FIRM: Flow-based Interference-aware Route Management in Wireless Mesh Networks

Youngbin Im,* Jeongkeun Lee,† Jinyoung Han,* Sung-Ju Lee,† and Ted "Taekyoung" Kwon*

*School of Computer Science and Engineering, Seoul National University, Korea
†Multimedia Communications and Networking Lab, Hewlett-Packard Laboratories, Palo Alto, USA
Email: ybim@mmlab.snu.ac.kr, jklee@hp.com, jyhan@mmlab.snu.ac.kr, sjlee@hp.com, tkkwon@snu.ac.kr

***Abstract*—In IEEE 802.11-based wireless mesh networks, routing is crucial in achieving high throughput in face of both inter-flow and intra-flow interference. Prior work focuses on finding the maximum available bandwidth path when a new flow enters the network. However, few has considered the effect of the new flow on the throughput of the existing flows. We propose a routing framework that uses the topology map of a mesh network with the carrier sense and interference relations and estimates the available bandwidth of a candidate path. We propose two algorithms for finding a route for a new flow: (1) FIRM searches for the maximum bandwidth path for the new flow, and (2) FIRM$^+$ not only considers the available bandwidth of a path for the new flow, but also the amount of throughput degradation of existing flows. We implement and evaluate FIRM and FIRM$^+$ with the IRU routing algorithm on a 15 node indoor IEEE 802.11a testbed. Various experiments reveal that FIRM$^+$ achieves the highest total throughput of all flows.**

I. Introduction

Routing in multi-hop wireless networks has been a crucial issue and there have been many proposed routing protocols. In contrast to mobile ad hoc networks, the backbone of most wireless mesh networks are static and hence more stable. The key issue of routing protocols in wireless mesh networks is how to define a routing metric that finds a high bandwidth path, and considers interference and wireless link characteristics. Wireless link metrics such as expected transmission count (ETX) [1] and expected transmission time (ETT) [2] are early proposals that typically achieve better throughput than the shortest hop count metric. Later on, more advanced metrics that consider interference and traffic load have appeared, some of which are proposed for multi-channel and multi-radio wireless mesh networks [3], [4].

Interference-aware Resource Usage (IRU) [4] is an interference-aware routing metric and it takes the number of interfering neighbors into account in the metric design. Recent proposals [5]–[7] present more comprehensive models to compute available path bandwidth based on interference. In particular, both interference and current network traffic load information are considered in [6], [7]. Salodinis et al [6] propose to use a 802.11 MAC based model to identify maximum bandwidth path(s) by using channel busy time and collision rate measurements from each node and link. The Contention-Aware Transmission Time (CATT) routing metric [7] is also based on the 802.11 DCF model and considers the current traffic load by taking link transmission attempt rate into account. Thus, both [6] and [7] require a special driver/hardware support to measure those MAC related parameters. Moreover, they do not consider the effect of a new flow on the existing flows and consequently the total network throughput could be degraded. The proposed solution for VoIP application [8] evaluates whether capacity constraints or QoS metrics will be satisfied if a new flow is admitted. However, this approach is restricted to VoIP traffic, and is not appropriate for general applications where the flow rates can be different.

In this paper, we present a route management framework that finds the best routing path not only for a newly arriving flow but also for existing flows based on the network topology, interference and traffic information. The contributions of this paper are as follows.

1) We propose a simple yet efficient model that computes the available path bandwidth based on topology/interference/load information.[1] This model does not require any special driver support.
2) We identify the potential drawback of routing solutions that target maximum available bandwidth; simply using the maximum bandwidth path for a new flow can degrade the performance of existing flows and the overall network. We propose a new routing metric that considers the effect of a newly entering flow on the existing flows.
3) We evaluate the throughput performance of the proposed routing metric and management system on a 15-node indoor 802.11a wireless mesh network testbed.

The rest of this paper is organized as follows. Section II presents the network model and management system architecture. Section III describes the proposed routing algorithms (FIRM, FIRM$^+$) and management operations. Performance evaluation on the testbed is presented in Section IV. After discussing how to extend the routing framework in Section V, we conclude this paper.

[1] Although the terms 'available path bandwidth' and 'available path throughput' have been used interchangeably in the literature to indicate the same notion of the amount of traffic one could get on a given routing path, we separately use the term 'bandwidth' for the above notion and use the term 'throughput' to indicate the actual traffic delivery rate that a flow gets as a result of routing actions.

II. System Model

We consider a multi-hop wireless mesh backbone network, which is connected to the wired network. For the sake of exposition, $n-1$ nodes belong to the wireless mesh network and one single node will serve as a correspondent host in the wired network. The $n-1$ wireless nodes can further be classified into three sets: a set of gateways, a set of Mesh Access Points (MAPs), and a set of Mesh Points (MPs). A gateway node p has two interfaces: (i) a wireless interface to communicate with MAPs and MPs, and (ii) a wired interface to directly communicate with the correspondent host. An MP is a mesh router that relays traffic between MAPs and gateways and an MAP functions both a mesh router and an access point for wireless clients. Any of MAPs and the correspondent host can be a source and a destination of a flow. The client-to-MAP association is out of scope of this paper and we focus on the routing issues inside the mesh backbone.

Our mesh routing scheme supports a flow-based approach. That is, different flows of the same <source, destination> pair can flexibly select different routes.

We assume that the system operates in an asynchronous carrier sensing multiple access (CSMA) mode such as the 802.11 MAC protocol. We do not assume the existence of an ideal MAC scheduling mechanism. In contrast to previous models in the literature (e.g., [9]), we do not consider a fine-grained TDMA-based scheduling that avoids conflicts among interfering links.

A. Mesh Management Server (MMS)

Although the proposed routing system can be implemented as a distributed routing protocol, we take a centralized management approach for mere simplicity of implementation and not as a deliberate architectural choice. As shown in Fig. 3, there is a Mesh Management Server (MMS) that resides in the wired network and it monitors and manages the mesh network.

The major roles of the MMS are three-folds. First, the MMS monitors the network topology and provides the topology information as described in Section II-B. We can use any interference estimation solution because we use only the general information that most solutions support. We use RBP (RSS-based prediction) [10] as it analyzes the radio propagation characteristics of the mesh network with small measurement overhead. RBP collects the received signal strength (RSS) information between nodes and builds the carrier sense and interference matrices by comparing the RSS values with the thresholds. In our previous studies [10]–[12], we have developed accurate 802.11 PHY models and thresholds for frame reception, carrier sense, and physical layer capture, all of which are incorporated into the RBP scheme.

Second, the MMS monitors the traffic and maintains a traffic map that includes the amount of traffic each flow injects into the network and the route of each flow. Monitoring the exact traffic amount of each flow is challenging. One solution is measuring the throughput of inbound and outbound flows at the gateway nodes. Although the flow throughput at the destination may not be the same with the measured throughput because of packet drops, measuring the throughput only at the gateways incurs no message overhead.

Third, based on the topology and traffic maps, the MMS finds the best path for each flow. We can use either table-based routing or source routing but we use source routing in this paper. If any of existing flows suffers from performance degradation or needs a new route due to a significant change in traffic load, the source node of such flow may request a new route to the MMS.

B. Topology Map

If node v_a can transmit directly to node v_b, this link is represented by a directed edge $e_k = (v_a, v_b)$, from node v_a to node v_b. We say the link e_k is *active* when there is a transmission from v_a to v_b. We assume that for each directed link $e_k = (v_a, v_b)$, there exists a corresponding reverse link $e_{k'} = (v_b, v_a)$. If only one directed link between a pair of nodes is detected by RBP, this asymmetric link is excluded from consideration because 802.11 MAC needs a symmetric link for data-ack exchange. The correspondent host and each gateway node are connected via a bi-directional wired link. These wired links are free from any wireless contention and interference.

Let E and V be the sets of the links and the nodes, respectively. We have a contention matrix $S\colon V \times V \to [0,1]$ and each element $s_{i,j}$ (a real number between 0 and 1) is defined as the probability that node v_i senses v_j's transmission. That is, the probability that v_i defers its own transmission when v_j's transmission is ongoing. Each node v_i has a set of nodes from which v_i senses the transmission

$$N_{\text{cs}}(v_i) = \{v_j \in V | s_{i,j} > 0\}.$$

Likewise, we define a hidden interference matrix $H\colon E \times V \to [0,1]$ and each wireless link e_k has a set of hidden interferers

$$N_{\text{int}}(e_k) = \{v_i \in V | h_{k,i} > 0\},$$

whose transmission interferes with the communication of link $e_k = (v_a, v_b)$ with a probability of $h_{k,i}$ (a real number between 0 and 1). In other words, when v_a and v_i transmit simultaneously, only $(1-h_{k,i})$ portion of v_a's transmission can be correctly received by v_b. Note that contention relations are sometimes coupled with interference relations. For instance, $h_{k,i}$ always takes a value of zero when $s_{a,i} > 0.5$ and $s_{i,a} > 0.5$: two mutually carrier sensing senders do not cause 'hidden' interference. Here, we only consider interference between MAC data frames. We ignore data-ack, ack-data, ack-ack interferences because they have small contribution (less than 3%) to total interference compared with the data-data interference [13]. In addition, we do not consider RTS/CTS in this model. A recent study [14] showed that the use of RTS/CTS does not improve multi-hop network performance in many cases. However, our interference model can be extended to cover the other interference cases and RTS/CTS with some modification.

In summary, a topology map consists of a directed network graph $G = (V, E)$, a carrier sense matrix S, and a hidden interference matrix H.

III. FIRM Route and Flow Management System

In this section, we first describe the routing metric FIRM that is computed as an estimation of the available bandwidth with the given topology and traffic matrices. We then extend FIRM to consider the effect of a newly arriving flow on the throughput of existing flows (FIRM$^+$).

A. FIRM Routing Metric

1) Available Link Bandwidth: We first derive the available link airtime during which a link can be additionally active to deliver the traffic of the new flow in the presence of other traffic flows already existing on the link and/or its carrier sensing neighbor nodes. The available link airtime is zero when the link is already saturated by existing traffic flows. At the end of this subsection, we will derive the available link bandwidth from the available link airtime by considering hidden interference.

Let us consider a link $e_k = (v_a, v_b)$. The available airtime of e_k, $\tau(e_k)$, is defined as

$$\tau(e_k) = \min(\tau_{\text{tx}}(v_a), \tau_{\text{rx}}(v_b)),$$

where $\tau_{\text{tx}}(v_a)$ and $\tau_{\text{rx}}(v_b)$ are the available airtime v_a can use for transmission and the available airtime v_b can use for reception, respectively.

$\tau_{\text{rx}}(v_b)$ is computed as

$$\tau_{\text{rx}}(v_b) = 1 - t_{\text{tx}}(v_b) - t_{\text{rx}}(v_b),$$

where $t_{\text{tx}}(v_b)$ and $t_{\text{rx}}(v_b)$ are the total airtime v_b uses for transmission and reception of existing traffic flows. They can be directly calculated from the traffic map, the bit rate, and the MAC overhead.[2]

To calculate $\tau_{\text{tx}}(v_a)$, we consider the channel busy time, which is the sum of the transmission time of the nodes that v_a senses. Thus,

$$\tau_{\text{tx}}(v_a) = 1 - t_{\text{tx}}(v_a) - t_{\text{rx}}(v_a) - \sum_{v_j \in N_{\text{cs}}(v_a)} (s_{a,j} \cdot t_{\text{tx}}^{-v_a}(v_j)),$$

where $N_{\text{cs}}(v_a)$ is the set of nodes that v_a senses their transmissions and $s_{a,j}$ is a carrier sense metric as defined in Section II-B. $t_{\text{tx}}^{-v_a}(v_j)$ is the airtime v_j uses for its transmissions to all other nodes except v_a. Note that $t_{\text{rx}}(v_a)$ already includes the airtime used for the transmissions from v_j to v_a.

Now we consider hidden interference to compute the effective airtime, i.e., available bandwidth that link e_k can effectively provide for a new flow in the presence of collisions caused by hidden interference. The available link bandwidth $d(e_k)$ is defined as

$$d(e_k) = \tau(e_k) \prod_{v_i \in N_{\text{int}}(e_k)} (1 - h_{k,i}\ t_{\text{tx}}^{-v_a}(v_i)),$$

where $N_{\text{int}}(e_k)$ is the set of hidden interferers for link e_k and $h_{k,i}$ is the level of interference on link e_k due to v_i's traffic. The term $h_{k,i}\ t_{\text{tx}}^{-v_a}(v_i)$ represents the effective interference that v_i imposes on e_k.

Here, we conservatively assume that each hidden interferer's transmission is independent of each other by ignoring the carrier sense relations between the hidden interferers. This is represented by the product operation.

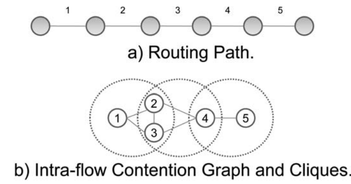

Fig. 1. Intra-flow contention example.

2) Available Path Bandwidth: We calculate the available path bandwidth for a given path by considering the contention and interference between the transmission attempts of multiple links on the given path to deliver the new traffic flow (intra-flow contention/interference). Note that the contention and interference from the existing flows (inter-flow contention/interference) has been taken care of in the available link bandwidth computation. Similar to the methodology in [6], we make cliques of links that contend with each other due to carrier sense, hidden interference and the fact that a node can not transmit and receive simultaneously.[3] Only one node in a clique can be active at a time. Fig. 1.a shows an example of a 5-hop path. Two adjacent links cannot be active simultaneously due to carrier sense between the senders of the two links. In addition, because link 3's sender interferes with the link 1's receiver, links 1, 2, and 3 contend with each other and are in the same clique. Likewise, links 2, 3, and 4 form another clique. Links 4 and 5 form a clique as well.

The maximum available bandwidth f_c for a clique c is constrained by $\sum_{\forall e_k \in c} \frac{f_c}{d(e_k)} \leq 1$, where the sum of the airtime to send traffic f_c for all the links in clique c cannot exceed 1. Thus, f_c is given by

$$f_c = (\sum_{\forall e_k \in c} \frac{1}{d(e_k)})^{-1}.$$

The available path bandwidth, FIRM(p) is computed by taking the minimum of all f_c of the path p. The FIRM routing protocol uses FIRM(p) as a routing metric and searches the path with maximum FIRM(p).

B. FIRM$^+$: Considering Effects on Existing Flows

The goal of FIRM and other load- or interference-aware routing protocols [6], [7] is to devise a routing metric that

[2]We do not model the MAC retransmission and backoff mechanisms to keep the model simple. Previous studies [6], [7], [15] provide more comprehensive 802.11 MAC models, but they require higher algorithm complexity [15], additional hardware support, or more measurement overhead [6], [7].

[3]We do not consider nodes with multi-radios.

enables us to find the maximum available bandwidth path for a newly arriving flow. These routing metrics have been shown to achieve throughput improvement over load-agnostic routing metrics such as ETX [1] and IRU (Interference-aware Resource Usage) [4]. However, they ignore the effect a newly entering flow has on the existing flows and the total throughput of the entire network may decrease even though the new flow achieves high throughput. To remedy this, we propose an extension of FIRM, FIRM$^+$. FIRM$^+$ explicitly takes into account the throughput reduction of existing flows.

Because the MMS maintains an up-to-date traffic map, we have a set of existing flows X and know the relevant information of each flow $x \in X$. Each flow x is associated with a path p_x and its traffic load is f_x. Let $p_{x'}$ be the path of interest that we wish to compute its routing metric $\mathrm{FIRM}^+(p_{x'})$ for a newly arriving flow x'.

We first compute $\mathrm{FIRM}(p_{x'})$, which is the available bandwidth for flow x' over path $p_{x'}$. We then compute the expected amount of throughput reduction of an existing flow $x \in X$, f_x^-, caused by adding the new flow x' (whose traffic load is $f_{x'}$) along the path $p_{x'}$.

$$f_x^- = \begin{cases} f_x - FIRM_{X-x+x'}(p_x) & \text{if } FIRM_{X-x+x'}(p_x) < f_x \\ 0 & \text{otherwise} \end{cases}$$

where $\mathrm{FIRM}_{X-x+x'}(p_x)$ is the available bandwidth for flow x over path p_x when f_x is removed along p_x and x' is added along $p_{x'}$ in the network (and hence traffic map X is updated). That is, we calculate how much bandwidth will be available for the existing flow x over p_x when the new flow whose load is $f_{x'}$ is added over path $p_{x'}$. Now we define $\mathrm{FIRM}^+(p_{x'})$ as

$$\mathrm{FIRM}^+(p_{x'}) = \mathrm{FIRM}(p_{x'}) - \sum_{\forall x \in X} f_x^-$$

which estimates the change of the total throughput the entire network will experience when the new flow x' is put on the path $p_{x'}$. Note that $\mathrm{FIRM}^+(p_{x'})$ becomes a negative when $\sum_{\forall x \in X} f_x^-$ is larger than $\mathrm{FIRM}(p_{x'})$. By selecting the path with the largest $\mathrm{FIRM}^+(p_{x'})$, we maximize the total throughput not the throughput of the new flow.

C. Route and Flow Management

When a new flow joins the network, the MMS first identifies a set of candidate paths to apply FIRM or FIRM$^+$ metric. There can be multiple ways to select the candidate paths and we use a hop distance to determine the scope of candidate paths. That is, a path connecting the source and the destination of the new flow within the shortest path's hop distance + y hops can be a candidate path, where y is a system parameter. This approach works with both on-demand and proactive routing. A proactive routing path computation is possible if the future traffic demand is given or predicted.

The MMS computes routing metrics of the candidate paths and selects the path p' with the highest metric value. We selectively use FIRM or FIRM$^+$ based on the network QoS policy. If we want to maximize the throughput of the new flow, we use FIRM; if we want to maximize the total network throughput, we use FIRM$^+$. In addition, our model can adopt other QoS criteria; for example, if fairness is the major concern, we can extend FIRM$^+$ to account for the fairness index in the metric or we can find the path that minimizes the maximum flow reduction of the existing flows. In this paper, we only consider FIRM and FIRM$^+$ in performance evaluation.

The FIRM metric can help us use rate control and admission control mechanisms. The MMS can assign not only a path p but also a flow rate $\mathrm{FIRM(p)}$ to a new flow; the new flow injection rate is regulated at its ingress router (either a MAP or a gateway) not to exceed $\mathrm{FIRM(p)}$ and prevent path p from congestion. If $\mathrm{FIRM^+(p)} \leq 0$, we may perform admission control and deny the new flow in order to maintain the throughput of the existing flows.

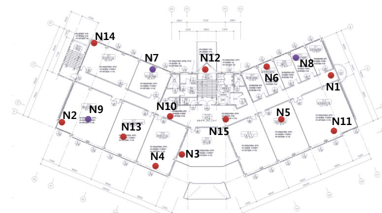

Fig. 2. SNU mesh testbed topology map.

IV. Evaluation

We evaluate the performance of FIRM and FIRM$^+$ by comparing them with IRU [4] on the 15 node wireless mesh network testbed. The testbed is deployed on a single floor in a building at Seoul National University (SNU). We first describe how we configure our experiments and perform UDP throughput measurement experiments in a simple scenario using a small number of mesh nodes to understand the behaviors of FIRM and FIRM$^+$. We then carry out our experiments in more complex scenarios.

A. Testbed Description and Experiment Setup

Our testbed consists of small-form factor single-board computers, each of which has a mini-PCI 802.11a card with the Atheros chipset. Figure 2 shows the map of our topology. In our experiments, first we perform RBP to obtain the topology map information including interference and carrier sensing relations. Based on the information, routing paths are selected according to FIRM, FIRM$^+$ and IRU algorithms.

In the simple scenario, two flows exist from the beginning and after 10 seconds, we initiate a new flow. The path selected by the new flow will vary depending on the routing algorithm. For the complex scenarios, we vary the number of gateways, the number of flows, and the traffic load of each flow. We use the 802.11a channel 44, which is verified to be free from external interferences. The bit rate of all the nodes is fixed to 6 Mbps and UDP packets are transmitted with 1024 byte length for each flow.

The routing metric of each link l in IRU [4] is defined as $IRU(l) = ETT(l) \times N(l)$ where $ETT(l)$ is the expected transmission time of link l and $N(l)$ is the number of neighbors with which transmissions over link l interfere. We include in $N(l)$ any node who can receive hellos from either the sender

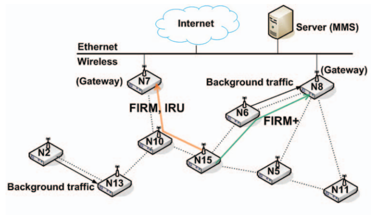

Fig. 3. Path allocation scenario.

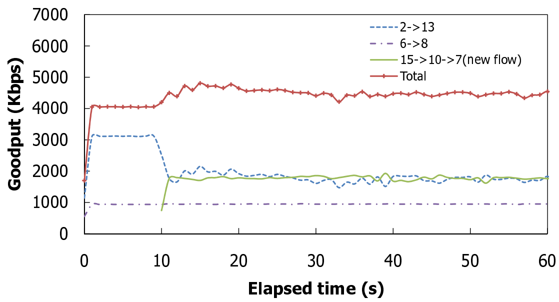

Fig. 4. The total throughput and the throughput of each flow with FIRM and IRU.

or the receiver of the link l with the success probability higher than 0.9.

B. Simple Scenario

Fig. 3 shows the topology of the simple scenario, where there are two gateways: N7 and N8. Two background flows exist: one from N2 to N13 and another from N6 to N8. The traffic rate of these flows are 3 Mbps and 1 Mbps, respectively. Note that there is no interference between these flows. After 10 seconds from the start, N15 starts to transmit a new flow to the Internet (or toward any gateway) with 2.7 Mbps traffic rate. When IRU or FIRM is used as a routing protocol, the path selected is N15-N10-N7. IRU selects this path because N8 has many neighbors (potential interferers). FIRM selects it so as not to share the link N6-N8 with the existing flow and consequently less expected path throughput compared with the alternative path. However, when we use FIRM$^+$ as the routing algorithm, the path N15-N6-N8 is selected because it considers the possible throughput reduction on the N2-N13 flow. Fig. 4 shows the throughput of each flow when FIRM or IRU is used. The existing flows starts sending their traffic at 0 sec. When the new flow from N15 to N7 starts at 10 sec, the existing flow from N6 to N8 continues to achieve almost 1Mbps throughput because this path is not interrupted by any other flow. However, the flow from N2 to N13 is substantially degraded by almost 50% because of hidden-interference from the new flow. Overall, the total throughput of the network is about 4.5 Mbps. Fig. 5 shows the throughput of each flow when FIRM$^+$ is used. When the new flow is added at 10 sec, in contrast to FIRM, the flow from N2 to N13 is not affected by the new flow. The throughput of the flow from N6 to N8 is slightly degraded due to the carrier sensing relation with the new flow. The total network throughput is almost

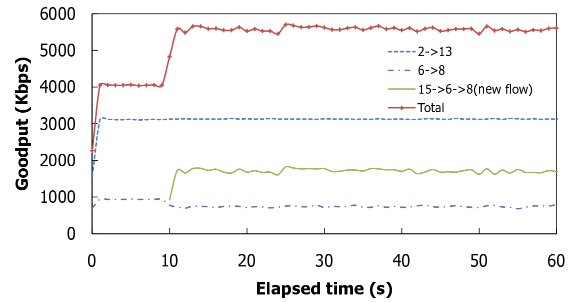

Fig. 5. The total throughput and the throughput of each flow with FIRM$^+$.

TABLE I
SCENARIO SETTINGS.

scenario	1	2	3	4
number of source	6	6	12	12
number of flows per source	1	1	1	2
offered load of each flow (Mbps)	0.52	1.56	0.78	0.45
total network load (Mbps)	3.12	9.36	9.36	10.80
number of gateways	1	3	3	3

5.8 Mbps. From Fig. 4 and Fig. 5, we demonstrate that FIRM$^+$ achieves higher network-wide throughput than FIRM or IRU. This is due to the fact that FIRM$^+$ considers the effect on the throughput of the existing flows when a new flow is selecting its path.

C. Complex Scenarios

We test four scenarios with the number of flows increased from the simple scenario. Table I lists the setting parameters of the four scenarios. Note that in scenario 4, each source has two different flows, which may select different paths. In all four scenarios, the total offered load is configured to be larger than the capacity of the mesh network. Each flow arrives at the mesh network in 10 sec interval and we measure the total network throughput after all flows join the network. Each plot in Fig. 6 is the aggregated throughput of all flows for different routing algorithms. In all cases, FIRM$^+$ achieves the highest total throughput. The total throughput of FIRM is higher than that of IRU except for scenario 1. The reason is that IRU considers only the number of interferers along a candidate path. Meanwhile, FIRM selects a path by considering the traffic load of the relevant flows.

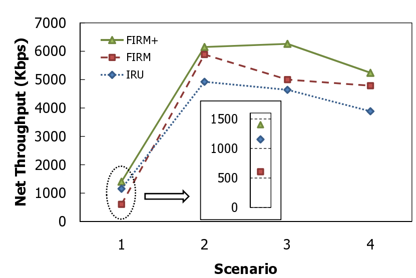

Fig. 6. Aggregated throughput in complex scenarios.

From Fig. 7, we observe that the total throughput changes over time with IRU, FIRM, and FIRM$^+$. Recall that each flow joins the mesh testbed at 10 sec interval. When the traffic

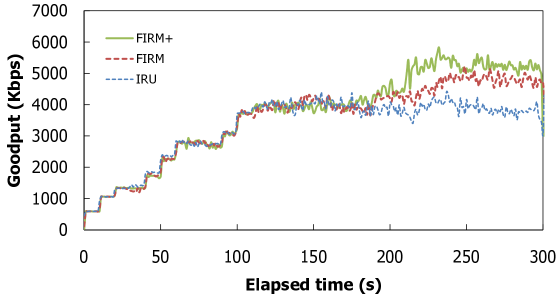

Fig. 7. The total throughput as a function of time in scenario 4.

load is light (until 100 sec), all routing protocols achieve the throughput almost equal to the sum of the offered load of all ongoing flows. Between 100 seconds and 180 seconds, when the overall traffic load is at a medium level, there is little difference between the three routing algorithms since the newly arriving flows do not degrade much of the throughput of the existing flows. After 180 seconds, as the traffic load increases and more links are saturated, FIRM$^+$ achieves higher throughput than others because it finds paths that degrade the throughput of the existing flows less than paths found by FIRM and IRU. When the offered load becomes the maximum with all the 24 flows being active, the packet drop ratio of IRU is 64% and it decreases to 51% with FIRM$^+$. Note that even though both IRU and FIRM search for the maximum bandwidth path in a greedy fashion, FIRM achieves higher throughput than IRU since IRU does not consider the throughput of individual flows in path selection.

V. Discussions

Our routing framework can be extended in many aspects. Although we fix the bit rate for simplicity, multi-bit rate can be taken into account in the modeling of the available bandwidth of a path. Since the available bandwidth analysis is based on the air time in our framework, it can be extended by considering MAC parameters and traffic load information. For instance, if we are aware of the traffic load of a flow, the packet size (or its distribution) of a flow, and the bit rate of each link, the air time can be readily analyzed. Taking one step further, in combination with the routing path assignment, we can assign optimal bit rates to all the links.

RBP and FIRM/FIRM$^+$ can easily adapt to multi-channel and/or multi-radio mesh networks. If there are multiple non-overlapping channels, we can apply RBP for the nodes (or their interfaces) that share the same channel. The topology map information of individual channels can be similarly used in FIRM and FIRM$^+$ routing algorithms.

VI. Conclusion

Recent studies on wireless mesh routing have focused on finding an interference-aware path with the maximum available bandwidth. However, the effect of a newly arriving flow on the performance of existing flows and the overall network throughput has been neglected. In this paper, we present a routing framework that considers both the throughput of the existing flows and the available bandwidth of a newly arriving flow. We proposed two routing algorithms: (1) FIRM seeks the maximum bandwidth path for the new flow, and (2) FIRM$^+$ finds the path that maximizes the sum of throughput of all the existing flows as well as the new flow. We carried out various experiments on a 15 node indoor IEEE 802.11a testbed and showed that FIRM$^+$ achieves higher total throughput than FIRM and IRU. FIRM outperforms IRU as IRU takes into account only the number of interferers while FIRM also considers the traffic load of the relevant flows.

Acknowledgments

This work was supported in part by the IT R&D program of MKE/IITA [2007-F-038-03, Fundamental Technologies for the Future Internet] and by Korea Research Council of Fundamental Science & Technology. The ICT at Seoul National University provides research facilities for this study.

References

[1] D. S. J. D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," *Wirel. Netw.*, vol. 11, no. 4, pp. 419–434, 2005.

[2] R. Draves, J. Padhye, and B. Zill, "Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks," in *Proc. ACM MobiCom*, Philadelphia, PA, USA, Sept. 2004.

[3] P. Kyasanur and N. H. Vaidya, "Routing and Link-layer Protocols for Multi-Channel Multi-Interface Ad Hoc Wireless Networks," *ACM SIGMOBILE Mobile Computing and Communications Review (MC^2R)*, vol. 10, no. 1, pp. 31–43, 2006.

[4] Y. Yang, J. Wang, and R. Kravets, "Load-balanced routing for mesh networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 10, no. 4, pp. 3–5, 2006.

[5] H. Zhai and Y. Fang, "Impact of routing metrics on path capacity in multirate and multihop wireless ad hoc networks," in *Proc. IEEE ICNP*, Santa Barbara, CA, USA, Nov. 2006.

[6] T. Salonidis, M. Garetto, A. Saha, and E. W. Knightly, "Identifying high throughput paths in 802.11 mesh networks: a model-based approach," in *Proc. IEEE ICNP*, Beijing, China, Oct. 2007.

[7] M. Genetzakis and V. A. Siris, "A contention-aware routing metric for multi-rate multi-radio mesh networks," in *Proc. IEEE SECON*, San Francisco, CA, USA, June 2008.

[8] A. Kashyap, S. Ganguly, S. R. Das, and S. Banerjee, "VoIP on Wireless Meshes: Models, Algorithms and Evaluation," in *Proc. IEEE INFOCOM*, Anchorage, AK, USA, May 2007.

[9] K. Jain, J. Padhye, V. N. Padmanabhan, and L. Qiu, "Impact of interference on multi-hop wireless network performance," in *Proc. ACM MobiCom*, San Diego, CA, USA, Sept. 2003.

[10] J. Lee, S. J. Lee, W. Kim, D. Jo, T. Kwon, and Y. Choi, "RSS-based Carrier Sensing and Interference Estimation in 802.11 Wireless Networks," in *Proc. IEEE SECON*, San Diego, CA, USA, June 2007.

[11] J. Ryu, J. Lee, S.-J. Lee, and T. Kwon, "Revamping the ieee 802.11a phy simulation models," in *Proc. ACM MSWiM*, Vancouver, BC, Canada, Oct. 2008.

[12] J. Lee, W. Kim, S. J. Lee, D. Jo, J. Ryu, T. Kwon, and Y. Choi, "An Experimental Study on the Capture Effect in 802.11a Networks," in *Proc. ACM WiNTECH*, Montreal, Canada, Sept. 2007.

[13] J. Padhye, S. Agarwal, V. Padmanabhan, L. Qiu, A. Rao, and B. Zill, "Estimation of Link Interference in Static Multi-hop Wireless Networks," in *Proc. ACM IMC*, Berkeley, CA, USA, Oct. 2005.

[14] S. Ray and D. Starobinski, "On False Blocking in RTS/CTS-Based Multihop Wireless Networks," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 2, pp. 849–862, Mar. 2007.

[15] Y. Li, L. Qiu, Y. Zhang, R. Mahajan, and E. Rozner, "Predictable performance optimization for wireless networks," in *Proc. ACM SIGCOMM*, Seattle, WA, USA, Aug. 2008.