the waiting duration for one successful channel contention can be denoted as $t_w = t/P_{succ}$. As a transmission duration of t_p follows directly after a successful channel contention, we have the expectation of one round channel contention and transmission as $t_w + t_p$. Therefore, a time-critical packet may arrive in MAC layer with probability $P_t = t_p/(t_w + t_p)$ when the channel is occupied by transmission. Also, with probability $P_w = t_w/(t_w + t_p)$, it may arrive when the channel is free for access. This part is similar to the description in chapter 5, and is presented here for the convenience of readers.

In an ordinary random access scheduling scenario, links with time-critical packets have to participate in the channel contention. Thus, the delay performance is really hard to be guaranteed. A common solution is to design special contention policy for these time-critical packets. Based on such consideration, we assume that p_c denotes the special channel contention probability for time-critical packets.

Thus, we can have the following successful channel contention probability P_c for time-critical packets when the channel is free

$$P_c = p_c \prod_{i=1}^{N} (1 - p_i). \tag{6.3}$$

Similar to the condition with non-time-critical traffic, we can have the expected waiting time for time-critical packet as $t_{w,c} = t/P_c$, while the channel is free of transmission. Then the overall expectation for delay can be presented as:

$$t_{e,c} = P_w \cdot t_{w,c} + P_t(t_{w,c} + E[t_p]) + t_p \tag{6.4}$$

The first part of $t_{e,c}$ is the expected delay time if the channel is free to access, and the second part represents the condition while another transmission takes place. The third part is the length of the packet. Therefore, the objective of our research turns to find out a mean for reducing $t_{e,c}$.

It follows that (6.4) can be further presented as:

$$t_{e,c} = \frac{t}{p_c \prod_1^N (1 - p_i)} + \frac{t_p}{t_w + t_p} \cdot \sum_{i=1}^{t_p} \frac{i}{tp} + t_p. \tag{6.5}$$

Clearly, $t_{e,c}$ is influenced by two major issues as shown in (6.5). The first issue is the probability of successful channel contention for time-critical packet. If the channel is busy, it takes more time to contend the channel. The second issue is t_w. If the channel is occupied by one transmission, it is impossible to stop this transmission immediately. The time-critical packet has to wait until the channel is free. The more probably channel is free, the less delay the time-critical traffic can achieve. Thus, to guarantee a better delay performance for time-critical traffic, two solutions can be used: 1) giving the time-critical traffic priority to contend the channel; 2) making the channel less busy. In the following section, we will try to find out how to use opportunistic scheduling to provide more spare time for time-critical traffic, which focus on the second approach.

6.2.2 Using Opportunistic Scheduling to Provide Optimized Channel Efficiency

Opportunistic scheduling is always considered as a method for improving throughput performance. However it is possible to use it for other purposes. For example, as optimized throughput can be achieved with opportunistic scheduling, we can say that the transmission rate is also maximized. If we can apply opportunistic scheduling in our VANET scenario, we can guarantee that required throughput is transmitted with the least time. To this end, the problem posed in the above section can be solved by opportunistic scheduling schemes.

In the last chapter, we have proved that individual threshold policy can be used to improve the throughput performance. Then TEOS can be used directly in this VANET scenario. From (6.5), we see that if we can augment t_w, a smaller $t_{e,c}$ can be achieved. Also, with individual threshold, denoted as T_i for link i, we have

$$P_{v,succ} = \sum_{i}^{N}(1 - F_X(T_i))p_i \prod_{j \neq i}(1 - p_j). \tag{6.6}$$

Then we have a smaller t_w, for $t_w = t/P_{v,succ}$. Thus, problem turns to be how to find the optimized threshold set $T = \{T_1, T_2, \ldots, T_N\}$ for all the links. Two objectives have to be achieved: 1) to provide the largest $t_{e,c}$; 2) to guarantee the required non-time-critical throughput $\boldsymbol{\mu}$.

6.2.3 Iterative Algorithm to Achieve minimum $t_{e,c}$

The derivation of the threshold set includes two phases. First, the iterative algorithm is presented. Second, a proof is given to show that the threshold set derived from the iterative algorithm can provide the minimum $t_{e,c}$.

First, we present the iterative algorithm to derive the threshold set for all the links. It is the same algorithm as we presented in the last chapter. We present it again for the convenience of the readers.

Two scales of iteration are used in this algorithm. In the large scale, we try to

approach a possible threshold set step by step, hereby, defined as step k. In the small scale, we derive the threshold for link i with the thresholds that have already been calculated in the current step k, e.g., $T_1^{(k)} \dots T_{i-1}^{(k)}$, and the thresholds that have not yet been renewed in the current step, e.g., $T_{i+1}^{(k-1)} \dots T_N^{(k-1)}$. While $k = 0$, we have the initial value for all the links as $T_1^{(0)} = T_2^{(0)} = \cdots = T_N^{(0)} = X_{max}$.

In step k, we have the following iteration for link i:

1. First, we denote $T_{-i} = \{T_1^{(k)}, T_2^{(k)}, \dots, T_{i-1^{(k)}}, T_{i+1}^{(k-1)}, \dots, T_N^{(k-1)}\}$. Derived from (A.18), we define:

$$g(T_i^*, T_{-i}) = -T_i^* - T_i^* P_{teos,succ} t_p + P_i t_p \int_{T_i^*}^{X_{max}} x \cdot f_X(x) dx. \tag{6.7}$$

   Then it is possible to have the optimized threshold T_i^* under the condition $g(T_i^*, T_{-i}) = 0$.

2. As presented in the proof of proposition 5.2, the unique solution T_i^* of $g(T_i^*, T_{-i}) = 0$ exists and is the optimized threshold for having the best S_{ave}^i under T_{-i}. Then we can calculate the current S_{ave}^i with (5.13).

3. Based on the comparison between current S_{ave}^i and μ_i, we can have the following judgement:

$$\begin{cases} \text{Iteration terminated, no solution,} & \text{if} \quad S_{ave}^i < \mu_i; \\ T_i^{(k)} = T_i^*, & \text{if} \quad S_{ave}^i = \mu_i; \\ \text{Find the maximal solution for} \quad S_{ave}^i(T_i^{(k)}, T_{-i}) = \mu_i, & \text{if} \quad S_{ave}^i > \mu_i. \end{cases} \tag{6.8}$$

4. If the algorithm does not terminate, go on the same procedure to calculate for the link $i + 1$ in step k. If it is already the last link in step k, move on to the step $k + 1$. If fixed points have arrived for all thresholds in T^k, the algorithm stops, and the current T^k is a solution to the scheduling problem.

The proof has already been provided, and is not included in this chapter. For the purpose of this VANET scenario, we have a new proposition:

Proposition 6.1 *The fixed point* $\{T_1^*, T_2^*, \ldots, T_N^*\}$ *derived from above algorithm holds the largest threshold for all the link, e.g.,*

$$T_i^* > T_i^\dagger, \forall \quad i, \text{ and } T_i^\dagger \text{ is a threshold from a solution set } T^\dagger. \tag{6.9}$$

Proof: The proof can be found in Appendix A.7.

Remark: From the proof, it is easy to see that even if there exists multiple solution sets, the one we derived from the iterative algorithm is the largest one. Thus, it is possible to have the best channel efficiency for the non-time-critical traffic. On the other hand, the time-critical traffic can always hold the best delay performance in this distributed scheduling scenario.

As the implementation of TEOS policy is provided in the last chapter, we do not repeat it here. However, it has to be noted that a real VANET can be much more complicated. To fully support such a VANET application, there is still a lot of research to be done. It needs the cooperation of the whole research community.

6.3 Numerical Results and Analysis

6.3.1 Analysis Scenario

VANET systems are multiform, and the simulation is therefore complicated. As this chapter is only a first-step attempt, we are not ambitious to cover too many aspects. A numerical analysis is initiated in a special case as depicted in the system model. AWGN channel with normalized SNR $\rho = 40$ is used for non-time-critical traffic in 3 links. The traffic load is measured by the channel probing probability p_i. With different p_i, the delay performance of time-critical traffic is different. The requirement of non-time-critical traffic is also important in the analysis, it is pre-fixed in different analysis.

Time-critical traffic is assumed to arrive stochastically. A packet transmission duration is fixed as $t_p = 50$ time slots. As used in the last chapter, channel contention mechanism for avoiding collisions is integrated with channel probing. If in one time slot there is only one link who performs the channel probing, it not only probes the

channel information, but also successfully contends the channel. A transmission may be carried on in the following time slot by this link.

6.3.2 Results and Analysis

First, we examine the influence of channel probing probability. If the requirement is fixed as $0.5Nats/s/Hz$, the threshold in TEOS can be different if we change the channel probing probability of non-time critical traffic. In Table.6.1, we show the threshold value for different traffic load.

Table 6.1: Threshold under Different Channel Contention Probability

p_i	0.05	0.1	0.15	0.2	0.25
Threshold	4.4868	4.7406	4.8447	4.8994	4.9289
p_i	0.3	0.35	0.4	0.45	0.5
Threshold	4.9425	4.9443	4.9362	4.9188	4.8918

In Table.6.2, a improvement of delay performance with TEOS is presented. Similar to the derivation above, the channel probing probability increases from 0.05 to 0.5. When TEOS is used in the system, the delay performance of time-critical traffic can be guaranteed. For the channel is spared for them. It is interesting that the biggest threshold leads to the best performance improvement in the system.

Table 6.2: Delay Performance Condition under Different Channel Contention Probability

p_i	0.05	0.1	0.15	0.2	0.25
Time Slots Spared	33.28	35.85	36.88	37.41	37.7
Delay Performance Improved	9.44	10.6	11.06	11.29	11.41
p_i	0.3	0.35	0.4	0.45	0.5
Time Slots Spared(%)	37.83	37.85	37.77	37.6	37.34
Delay Performance Improved(%)	11.47	11.48	11.44	11.37	11.26

Chapter 7

Conclusion and Perspective

7.1 Conclusion

In this thesis, four parts of my research work are presented. It follows the idea that rich physical layer and MAC layer characteristics can be exploited to provide better service quality in wireless ad-hoc network. Physical layer security is introduced into the system to guarantee the network security. Correspondingly, a MAC layer scheduling framework called SecDCF is invented to handle the multiple physical layer coordination. To solve throughput and fairness problem, a scaled function is proposed, and a QoS-Secure-oriented Opportunistic Scheduling scheme is developed to guarantee both security and throughput in the network. Further researches are conducted to handle a more practical situation in wireless ad-hoc network. Individual requirements are considered in our TEOS scheme. An iterative algorithm is then developed for providing better adaptability for the system. A special case in VANET also shows that TEOS can be used to provide better delay performance from another perspective of view.

As a conclusion, the contribution in this thesis can be listed as follows:

1. SecDCF To apply physical layer security and opportunistic scheduling in wireless ad-hoc network at the same time, a MAC layer scheduling framework called SecDCF (Secure Distributed Controlling Function) is designed. Prototype secure physical layer realization is considered. On the other hand, a special design

for allowing integrating opportunistic scheduling policies into this framework is also presented to support our further research.

2. Scheme called QSOS (QoS-Secure-oriented Opportunistic Scheduling) is designed to provide throughput optimization and fairness among different links. Corresponding policy is simulated and verified in SecDCF to show that QSOS can outperform traditional scheduling schemes in this new scenario.

3. As capacity optimization is not the only concern in network design, diversified link requirements from both secure and regular links are taken into account. A new scheme called TEOS (Threshold Enabled Opportunistic Scheduling) is proposed by us to provide more delicate scheduling for each link. Also, we provide a method to judge if a set of throughput requirement can be achieved.

4. To show the capability of TEOS, a VANET scenario is presented with time-critical traffic and non-time-critical traffic. We show that by applying TEOS, we can provide better delay performance to time-critical traffic, while throughput performance of non-time-critical traffic is not affected.

7.2 Future works

The presentation in this dissertation is near its end, however, the future research work will never end. A major concern about the technology development is that someday we will hold something too powerful to be controlled by ourselves. I don't know if it would come true, yet what I am sure is that we are making our lives better and better, and that is what inspires us to climb the peak of the science.

During my research, the unstable and unpredictable secure physical channel is always a big concern. It is my motivation of applying opportunistic scheduling with physical layer security. However, it is only an initial research. Physical layer security will be a big part of my future work, and I would like to try some testbed for realizing an applicable secure physical layer.

On the other hand, TEOS is also a good topic to advance. As the community is attracted by derivation of capacity, TEOS shows that there is also another research

path that opportunistic scheduling can be applied. It will be another major topic of my future research.

Appendix A

Proof

A.1 Proof of Proposition 4.1

As (4.3) is formulated as the same form of Proposition 3.1 in [12], the proof can be applied directly to our proposition. It has to be noted that this proof is not a part of our contribution in the research. It is presented here as a necessary background knowledge.

The proposition is proved based on the theorem 1 of chapter 6 in [50]. To find out a way for maximizing the average $\frac{E[S_V t_p]}{E[T_V]}$, it is important to find the optimal stopping algorithm $V(s)$ such that

$$D^*(s) = E[R_{V(s)}t_p - sT_{V(s)}] = \sup_{V \in Q} E[R_V t_p - sT_V]. \tag{A.1}$$

According to theorem 1 in chapter 3 of [50], this policy $V(s)$ exists if we have the following conditions:

$$E \sup_n Z_n < \infty, \quad and \quad \limsup_{n->\infty} Z_n = -\infty \quad a.s., \tag{A.2}$$

where $Z_n = S_n t_p - s(\sum_{j=1}^{n} K_j t + t_p)$, and K is the number of time slots used for achieving a successful channel probing.

(A.2) can be proved according to the theorem 2 in chapter 4 of [50]. Thus, the

existence of $V(s)$ is proved, and the only problem is to find out the optimal policy V^*. The policy set $V_{(s)}$ can be presented as:

$$V(s) = \min\{n \geq 1 : R_n t_p \geq D^*(s) + st_p\}, \tag{A.3}$$

and $D^*(s)$ satisfies the optimality equation as:

$$E[\max(R_n t_p - st_p - Kst, D^*(s) - Kst)] = D^*(s). \tag{A.4}$$

As $D^*(s) = 0$ according to theorem 1 of chapter 6 in [50], we can simplify (A.4) as $E[R_n - s^*]^+ = \frac{s^* t}{t_p \sum_{i=1}^{N} P_i}$. The uniqueness of the solution can be easily derived by using Dominated Convergence Theory in [55]. Thus, the proposition is proved.

A.2 Proof of Proposition 4.2

First, we prove the existence of optimal throughput. It is clear that the numerator in (4.11) has an upper boundary, because it is the expectation of transmission rate. Also we can see that the denominator has a lower boundary as $\frac{t}{t_p}$. Thus, there is an upper boundary of the right hand side of (4.11), which is the optimal throughput. Thus, the weight w_v^* at this point of optimal throughput is the optimal weight.

Following the definition, the optimal throughput is the maximum point of this function. Thus, the derivative at this point is equal to zero as:

$$\frac{\mathrm{d}Z_v^*(w_v, w_{-v})}{\mathrm{d}w_v} = 0 \tag{A.5}$$

It then follows that:

$$-P_v w_v \lambda_v s^* F_v'(w_v \lambda_v s^*)[\frac{t}{t_p} + \sum_{j=1}^{N} P_j(1 - F_j(w_j \lambda_j s^*))] + P_v \int_{w_v \lambda_v s^*}^{\infty} r \mathrm{d}F_v(r) \cdot F'(w_v \lambda_v s^*) = 0, \tag{A.6}$$

which can be finally derived as:

$$w_v\lambda_v s^* = \frac{P_v \int_{w_v\lambda_v s^*}^{\infty} r\mathrm{d}F_v(r)}{\frac{t}{t_p} + \sum_{j=1}^{N} P_j(1 - F_j(w_j\lambda_j s^*))}. \tag{A.7}$$

It is exactly the same form as (4.11), which means the two curves $y = Z_v^*(w_v, w_{-v})$ and $y = x$ intersects at the maximum point. The convergence of this algorithm is similar to the iterative algorithm of Proposition 4.1, and is not repeated here.

A.3 Proof of Proposition 4.3

Considering the definition of pareto optimality, the optimality point is achieved while no pareto improvement exists. In the scenario of a two-link network, we assume that the weight of one link is fixed, i.e. the weight w_1 of link 1. It has been proved in Proposition 4.2 that the optimal point of the overall throughput exists. Then for link 2, the weight we use to achieve this optimal throughput can be calculated, and there is no pareto improvement at this weight. The case is the same if we fix the weight w_2 of link 2. We define $W_1 = w_1 s^* \lambda_1$ and $W_2 = w_2 s^* \lambda_2$. According to (4.10) and (4.11), we denote the overall throughput as follows:

$$Z(W_1, W_2) = \frac{P_1 \int_{W_1}^{\infty} r\mathrm{d}F_1(r) + P_2 \int_{W_2}^{\infty} r\mathrm{d}F_2(r)}{\frac{t}{t_p} + P_1(1 - F_1(W_1)) + P_2(1 - F_2(W_2))}. \tag{A.8}$$

Thus, we can have the following equation:

$$\frac{\mathrm{d}Z(W_1, W_2)}{\mathrm{d}W_1} = 0, \tag{A.9}$$

and

$$\frac{\mathrm{d}Z(W_1, W_2)}{\mathrm{d}W_2} = 0. \tag{A.10}$$

It then follows

$$W_1 = \frac{P_1 \int_{W_1}^{\infty} r\mathrm{d}F_1(r) + P_2 \int_{W_2}^{\infty} r\mathrm{d}F_2(r)}{\frac{t}{t_p} + P_1(1 - F_1(W_1)) + P_2(1 - F_2(W_2))} \tag{A.11}$$

and

$$W_2 = \frac{P_1 \int_{W_1}^{\infty} r \mathrm{d}F_1(r) + P_2 \int_{W_2}^{\infty} r \mathrm{d}F_2(r)}{\frac{t}{t_p} + P_1(1 - F_1(W_1)) + P_2(1 - F_2(W_2))}, \tag{A.12}$$

which means $W_1 = W_2$. As the two curves $y = Z^*(W_1, W_2)$ and $y = x$ intersects at the maximum point, we have proved this proposition.

A.4 Proof of Proposition 5.2

Derived from (5.13), we can have

$$S_{ave}^i = \frac{t_p}{t_w^i + t_w^i \cdot P_{teos,succ} \cdot t_p} \int_{T_i}^{\overline{X}} x \cdot f_X(x) dx \tag{A.13}$$

$$= \frac{t_p \cdot p_i \prod_{j \neq i}(1 - p_j)}{t + t_p \sum_{k=1}^{N}(1 - F_X(T_k)) p_k \prod_{j \neq k}(1 - p_j)} \int_{T_i}^{\overline{X}} x \cdot f_X(x) dx. \tag{A.14}$$

To examine the influence of threshold set $\mathbf{T_o}$, we have to see how T_i and $T_j (j \neq i)$ affect S_{ave}^i. As we have

$$\frac{\partial S_{ave}^i}{\partial T_j} = \frac{P_i t_p^2 P_j f_X(T_j) \int_{T_i}^{\overline{X}} x \cdot f_X(x) dx}{(t + t_p P_{teos,succ})^2} \geq 0, \tag{A.15}$$

it is clear that the existence of T_j can provide better effective transmission rate for link i.

Then the only problem is T_i. As we have

$$\frac{\partial P_{teos,succ}}{\partial T_i} = -P_i f_X(T_i), \tag{A.16}$$

so

$$\frac{\partial S_{ave}^i}{\partial T_i} = \frac{P_i t_p f_X(T_i)[-T_i t - T_i P_{teos,succ} t_p + P_i t_p \int_{T_i}^{\overline{X}} x \cdot f_X(x) dx]}{(t + t_p P_{teos,succ})^2}. \tag{A.17}$$

In this case, we only have to examine $g(T_i)$ as follows:

$$g(T_i) = -T_i t - T_i P_{teos,succ} t_p + P_i t_p \int_{T_i}^{\overline{X}} x \cdot f_X(x) dx. \tag{A.18}$$

It can be derived that

$$g^{'}(T_i) = -t - P_{teos,succ} t_p < 0, \tag{A.19}$$

which means $g(T_i)$ is strictly descending. Thus, the maximizer is at $g(T_i) = 0$, and if $g(\underline{X}) > 0$, there is always a maximizer T_i.

As a consequence, we need to make sure that $g(\underline{X}) > 0$, i.e.,

$$-\underline{X} t - \underline{X} P_{teos,succ} t_p + P_i t_p \int_{\underline{X}}^{\overline{X}} x \cdot f_X(x) dx > 0. \tag{A.20}$$

So we need

$$P_i t_p (\int_{\underline{X}}^{\overline{X}} x \cdot f_X(x) dx - \underline{X}) > (t + \sum_{j \neq i} P_j t_p) \underline{X}. \tag{A.21}$$

After the organization, (A.21) is surprisingly as follows:

$$S_{ave}^{i} > \underline{X}. \tag{A.22}$$

As a conclusion, we can say that if (A.22) can be satisfied, it is for sure there exists a threshold policy which can provide better throughput for link i. However, it is possible that some of the links in the network is with very bad channel condition, or the probing probability is rather small. For these links, we can use $\underline{X}$ as the corresponding threshold. While k ($k < N$) links in the network are not in such terrible condition, we can still have a better throughput for all the links. For we have:

$$S^i_{ave}(T_i = \underline{X}) = \frac{t_p}{t^i_w + t^i_w \cdot P_{teos,succ} \cdot t_p} \int_{T_i}^{\overline{X}} x \cdot f_X(x)dx > S^i_{ran}, \quad \forall S^i_{ran} \leq \underline{X}. \quad \text{(A.23)}$$

If none of the links in the network can satisfy (A.22), which means that all the links are with very bad condition. The only solution is to stay with random access. However, this is negligible and trivial for the study in this paper.

A.5 Proof of Proposition 5.3

First, we prove that the iterative algorithm converges to a certain point. As we have shown in Appendix A.4, $g(T_i)$ is strictly descending. Following the iterative algorithm, we can prove that $T_i^{(k+1)} \leq T_i^{(k)}$. Also, it is clear that all threshold sets $\{\mathbf{T}\}$ have lower bounds according to the individual requirement μ and the optimized algorithm. Thus, if the algorithm does not terminate, it converges to a certain threshold set.

Second, we prove that the iteration can achieve a fixed point according to the algorithm, and this fixed point must satisfy the following two terms for all i:

$$\begin{cases} g(T_i) \leq 0; & (a) \\ S^i_{ave}(\mathbf{T}) = \mu_i. & (b) \end{cases} \quad \text{(A.24)}$$

Next we prove that for a threshold set satisfying (A.24), it is a fixed point of the algorithm. We assume that $\mathbf{T}^* = \{T_1^*, T_2^* \ldots, T_N^*\}$ is a threshold set for the problem. As we can get the unique $\tilde{T}_1^*$ from $g(\tilde{T}_1^*, T_{-1}) = 0$, and obviously,

$$S^i_{ave}(\tilde{T}_1^*, T_{-1}) \geq S^i_{ave}(T_1^*, T_{-1}) = \mu_1. \quad \text{(A.25)}$$

If we have $S^i_{ave}(\tilde{T}_1^*, T_{-1}) = \mu_1$, then $\tilde{T}_1^* = T_1^*$. If $S^i_{ave}(\tilde{T}_1^*, T_{-1}) > \mu_1$, according to (A.24).a, we can find the unique $T_1 > \tilde{T}_1^*$, so that

$$S^i_{ave}(T_1, T_{-1}) = S^i_{ave}(T_1^*, T_{-1}). \quad \text{(A.26)}$$

Thus, we have $T_1 = T_1^*$, and we do not change T_1^*. Similarly, we do not change

$T_2^*, \ldots, T_N^*$ under the algorithm. It is a fixed point for this iteration. We have proved the existence of the fixed point.

Then we prove that if $\mathbf{T}^*$ is a fixed point, it has to satisfy (A.24). We assume that issue (A.24).b can not be satisfied, then we have two possible situations:

1. $\exists i$, $s.t.$ $S_{ave}^i < \mu_i$, then the iteration should terminate;

2. $\exists i$, $s.t.$ $S_{ave}^i > \mu_i$, then we can find the unique $T_i > T_i^*$ that can satisfy $S_{ave}^i = \mu_i$.

Obviously, it is contradicted to the assumption. Thus, item (A.24).b should always be satisfied.

Then assuming that issue (A.24).a can not be satisfied, we have the following situation: $\exists i$, $s.t.$ $T_i^* < S_{ave}^i$. We can always find a unique T_i, so that we can have $T_i > T_i^*$ and $T_i^* = S_{ave}^i$. Again, it is contradicted to the assumption. Thus, item (A.24).a should always be satisfied.

Furthermore, we show that the converge point of the algorithm can satisfy (A.24).

1. For item (A.24).a, it always holds as required in the algorithm.

2. For item (A.24).b, as we always have $S_{ave}^i = \mu_i$, it is always satisfied. Otherwise, the iteration terminates.

Thus, this algorithm converges to a fixed point according to the iterative algorithm. It is obvious that this fixed point is a solution as it satisfies (A.24). Thus, we have proved the proposition.

A.6 Proof of Proposition 5.4

We assume that the iteration stops during step k with link $i(1 \leq i \leq N)$. According to the terminate condition, we have

$$S_{ave}^i(T_1^{(k)}, T_2^{(k)}, \ldots, T_{i-1}^{(k)}, T_i^*, T_{i+1}^{(k-1)}, \ldots, T_N^{(k-1)}) < \mu_i. \tag{A.27}$$

Since

$$\frac{\partial S^i_{ave}}{\partial T_j} > 0, \forall j \neq i, \tag{A.28}$$

it is clear that S^i_{ave} is increasing with T_j. As a result, for those

$$\begin{aligned} T_1 \leq T_1^{(k)}, \quad \ldots, \quad T_{i-1} \leq T_{i-1}^{(k)}, \\ T_{i+1} \leq T_{i+1}^{(k-1)}, \quad \ldots, \quad T_N \leq T_N^{(k-1)}, \end{aligned}$$

there is no such $\mathbf{T}$ that can satisfy $S^i_{ave}(\mathbf{T}) \geq \mu_i$.

Thus, to satisfy the requirement μ_i, we need another threshold set for a larger S^i_{ave}. It is clear that we need to increase at least one of $T_1^{(k)}, T_2^{(k)}, \ldots, T_{i-1}^{(k)}, T_{i+1}^{(k-1)}, \ldots, T_N^{(k-1)}$. We suppose $\mathbf{T}^* = \{T_1^*, T_2^*, \ldots, T_{i-1}^*, T_i^*, T_{i+1}^*, \ldots, T_N^*\}$ is such a solution. Then by the above argument, there exist at least one of T_j^* $(j \neq i)$, such that

$$\begin{aligned} T_j^* > T_j^{(k)}, \quad \text{if} \quad j < i, \\ T_j^* > T_j^{(k-1)}, \quad \text{if} \quad j > i. \end{aligned}$$

For these T_j^*, we can always find out k_j satisfying:

$$T_j^{(k_j+1)} < T_j^* \leq T_j^{(k_j)}, \quad 0 \leq k_j \leq k-1. \tag{A.29}$$

For the other T_j^*, we set k_j as k. Then let $m = \min_{1 \leq j \leq N}\{k_j\}$, and $j^* = \min\{j, \text{where } k_j = m\}$.

Then,

$$\begin{cases} 1 \leq n \leq j^* - 1, & T_n^* \leq T_n^{(m+1)} \\ n = j^*, & T_n^{(m+1)} < T_n^* \leq T_n^{(m)} \\ n \geq j^* + 1, & T_n^* \leq T_n^{(m)} \end{cases}$$

Thus, we have

$$S_{ave}^{j^*}(T_1^*, T_2^*, \ldots, T_N^*) \leq S_{ave}^{j^*}(T_1^{(m+1)}, T_2^{(m+1)}, \ldots, T_{j^*-1}^{(m+1)}, T_{j^*}^*, T_{j^*+1}^{(m)}, \ldots, T_N^{(m)}) < \mu_{j^*}. \tag{A.30}$$

Since $T_{j^*}^* > T_{j^*}^{(m+1)}$, this is a contradiction.

Thus, we have proved that there is no solution if the algorithm terminates in the iteration.

A.7 Proof of Proposition 6.1

By contradiction, we assume that $T^\dagger$ is a solution set such that at least one of $T_i^\dagger > T_i^*$. Then we construct the following condition.

For $1 \leq i \leq N$, if $T_i^\dagger \leq T_i^*$, set $k_j = \inf$; for those $T_i^\dagger > T_i^*$, there exists a unique k_j, such that we have:

$$T_i^{(k_j+1)} < T_i^* \leq T_i^{(k_j)}. \tag{A.31}$$

Let

$$m = \min_{1 \leq j \leq N} \{k_j\}. \tag{A.32}$$

It is clear that m is infinite according to the assumption. Let

$$j^* = \min\{1 \leq j \leq N, \quad \text{s.t.} \quad k_j = m\}. \tag{A.33}$$

Thus, we have

$$T_{j^*}^{(m+1)} < T_{j^*}^* \leq T_{j^*}^{(m)}. \tag{A.34}$$

It then follows that

$$S_{ave}^{j^*}(T_1^\dagger, T_2^\dagger, \ldots, T_N^\dagger) \leq S_{ave}^{j^*}(T_1^{(m+1)}, T_2^{(m+1)}, \ldots, T_{j^*-1}^{(m+1)}, T_{j^*}^*, T_{j^*+1}^{(m)}, \ldots, T_N^{(m)}) < \mu_{j^*}. \tag{A.35}$$

This is a contradiction to the assumption that $T^\dagger$ is a solution set.

References

[1] J. Wu and I. Stojmenovic, "Ad hoc networks," *IEEE Computer*, vol. 37, no. 2, pp. 29–31, 2004.

[2] W. Kiess and M. Mauve, "A survey on real-world implementations of mobile ad-hoc networks," *Ad Hoc Networks*, vol. 5, no. 3, pp. 324–339, 2007.

[3] R. Rajaraman, "Topology control and routing in ad hoc networks: A survey," *ACM SIGACT News*, vol. 33, no. 2, pp. 66–73, 2002.

[4] I. Chlamtac, M. Conti, and J. Liu, "Mobile ad-hoc networking: imperatives and challenges," *Ad Hoc Networks*, vol. 1, no. 1, pp. 13–64, 2003.

[5] D. Miorandi, S. Sicari, F. Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[6] J.-P. Hubaux, L. Buttyan, and S. Capkun, "The quest for security in mobile ad hoc networks," *ACM Symposium on Mobile Ad Hoc Networking and Computing*, 2001.

[7] D. Djenouri, L. Khelladi, and N. Badache, "A survey on security issues in mobile ad hoc and sensor networks," *IEEE Commun. Surveys and Tutorials*, vol. 7, no. 4, 2005.

[8] E. Cayirici and C. Rong, "Security in wireless ad hoc and sensor networks," *Wiley*, 2009.

[9] L. Hanzo and R. Tafazolli, "A survey of qos routing solutions for mobile ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 9, no. 2, pp. 50–70, 2007.

[10] S. Kumar, V. Raghavan, and J. Deng, "Medium access control protocols for ad hoc wireless networks: a survey," *Ad Hoc Networks*, vol. 4, no. 3, pp. 326–358, May, 2006.

[11] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, 2006.

[12] D. Zheng, W. Ge, and J. Zhang, "Distributed opportunistic scheduling for ad-hoc networks with random access: an optimal stopping approach," *IEEE Trans. Inform. Theory*, vol. 55, no. 1, 2009.

[13] D. SUN, X. WANG, Y. Zhao, and Y. Wu, "Secdcf: An optimized cross-layer scheduling scheme based on physical layer security," *Proc. ICC 2011*, 2011.

[14] D. SUN, Y. WU, L. YANG, and J. LI, "Exploring threshold enabled opportunistic scheduling under individual throughput requirement," *Submitted to ICC'2013*, 2012.

[15] D. SUN, H. BENABOUD, and N.MIKOU, "A research on opportunistic scheduling in wireless ad-hoc networks with physical layer security," *Submitted to Security and Communication Networks*, 2012.

[16] D. SUN, H. BENABOUD, and N.MIKOU, "Exploring opportunistic scheduling in ad-hoc network with physical layer security," *Proc. JNS2 2012*, 2012.

[17] D. A. Bayer, "Accomplishments of the darpa suran program," *Proceeding, Military Communications Conference, 1990. MILCOM '90,*, vol. 2, pp. 855–862, 1990.

[18] D. Welch and S. Lathrop, "Wireless security threat taxonomy," *Proc. IEEE Systems, Man and Cybernetics Society Information Assurance Workshop*, pp. 76–83, 2003.

[19] R. Negi and S. Goel, "Secret communication using artificial noise," *Proc. VTC Fall 2005*, vol. 3, pp. 1906–1910, 2005.

[20] E. Tekin and A. Yener, "The general gaussian multuple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. on Inform. Theory*, vol. 54, no. 6, 2008.

[21] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[22] C. E. Shannon, "Communication theory of secrecy systems," *Bell Sys. Tech. Journ.*, vol. 28, pp. 656–715, 1949.

[23] C. Peiket, "Theoretical foundations of cryptography," 2010. Available as: "https://wiki.cc.gatech.edu/theory/images/1/1f/Lec2.pdf".

[24] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 24, pp. 339–348, 1978.

[25] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," 2010. Available as: arXiv:1011.3754.

[26] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wire-tap channel," *IEEE Trans. on Information Theory*, vol. 24, pp. 451–456, 1978.

[27] R. Liu and W. Trappe, eds., *Securing wireless communications at the physical layer*. Springer Pub.

[28] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," *Proc. of ISIT 2006*, 2006.

[29] X. Zhou and M. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *Proc. on Int. Conf. on Signal Processing and Commun. Syst.*, 2009.

[30] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, no. 5255, 2000.

[31] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," *Proc. IEEE ICASSP*, pp. 3013–3016, 2008.

[32] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," *Proc. MobiCOM 2008*, 2008.

[33] S. Bellofiore, C. Balanis, J. Foutz, and A. S. Spanias, "Smart-antenna systems for mobile communication networks," *Antennas and Propagation Magazine, IEEE*, vol. 44, no. 3, pp. 145–154, 2002.

[34] X. Zhou, R. Ganti, and J. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE TRANS. on WIreless Communiations*, vol. 10, no. 2, pp. 425–430, 2011.

[35] O. Edfors, M. Sandell, J.-J. van de Beek, S. Wilson, and P. Borjesson, "Ofdm channel estimation by singular value decomposition," *IEEE TRANS. on Communiations*, vol. 46, no. 7, pp. 931 – 939, 1998.

[36] S. Coleri, M. Ergen, A. Puri, and A. Bahai, "Channel estimation techniques based on pilot arrangement in ofdm systems," *IEEE TRANS. on Broadcasting*, vol. 48, no. 3, pp. 223 – 229, 2002.

[37] M. Grossglauser and D. N. C. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM TRANSACTIONS ON NETWORKING*, vol. 10, no. 4, pp. 477–486, 2002.

[38] R. Knopp and P. A. Humblet, "Information capacity and power control in single-cell multiuser communications," *Proc. Int. Conf. Communications*, vol. 1, pp. 331–335, 1995.

[39] D. Tse, "Optimal power allocation over parallel gaussian channels," *Proc. Int. Symp. Information Theory*, 1997.

[40] X. Liu, E. Chong, and N. Shroff, "A framework for opportunistic scheduling in wireless networks," *Computer Networks*, vol. 41, no. 4, 2003.

[41] S. Borst, "User-level performance of channel-aware scheduling algotirthms in wireless data networks," *Proc. IEEE INFOCOM03*, 2003.

[42] S. Patil and G. de Veciana, "Measurement-based opportunistic scheduling for heterogenous wireless systems," *IEEE TRANSACTIONS ON COMMUNICATIONS*, vol. 57, no. 9, 2009.

[43] A. Gyasi-Agyei, "Multiuser diversity based opportunistic scheduling for wireless data networks," *Communications Letters*, vol. 9, no. 7, 2005.

[44] D. Aguayo, J. Bicket, S. Biswas, G. Judd, and R. Morris, "Link-level measurements from an 802.11b mesh network," *Proceedings of ACM Annual Conference of the Special Interest Group on Data Communication 2004 (SIGCOMM'04)*, 2004.

[45] S. Tan, D. Zheng, J. Zhang, and J. Zeidler, "Distributed opportunistic scheduling for ad-hoc communications under delay constraints," *Proceedings of IEEE INFOCOM 2010*, March, 2010.

[46] Vocal, "802.11 distributed coordination function (dcf)," 2012. Available as: "http://www.vocal.com/networking/802-11-distributed-coordination-function-dcf/".

[47] M. S. Gast, ed., *802.11Wireless Networks: The Definitive Guide*. O'Reilly.

[48] H. Harada and R. Prasad, eds., *Simulation and software radio for mobile communications*. Artech House.

[49] T. Li, D. Leith, and D. Malone, "Buffer sizing for 802.11-based networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 19, no. 1, pp. 156–169, 2011.

[50] T. Ferguson, "Optimal stopping and applications," 2008. Available as: "http://www.math.ucla.edu/tom/Stopping/contents.html".

[51] Y. He and H. Abdel-wahab, "Hqmm: A hybrid qos model for mobile ad-hoc networks," *Proc. 11th IEEE symposium on Computers and Communications*, 2006.

[52] R. Liu, G. Cao, J. Zhang, P. Song, and B. Cui, "Research on dynamic web services management based on qos," *JDCTA*, vol. 4, no. 5, pp. 55–61, 2010.

[53] W. Almobaideen, K. Hushaidan, A. Sleit, and M. Qatawneh, "A cluster-based approach for supporting qos in mobile ad hoc networks," *JDCTA*, vol. 5, no. 1, pp. 1–9, 2011.

[54] C. Perkins and E. Royer, "Ad hoc on demand distance vector (aodv) algorithm," *Proc. WMCSA'99*, pp. 90–100, 1999.

[55] Y. Chow, H. Robbins, and D. Siegmund, eds., *Great Expectations: Theory of Optimal Stopping*. Houghton Mifflin.

SUN Donglai

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(MIKOU Noufissa) Principal Adviser

Approved for the University Committee on Graduate Studies
