IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, Oct-Nov, 2013
ISSN: 2320 - 8791
www.ijreat.org

A Priority And Fair Connection Based Opt Packet Scheduling In Ieee 802.11 Based Mesh Topology

Mrs.Sajini.S
Assistant Professor
Department of Computer Science and Engineering
S.A Engineering College, Chennai

***Abstract*— Modern real-time wireless networks require high security level to assure confidentiality of information stored in packages delivered through wireless links. However, most existing algorithms for scheduling independent packets in real-time wireless networks ignore various security requirements of the packets. Also, Packet transmission scheduling for supporting realtime traffic in aWMN is difficult, and one of the main challenges is to coordinate temporal operations of the mesh access points (APs) in order to provide strict latency guarantee while efficiently utilizing the radio resources. In this paper, A new connection-based scheduling (CBS) scheme with a novel dynamic security-aware packet-scheduling algorithm is proposed. Connections with more hops are given a higher priority, and connections with a lower priority can only use resources remaining from serving all higher priority ones. For each multihop connection, the scheduling minimizes latency between successive hops. A connection-based optimization problem is formulated with an objective to minimize the amount of required AP resources, subject to the latency requirement of the connections. Also the proposed algorithm is capable of achieving high quality of security for realtime packets while making the best effort to guarantee realtime requirements (e.g., deadlines) of those packets. Experimental results show that compared with two baseline algorithms, the proposed algorithm can substantially improve both quality of security and real-time packet guarantee ratio under a wide range of workload characteristics.**

***Keywords*—Wireless networking, packet scheduling, resource utilization, Security aware connection based scheduling, Performance.**

I. INTRODUCTION

In the recent years, wireless technology has become one of the hottest buzzwords of the IT industry and academe due to the rapid growth of applications using wireless networks. Nowadays, people can access to the Internet at homes, hotels, airports, and even cars to conduct business, transfer money, play games and the like.

Nobody will doubt the fact that wireless networks bring incredible productivity and new efficiencies to our work. Based on the 2005 survey report of National Telecommunications Cooperative Association (NTCA), 62% of survey respondents are providing wireless services to their customers and 56% offer real time services like mobile voice. The worldwide market value of wireless applications is $433 billion in 2003 and projected to grow to almost $6708 billion by 2008. Even more excitingly, with the development of wireless technology, an increasing number of innovative applications like GPS, portable printing, signature capture are being used or will be used to improve our lives. As users become increasingly mobile and business applications become more interactive, traditional wireless communication technology is unable to satisfy real-time transmission requirements in mobile electronic commerce applications. To overcome this problem, real-time wireless communication techniques allowing users to collect and transmit data in a timely manner attracts many scholars and researchers.

It should be noted that supporting efficient and reliable data transmission, especially real time data transmission, over wireless networks is extremely difficult and challenging because wireless networks must be facing more complicated environments compared with conventional wired networks. For instance, wireless networks could be disturbed by radio wave and thunderstorms or blocked by physical objects like mountains or skyscrapers. Even worse, high mobility coupled with a variety of explosively increased users makes existing security policies in wireless networks inefficient or even useless, meaning that wireless networks can be easily attacked by computer viruses, worms, spy wares, and similar threats. These security threats cause downtime or continual patching in wireless networks and thus lead to severe disruption in wireless commercial business. Therefore, boosting security of wireless networks has become one of the most important issues in the arena of wireless communications.

Also in infrastructure-based wireless mesh networks (WMNs), such as a wireless local area network (WLAN) mesh network, mesh access points (APs) are connected to each other via one or multiple hops. Each AP is responsible

for forwarding packets for the end users associated to it as well as exchanging packets with neighboring APs based on the destinations of the packets. The end-to-end transmission delay of a packet generally increases with the number of hops. Quality of service (QoS) provisioning and efficient radio resource utilization require to coordinate temporal operations among the APs. A scheduling scheme for real-time traffic should achieve bounded and acceptable end-to-end packet transmission delay while efficiently utilizing the radio resources. This is a very challenging issue in WMNs due to the fact that each AP may receive packets from and forward packets to multiple other APs, but each radio in an AP can only communicate with one other AP at a time.

To overcome the above security issues and transmission delay of packets i.e., scheduling problem and to provide Quality of service number of innovations were researched. The scheduling problem in a WMN is similar to a job-shop scheduling (JSS) problem. A job shop consists of a set of machines that perform operations on jobs. Packets and APs in a WMN are similar to jobs and machines in a job shop, respectively, in the sense that any job/packet must be processed by a subset of the machines/radios according to a predetermined order, and each machine/radio can only process one job/packet at a time. It is proved that the JSS problem is NPhard. While the processing of one job requires availability of one machine in a JSS problem, one packet transmission in a WMN requires availability of both the transmitting and receiving APs. This makes the packet scheduling problem in a WMN more difficult than the JSS problem. Having multiple radios working at different frequency channels in each AP may simplify QoS provisioning, one such example is the even-odd scheduling proposed, but this is at a price of wasting the radio resources.

Current research work on traffic scheduling in wireless multihop and mesh networks mainly focuses on fair scheduling or throughput maximization when supporting non-realtime traffic. There has been very limited work on real-time scheduling in WMNs. In 2007 J. Zou and D. Zhao proposed a bottleneck first scheduling (BFS) scheme, which achieves capacity performance very close to the global optimal results. However, the complexity of BFS can be high due to the fact that the scheme tries to coordinate transmission times at different APs for different connections. For each connection, the order of making scheduling decisions for each of its hops is not necessarily the same as the order in which the packets are forwarded. Because of this, it may take multiple iterations for BFS to reach a feasible scheduling solution

Along with this an array of security policies such as authentication and confidentiality strategies and 802.11 wireless communication protocol based security schemas have been proposed and applied in real-time wireless networks. All the proposed protocols lack in either security or scheduling problem. In this paper, a new scheme is proposed which proposes that the connections with a larger number of hops are given a higher priority and their scheduling decisions are made first. Connections traversing a fewer number of hops use resources remaining from serving higher priority connections. For each connection, the transmitting time at the bottleneck AP along its route is determined first, and the transmission time of every other hop is determined to minimize latency between successive hops in order to minimize the overall multihop transmission delay. Since the scheduling decisions for higher priority connections are made independent of those for lower priority ones, the scheduling process using CBS is simpler than using BFS. A connection-based optimization (CB-OPT) problem is formulated with an objective to minimize the amount of required AP esources for serving real-time traffic, subject to the latency requirement of each connection. Also it considers the security and authentication of a packets delivered and as well at the guarantee ratio. In this CB-OPT problem integrates the packet-scheduling algorithm with dynamic security. In doing so, we build a new secure packet scheduling scheme for real-time wireless networks. In Section II we describe the system model on which this work is based. The proposed CBS scheme with security aware scheduling is described in Section III. A connection-based optimum security aware scheduling problem is formulated in Section IV. Numerical results are shown in Section V to demonstrate both the connection and packet level performance, and Section VI concludes the paper.

II. SYSTEM DESCRIPTION

A. MESH Network

We consider a WMN where mesh APs are interconnected through one or multiple hops. Each AP is equipped radio for communicating with its associated mobile stations (MSs) as well as with other APs. A number of MSs are associated to each AP, which is referred to as the home AP of the MSs. We consider that mesh APs are fixed and MSs are relatively static so that mobility is not a problem. Each AP stores a routing table which records the next hop AP for specific destinations. We assume that the routing tables are relatively static. Dynamically changing the routing tables is possible but may trigger re-scheduling, which introduces extra overhead. Channel time is divided into equal size time slots. One packet transmission can take one or multiple time slots. All system time is normalized to the duration of a time slot. TDMA is adopted for serving real-time traffic. Compared to contention-based MACs, such as CSMA/CA, TDMA allows centralized slot assignments and is more efficient for providing strict latency requirement. A limited number of frequency channels are available for the network. Co-channel interference is present among APs sharing the same frequency channel. A packet cannot be received correctly if there is more than one AP transmitting within the interference range of the desired receiver. We consider that

a frequency channel assignment scheme is in place and the frequency assignments are relative static for the duration of the real-time connections. Frequency channel assignment in a WMN is another important and challenging research topic and is beyond the scope of this paper. Several frequency assignment schemes are proposed in [7].

We consider access traffic. Each connection is between an MS in the WMN and a station in the wireline network. We assume that the wireline network always has sufficient resources to support a connection as long as the WMN can accept it. We focus on constant-bit-rate (CBR) traffic and use *Tp,i* and *di*, respectively, in number of time slots, to represent the packet transmission time and maximum tolerable delay of a packet for connection *i*. Besides the real-time CBR traffic, the system may support other types of traffic, but the realtime traffic is given the highest priority and its performance is not affected by other traffic. We assume that transmission delay introduced by the wireline network can be neglected, compared to that in the wireless network. In the remaining part of the paper, we only consider packet transmission scheduling in theWMN. One of the mesh APs is connected to the wireline backbone network and referred to as *root AP*, which is the central station responsible for admission control and resource allocation for all QoS traffic in the network. The root AP has information about the resource availability at each AP. A new connection with strict QoS requirements should pass admission control before entering the system. Details about the admission control in a WMN can be found . Each hop along the route of a connection has an index number. The first hop in the uplink (from the MS to the wireline network) is the hop from the MS to its home AP, and the first hop in the downlink (from the wireline network to the MS) is the hop from the root AP to the next downstream AP. The index number of the hops increases along the direction where packets are forwarded.

B. Security Aware Scheduling

In this study, we model a wireless channel as an NN switch. Although each wireless node may have a single transmitter and a single receiver, it is common that the transmitter and receiver are combined in a transceiver. As such, a node can not transmit and receive packages simultaneously. In our switch model, there exists a packet scheduler matching transmitters to corresponding receivers. The detailed information regarding the switch model. In addition to the switch, other three key components in the system include a Security Level Controller (SLC), an Admission Controller (AC), and an EDF (Earliest Deadline First) scheduler as depicted in Fig. 1. This architecture is designed for a link between two nodes in a wireless network. All packets are submitted independently to the wireless link with arrival rates abided by Poisson distribution. The function of the Admission Controller is to determine whether incoming packets can be accepted or not. The Security Level Controller aims at increasing security levels of real-time packets residing in the Accepted queue that can be finished before their deadlines. The EDF scheduler makes use of the Earliest Deadline First policy to schedule admitted packets in which security levels are maximized by the Security Level Controller.

C. Packet Model

Our packet model assumes that all packets have soft deadline and each packet is independent of one another. We also assume that packets' arrival times follow the classical Poisson distribution. Packet Pi is represented as a tuple (*ATi*, *PTi*, *SLi*, *Di)*, where *ATi* and *PTi* denote the arrival time and the processing time of packet *i*. *SLi* and *Di* represent the security level and soft deadline of packet *i*. Besides, without loss of generality we assume that each packet is assigned a quality of security measured as a security level *SLi* that in the range [1, 2, ..., 10], where 1 and 10 are the lowest and highest levels of security. For example, if packet *i* has a value of 1 as a security level, this means that the packet has the lowest security level. Although wireless network devices are unable to determine security levels, packets' security levels can be straightforwardly derived from the security requirements of applications.

To calculate the security overhead without loss of generality, we make use of formula (1) to model the security overhead envisioned as the extra processing time experienced by packet *i*.

$$SOi = ETi * (SLi/R) \quad (1)$$

where *SOi* is the security overhead of packet *i*, *SLi* is the security level provided to packet *i*, *ETi* is the transmission time of the packet. And *R* is set to 10. Thus, the total processing time *WLi* of packet *i* can be expressed as:

$$WLi = ETi + SOi = ETi * (1 + SLi/R) \quad (2)$$

III. Security Aware Connection Based Scheduling

A. Connection Based Scheduling

Define *TSI* as the duration of one scheduling interval (SI), each of which consists of two parts: a real-time portion and a non-real-time portion for processing real-time and non-realtime data traffic, respectively. We set *TSI* to be equal to the packet inter-arrival time of a real-time CBR connection. That is, one packet is generated from each CBR connection in every SI. To provide a constant service rate to each CBR connection, one packet is served for each connection in every SI. In this way, we only need to describe the scheduling of each AP in a typical SI. All other SIs of the AP repeat the same schedule. Below we use "packet *i*" to denote the packet to be scheduled for connection *i* in the considered SI. It is possible that the CBR connections have different packet inter-arrival times. In this case, the duration of the SI can be set to be the least common multiple (LCM) of all the packet inter-arrival times (in number of time slots). Then one or multiple

packets (depending on the ratio of the LCM to the packet inter-arrival time of a particular connection) are served for a connection during each SI. The proposed scheduling scheme can then be extended to serve heterogeneous CBR traffic with different packet inter-arrival rate. We define a binary variable, Am,t, with $Am,t = 1$ representing that AP m has not been scheduled for serving real-time traffic at time t and $Am,t = 0$ otherwise. We further define tm,min = argmin$t$ $\{Am,t = 0\}$, and tm,max = argmax$t$ $\{Am,t = 0\}$, where t is in the considered typical SI of AP m. Then the real-time portion in the typical SI of AP m is $Trt,m = tm$,max $- tm$,min. Given the total number of real-time connections, it is desired to minimize the real-time portion subject to the delay constraints of the connections. Let $\tau i,h$ be the time when packet i is transmitted at hop h. The task of the scheduling is to find $\tau i,h$'s, $h = 1, 2, \ldots, Hi$, to satisfy the latency requirement of all connections, while keeping the real-time portions as short as possible for all APs along the route of the connection. The values of $\tau i,h$'s (normalized to the duration of a slot time) are integers. Before making scheduling decisions for connection i, some time slots of the APs along the route of the connection may have been scheduled for serving other connections. Define Di,h as a set of time slots that $\tau i,h$ can possibly take. Let m and n, respectively, represent the transmitting and receiving APs of the h-th hop of connection i. If $t \quad Di,h$, then $Am,t = 1$, $Am,t+1 = 1$, ..., $Am,t+Tp,i-1 = 1$, and $An,t = 1$, $An,t+1 = 1$, ..., $An,t+Tp,i-1 = 1$. Co-channel interference is another factor that affects Di,h. If $t \quad Di,h$, then no AP that is assigned to the same frequency channel as AP m and within the interference range of AP n has been scheduled to transmit at time $t, t + 1, \ldots, t + Tp,i - 1$. Meanwhile, AP m should not be in the interference range of any AP that has been scheduled to receive at the same frequency channel at time $t, t + 1, \ldots, t + Tp,i - 1$.

In general, connections with a larger number of hops are more likely to experience a longer delay, and therefore their scheduling decisions are made earlier, and the scheduling decisions of connections with a fewer number of hops are made using the remaining resources. Furthermore, an AP with a higher traffic load has less flexibility in arranging its timeline and therefore should be given a higher priority in scheduling. We define the bottleneck AP along the route of connection i as the AP which transmits and receives the largest number of packets in one SI. Let h denote the index of the hop along the route of packet i and with the bottleneck AP as the transmitter. When scheduling for connection i, the value of $\tau i,h$ is determined first, and transmitting times at other hops along the route of the connection are then determined one by one from hop $h + 1$ to hop Hi, and then from hop $h - 1$ to the first hop. This process is outlined in Pseudocode 1, where M is the total number of APs, N is the total number of connections, and N is a set of connections that have not been scheduled at the current iteration.

Pseudocode 2 describes how to find $\tau i,h$ for a typical hop h of packet i with APs m and n as the transmitter and receiver, respectively. There are three different cases to be considered depending on which hops have been scheduled at the time to determine $\tau i,h$. Case 1: no hop has been scheduled for the packet; Case 2: the immediate upstream hop, i.e., the $(h - 1)$-st hop, has been scheduled; and Case 3: the immediate downstream hop, i.e., the $(h+1)$-st hop, has been scheduled. In Pseudocode 2, specifies a lower limit, Tmin, and an upper limit, Tmax, so that all values of t in (for Cases 1, 2, and 3, respectively) can ensure $\tilde{} Trm,m \leq TSI$, where $\tilde{} Trm,n$ is the real-time portion of AP n, assuming $\tau i,h = t$. In Case 1, $\tau i,h$ can take any time slot in Di,h as long as both Trt,m and Trm,n can still be kept within one SI after $\tau i,h$ is determined. In Case 2, besides the same considerations as in the previous case, the code selects the value for $\tau i,h$ so that i) $\tau i,h > \tau i,h-1$ in order for the processing time in the h-th hop to be later than that in the $(h-1)$-st hop, and ii) $(\tau i,h - \tau i,h-1)$ is minimized in order to minimize the delay between successive hop transmissions. The scheduling in Case 3 is similar to that in Case 2 except that $\tau i,h < \tau i,h+1$ and $(\tau i,h+1 - \tau i,h)$ is minimized.

B. Security Aware Algorithm

The main goal of this study is to maximize the overall system performance, which reflects the guarantee ratio and security level. To achieve this goal, we designed the SCBT scheduling algorithm with security awareness. SCBT aims to maintain high guarantee ratios while maximizing the security levels. We can accomplish high performance and high security level by applying the Security Level Controller to our SCBT algorithm.

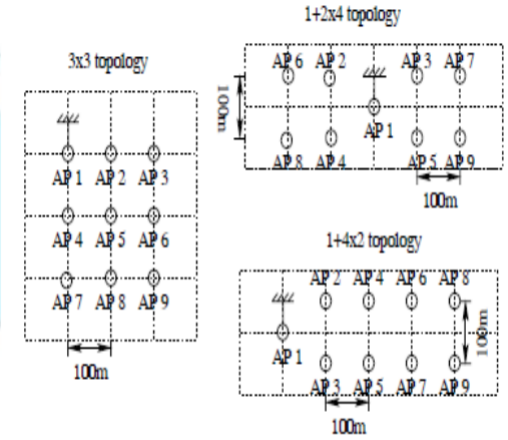

Fig. 1. Mesh topologies.

The above Fig1. Shows the mesh topologies and the Fig. 2 below outlines the flow chart of the security-aware CBT scheduling algorithm for wireless links. The SCBT algorithm strives to maximize the security level of a packet residing in the accepted queue while making the best effort

to guarantee its deadline. If the deadline of the packet can be met, the packet will be admitted in the accepted queue. Otherwise, the packet will be dropped and placed in the rejected queue . The following constraint shows whether the packet is equipped to meet its deadline.

CTi − *STi* <= *di* where *STi* is the start time of transmission of the *i*th packet, *CTi* is the completion time of the transmission, and *di* is the packet's deadline. The packets stored in the accepted queue are scheduled depending on their specified deadlines, meaning that the packets with earlier deadlines will be processed first. The SCBT algorithm initializes the security levels of all packets to the minimum levels. Then, SPSS gradually enhances the security level of each packet *Pi* under the condition that (1) the current packet *Pi* can be transmitted before its deadline; and (2) the deadlines of the packets being processed later than *Pi* also can be guaranteed. The above criterion is important and reasonable because if a packet is admitted to the realtime wireless link, then the packet's timing constraint has to be guaranteed. In other words, the SPSS algorithm ensures that an admitted packet is not adversely affected by subsequently admitted packets.

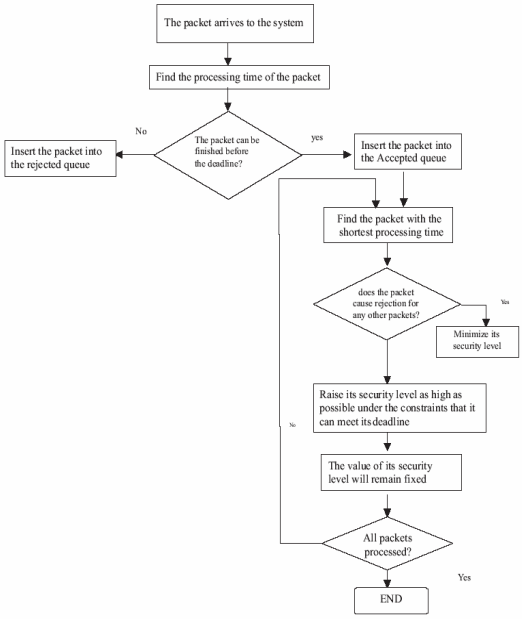

Fig 2 The working process of SCBT

The following steps delineate the procedure of the SPSS scheduling. Step 1: initialize the scheduler; the security values of incoming packets; and the number of rejected packets is set to zero. Wait for any incoming packets. Step 2: if a packet *I* arrives and it is the only packet available, process the packet immediately using its highest security level. The starting time *(STi)* and the completion time *(CTi)* of the packet are calculated. Step 3: All the packets arriving in the scheduler during the time period *[STi, CTi]* are temporarily stored into a waiting queue in the non-decreasing order of their deadlines. The starting time of the next packet *STi* + 1 is set to *CTi*. Step 4: the admission controller is responsible for deciding whether a packet in the waiting queue can be accepted by considering the deadline of this packet. If the packet's deadline and security requirement can both be guaranteed, the packet will be forwarded into the accepted queue (step 3 and step 5). Otherwise, being put into the rejected queue will drop the packet; the number of rejected packets is increased by one. Step 5: the security level controller raises the security levels of all the packets residing in the accepted queue as high as possible. The enhancements of the security levels for realtime packets residing in the accepted queue are subject to the following two constraints: (1) Increasing of an accepted packet's security level should still guarantee the deadline of the packet. (2) The increase of security levels must not lead to any rejection of currently accepted packet. Step 6: At this point, the security level *SLi*+1 of the next starting packet is maximized. The packet's completion time *CTi*+1 is calculated. Steps 3-6 are repeatedly executed until all the arriving packets are processed in one run.

IV. SIMULATION RESULTS

We first consider WMNs with three different topologies as shown in Fig. 1 with AP 1 as the root AP in each topology. MSs are uniformly distributed in the network area, and each MS is associated to its nearest AP. The transmission range and interference range of each AP are 150m and 250m, respectively. The physical channel transmission rate is 2 Mbps. Homogeneous CBR voice traffic is considered. The connection requests arrive at the network according to a Poisson process and each is associated to one of the MSs with equal probability. The duration of the connections follows an exponential distribution with an average of 60s. For each connection, one voice packet is generated every 20 ms, and the maximum packet transmission delay is 60ms. The shortest path routing is used. We write a discrete event simulation program using Java and compare the proposed Security Aware CBS with CBS. It is seen that the connection blocking performance using Security aware CBS is close to that using CBS in all three topologies. The WMN with 1+2x4 topology achieves the lowest connection blocking rate and the one with 1+4x2 topology achieves the highest connection blocking rate. This can be explained by the effect of bottleneck APs on the overall system capacity. For access traffic, the bottleneck of the WMN is the root AP or the APs one hop away from it. The bottleneck can be any AP from AP 1 to AP 5 in the 1+2x4 topology, AP 1 to AP 4 in the 3x3 topology, and from AP 1 to AP 3 in the 1+ 4x2 topology. We define the bottleneck region size (BRS) as the number of possible bottleneck APs in a WMN. The BRS is 5 in the 1+2x4 topology, 4 in the 3x3 topology, and 3 in the 1+ 4x2 topology. A larger BRS allows traffic to be more evenly distributed in the network, resulting in higher network capacity and lower connection blocking rate.

V. CONCLUSION

In real-time wireless networks not only high guarantee ratio is required for packets, but also high quality of security is needed to protect data stored in the packets transmitted through wireless networks. To develop real-time wireless networks with high quality of security and guarantee ratio, we proposed a novel dynamic Security-Aware Connection Based Scheduling algorithm (or SCBS for short), which is capable of achieving high quality of security for real-time packets while making the best effort to guarantee real-time requirements of those packets. The SCBS algorithm is designed in a way that makes it possible to achieve a reasonably high guarantee ratio and optimized security level. In particular, our SCBS algorithm leverages an intelligent Security Level Controller to adaptively assign security levels to incoming real-time packets transmitted via a wireless network link. The experimental results show that our approach delivers significant improvements in guarantee ratio, security level, as well as overall system performance under a wide range of workload patterns. Specifically, our approach can provide overall performance improvement by up to 15%. Also achieves close-to optimum connection blocking performance, while providing guaranteed packet-level performance. Research on the realtime traffic scheduling for supporting variable bit rate realtime traffic is underway.

REFERENCES

[1] A. Jain and S. Meeran, Deterministic Job-Shop Scheduling: Past, Present and Future. Oct. 1998.

[2] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.

[3] G. Narlikar, G. Wilfong, and L. Zhang, "Designing multihop wireless backhaul networks with delay guarantees," in Proc. 25th IEEE International Conf. Computer Commun., Apr. 2006, pp. 1-12.

[4] J. Tang, G. Xue, C. Chandler, and W. Zhang, "Link scheduling with power control for throughput enhancement in multihop wireless networks," IEEE Trans. Veh. Technol., vol. 55, no. 4, pp. 733-742, May 2006.

[5] J. Ju and V. Li, "TDMA scheduling design of multihop packet radio networks based on latin square," IEEE J. Select. Areas Commun., vol. 17, no. 8, pp. 1345-1352, Aug. 1999.

[6] J. Zou and D. Zhao, "G-BFS: a scheme for scheduling real-time CBR traffic in IEEE 802.11-based mesh networks," in Proc. 2007 IEEE Wireless Commun. Networking Conf., Mar. 2007, pp. 4268-4273.

[7] D. Niyato, E. Hossain, and V. Bhargava, "Scheduling and admission control in power-constrained OFDM wireless mesh routers: analysis and optimization," IEEE Trans. Wireless Commun., vol. 6, no. 10, pp. 3738- 3748, Oct. 2007.

[8] X. Wang, "Traffic scheduling with efficient channel assignment in WLAN mesh networks," master's thesis, McMaster University, Dec. 2007.

[9] Zhao, J. Zou, and T. Todd, "Admission control with load balancing in IEEE 802.11-based ESS mesh networks," ACM Wireless Networks, to appear.