Architecture for Delay-Sensitive Communications in Mobile Optical Free-Space Networks

Ionut Cardei
Florida Atlantic University
icardei@cse.fau.edu

Allalaghatta Pavan
Honeywell Labs

Riccardo Bettati
Texas A&M University

***Abstract*-Mobile Optical Free Space networks are an emerging architecture that can provide high speed connectivity between a ground-based backbone network and mobile users in challenging environments. In such a network traffic could be relayed by airborne or ground routers using wireless optical links. The variable nature of the wireless optical channel complicates support for real-time distributed applications demanding bounds on communication delay. In this paper we present an architecture for provisioning end-to-end statistical delay guarantees in MOFS networks. We describe a delay model that uses a concept of virtual traffic to accommodate link capacity variation. The link delay estimation is integrated with a population-insensitive utilization based flow admission control technique and IP Differentiated Services. The models and architecture for QoS are presented and the system performance is analyzed.**

I. Introduction

The concept of a Mobile Optical Free Space (MOFS) network involves a range of ground and airborne communication nodes that extend Gbps connectivity from the ground-based fiber network backbone to forward deployed terminals or subnetworks located in or close to an area of operation (Fig. 2). Such a network could have applications for homeland defense, ad-hoc high speed connectivity for remote networks, and infrastructure-less networking in urban areas.

DARPA* sponsors the THOR program that targets development of key enabling technologies for MOFS networks [1], [2]. Several key issues are being addressed to implement this network. The first problem is beam pointing, acquisition and tracking (PAT) with a lightweight terminal on a mobile platform [3]. Another issue is signal fading caused by scintillation from atmospheric turbulence, especially on long links [4]. Fading is mitigated by terminals with improved link margins and by using Forward Error Correction (FEC), Automatic Repeat reQuest (ARQ) or a hybrid data link protocol [5]. Similarly, cloud obscuration is a major issue for any wireless optical network, as links may become unusable due to absorption. Using multi-link terminals, the connectivity throughout the network increases and redundant/backup links can be set up. When clouds intervene and obscure links, new connections are established between nodes that have clear line of sight, and packets are routed on alternate paths.

Once the technological problems of implementing the free-space wireless links in a mobile and dynamic environment are solved, a major issue still remains communication Quality of Service. Users expect the same application performance as in wired networks.

The main objective of our project is the design a set of protocols for MOFS network, collectively called *OptiExpress*, a) NetEx, for statistical QoS guarantees for end-to-end communication QoS and b) HydraNet-DS, for fault tolerant TCP services. OptiExpress includes a QoS mechanisms capable to accommodate variations in network quality at different levels, and still provide acceptable communication services. Specifically, it can accommodate link quality degradation causing link capacity variation, short term link outages (< 10 ms), topology changes, and long term link outages. Our approach leverages standard IP protocols and is implementable on COTS IP routing equipment with only minor changes to the IP protocol stack.

In this paper we report on the QoS architecture for statistical delay guarantees for end-to-end packet communication. Another area of our research is a mechanism, HydraNet-DS, for reliable TCP services that uses transparent connection redirection and server replication. This will be presented in another article.

Our approach for QoS uses a model for the probabilistic behavior of the optical link capacity and a description of the application traffic to derive a statistical model for end-to-end packet delays. With this model, described in Section II, the QoS architecture determines the probability that a random packet exceeds the delivery deadline on a link (delay violation probability). The model is extended for end-to-end probabilistic guarantees on the links that form the route from a flow source to the destination. The QoS architecture can

*This material is based upon work supported by the U.S. Air Force and DARPA under Contract No. F33615-02-C-1247. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. Air Force and DARPA.

handle changes to routes through a process of QoS reconfiguration that involves flow adaptation.

OptiExpress provides a service for QoS negotiation and admission control. Application controllers and network managers submit flow admission requests. Once the admission request is analyzed by a bandwidth broker, and the bandwidth demanded along the source-destination path is reserved, the flow is assigned a Differentiated Services Code Point [6] corresponding to values for bandwidth, delay and delay violation probability from the acceptable QoS domain. The admission algorithm limits the total bandwidth allocated per class for each link to the safe utilization limit. The theory described in Section II guarantees that all admitted flows will not exceed delay limits associated with the assigned traffic class. This approach for flow admission is called Utilization Based Admission Control and was first introduced in [7].

We implemented this architecture in the OPNET discrete event network simulator [8] and we evaluated its performance for various operational scenarios and applications.

Earlier results related to this project have been published in [9]. MOFS networks are an emerging technology. We believe this effort is the first to address the aspects of QoS in this type of network. However, QoS frameworks for wireless ad-hoc networks with RF links have been studied extensively. The greatest obstacle for QoS guarantees in MOFS networks is that link capacity is variable and connectivity is intermittent. In this context frameworks for delay guarantees developed for wired networks ([10],[11]) cannot be applied directly.

Ref. [12] proposes an approach for statistical delay and drop guarantees in single-hop wireless networks using admission control and earliest deadline first scheduling. The delay model requires the instantaneous channel state. In contrast, our approach models channel disturbance as virtual traffic which is used to reduce the utilization limit on a link. Other efforts for QoS in MANETs look into bandwidth reservation and QoS routing. Insignia [13] is an in-band signaling system for bandwidth reservation in IP MANETs compatible with multiple routing protocols. Other protocols for QoS routing are proposed in [14] and [15].

The next section describes the delay analysis for a link server, the end-to-end guarantees mechanisms and the QoS reconfiguration. Section III presents the QoS architecture in detail, including the network model, the QoS model and the protocol architecture. Section IV continues with a review of the performance results. The paper concludes in Section V with a summary and comments on future work.

II. Delay Guarantees

In this section we summarize the delay analysis on which the QoS architecture is based upon. Preliminary results for this analysis were initially published in [9]. In this paper we adapt its mechanisms to the MOFS network running the TCP/IP communication protocols.

A. Link Server Delay Analysis

The analysis applies to networks that use static-priority packet schedulers. Packets from real-time flows that must be delivered with delay limits are assigned to a traffic class. Each class is associated with a differentiated services code point (DSCP) [6] that defines how routers service the packet, inclusive the scheduling priority. For a packet of priority i, the *probabilistic delay guarantee* on a link is a bound on the probability that a random packet will exceed a deadline ε_i, and can be expressed as:

$$P(D_i > d_i) \le \varepsilon_i.$$

The packet delay D_i is a random variable, and d_i is the maximum acceptable deadline for the link.

Data links have variable bit rates and suffer from short-term interruptions. Define $C(t)$ as the capacity available for traffic on a link as a function of time. The maximum capacity on a link is C. C is perceived above the data link layer and is reduced by the effects of FEC and ARQ overhead. Then, $C(t) = C - C_v(t)$, where $C_v(t)$ is part of link capacity that is not available due to link quality variation and outages.

A resource model where the effective capacity for transmission on a link is time-variable $C(t)$, is equivalent to a model where the link capacity is indeed constant, C, and where a *virtual,* highest-priority traffic $C_v(t)$ models the variable part of the link data rate. Fig. 1 shows the concept of virtual traffic.

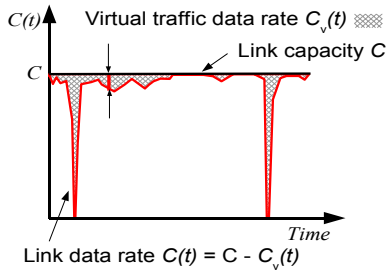

Fig. 1. Link capacity and virtual traffic.

Packet delays in the link model with the variable capacity $C(t)$ are equal to delays in the model with constant link capacity C and a virtual traffic $C_v(t) = C - C(t)$ that (virtually) is scheduled with the highest priority. Define $S(t)$ to be the stochastic service curve of the wireless optical link. Then, the virtual traffic has a service curve $B'(t) = C\ t - S(t)$. Now, assume G_i is the groups of flows of priority i arriving at a link of capacity C, and $b_{ij}(t)$ and $B_{ij}(t)$ are the deterministic and statistical traffic envelopes for the traffic arrival of the j^{th} flow from G_i. The delay violation probability on a link with variable quality is:

$$P(D_i > d_i) \le \max_{t>0} P(B'(t+d_i) + B^*(t+d_i) \ge C(t+d_i)), \quad (1)$$

where $B^*(t)$ is the service curve of the aggregated traffic of the same priority i and higher priorities. (note that priority 0 is the highest priority):

$$B^*(t+d_i) = \sum_{q=1}^{i-1} \sum_{j \in G_i} B_{q,j}(t+d_i) + \sum_{j \in G_i} B_{i,j}(t)\ . \quad (2)$$

$B^*(t+d_i)$ and $B'(t+d_i)$ are independent and the c.d.f. of their sum can be computed by convolution. It is important to notice that (1) is valid regardless of the wireless link model used.

If the number of flows is large enough and if they are independent, the distribution of $B^*(t+d_i)$ can be approximated

with the Central Limit Theorem. Let $n_j = |G_j|$ be the number of flows in group j on a link. We consider a deterministic leaky bucket arrival envelope for flows in G_j, $b_{i,j}(t) = \sigma_j + \rho_j t$, where ρ_j is the average flow data rate for class j and σ_j is the maximum packet size. By using a Gaussian approximation over intervals, the c.d.f. of $B^*(t+d_i)$ is bounded by a normal distribution $N(\phi_i(t), RV_i(t))$:

$$P(B^*(t+d_i)<x) \le \Phi\left(\frac{x-\phi_i(t)}{\sqrt{RV_i(t)}}\right), \quad (3)$$

where $\phi_i(t)$ is the mean aggregate data rate of the flows forming B^*, $\phi_i(t)=(t+d_i)\sum_{q=1}^{i-1} n_q\rho_q + t\, n_i\rho_i$. $RV_i(t)$ is the aggregate rate variance envelope of the B^* flows, $RV_i(t)=(t+d_i)\sum_{q=1}^{i-1} n_q\rho_q\sigma_q + t\, n_i\rho_i\sigma_i$, and $\Phi(a)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{a}\frac{e^{-x^2}}{2}dx$ is the c.d.f. of the normal distribution.

B. End-to-end Delay Guarantees

Once the delay violation probability for each link is computed, we determined the end-to-end delay guarantee along a path for a flow of priority i. d_i is divided into delay limits for each link along the path R: $d_i=\sum_{k\in R} d_i^k$. The end-to-end delay delay guarantee is satisfied when

$$P(D_i^e > d_i) \le 1 - \prod_{k\in R}(1 - P(D_i^k > d_i^k)) \quad (4)$$

One way to compute an end-to-end delay breakdown is to split it equally per link: $d_i^k = d_i/|R|$, for all links $k \in R$. Some links may be considerably slower than others, so a better approach is to assign a delay per link inverse proportional to the link capacity: $d_i^k = \frac{d_i}{C_k \sum_{j\in R} 1/C_j}$, for all links k belonging to route R. Before a flow can be admitted, the test (4) checks whether delay guarantees can be satisfied. This computation is time-consuming, since it involves convolutions and may impose a high overhead in scenarios with heavy load.

To avoid this overhead, our QoS architecture uses Utilization Based Admission Control, first proposed in [7]. Its goal is to avoid this costly computation for each flow admission. To do this, UBAC must use a delay computation that is insensitive to flow population. All flows from a class i share a dedicated fraction of the link capacity, $\alpha_i C$. Hence, admission control limits the total number of flows from a class i on a particular link to

$$n_i = \lfloor \alpha_i C/\rho_i \rfloor \quad (5)$$

with $\alpha_i \in [0,1]$ and $\sum_{class\, i} \alpha_i \le 1$. The isolation between classes guarantees that the assumptions for (2) and (3) are respected and, therefore, the delay guarantees are satisfied.

Using (5) the mean rate and the rate variance for the aggregate traffic of the same or higher priority from (3) are upper bounded, eliminating the dependence on flow count:

$$\phi_i(t) = (t+d_i)\sum_{q=1}^{i-1}\alpha_i C + t\,\alpha_i C \text{ , and}$$

$$RV_i(t) = (t+d_i)\sum_{q=1}^{i-1}\alpha_i\sigma_i C + t\,\alpha_i\sigma_i C \ . \quad (6)$$

These equations can be easily integrated into the computation of (3) and the end-to-end delay guarantee condition (4).

We notice that the delay guarantee model in this section only considers queuing delay and transmission delay. Other contributing delays that can be more easily estimated must be factored in during QoS reconfiguration and admission control, such as propagation delay, delay overheads from FEC, and packet forwarding.

C. QoS Reconfiguration

From a practical perspective, the user (e.g. application/network manager) defines the QoS specification for traffic classes, including σ, ρ, d^e_i and the flow priority. The user also defines the capacity partition $<\alpha_i>$, $i = 1..m$. It is very probable that the end-to-end delay constraints computed with (4) may not be satisfied for at least one flow class on at least one end-to-end path while using the original parameters. In this case the user could either increase the maximum delay limits or increase the delay violation probability for classes that do not have the end-to-end delay constraints satisfied. Both approaches are unacceptable from the user's viewpoint, as they interfere with the application QoS requirements.

Our approach to mitigate this issue is to uniformly reduce the link capacity allocated to all real-time traffic classes to a fraction ν, called *safe utilization bound*. The maximum number of flows from a class i admissible on a link of capacity C becomes

$$n_i = \left\lfloor \frac{\nu\,\alpha_i C}{\rho_i} \right\rfloor, \quad (7)$$

with $\nu \in (0,1)$, preferably $\nu \to 1$. All network capacity that is not used by real-time traffic will remain available for best-effort service. To select the highest possible value for the safe utilization bound we use binary search. The condition for selecting the lower/upper half is whether the delay guarantees hold for all classes and for all source – destination pairs. The search is in a continuous space and it stops when ν converges. For most scenarios used in our experiments, utilization bounds of 70 – 90% have been reached frequently.

To summarize, UBAC replaces the expensive admission-time convolution computation with a simple check if the number of flows of class i has exceeded limit n_i on all links along a route. In addition, UBAC requires the computation of the safe utilization bound, but only when at least one route changes.

After the safe utilization bound is computed, UBAC reconsiders admission for all flows for which the source-destination path has changed. If there are n admitted flows on a link and $n > n_i$, then $n - n_i$ lower priority flows are selected for adaptation. Admission is attempted in another class or the flow is terminated. Adaptation follows policies configured by the network application/manager.

This configuration process followed by re-admission for

some flows is called "QoS reconfiguration". It is performed only when routes change and not whenever a new flow is admitted to the network.

Limitations

There are several issues with the approach for QoS guarantees presented in this section.

1. One concern is that this method for computing ν artificially lowers the maximum link utilization because ν is computed to satisfy all links in the network – fitting one critical link and possibly underestimating for all others. Having additional information on traffic patterns and volume it is possible to use per-link safe utilization limits.
2. Dependency on routing information for computing ν requires a centralized solution. This is the trade-off for having UBAC, with its very cheap admission control, that simply limits flows count along a route. Route information is necessary in order to avoid storing flow state inside the network. With UBAC, flow state and reservation state is maintained only by the bandwidth broker.
3. Scalability. The number of single-path routes in the network is $O(|V|^2)$, where V is the set of edge routers. For large networks, the complexity of the QoS reconfiguration process may cause high overhead and increased latency penalties during transient periods when routes have not converged yet. In Section III we sketch an approach for improving scalability by partitioning the MOFS network into QoS domains.

D. Link Estimation

A leaky bucket model for the virtual traffic arrival is considered for the QoS reconfiguration procedure to compute the safe link utilization limits, as described earlier. The link capacity C is determined from the parameters of the optical terminal. Link rate history, weather information and theoretic link fault models are different ways to compute the leaky bucket parameters, σ_v and ρ_v, for the virtual traffic. Measurements for link faults [16] on wireless optical links indicated link outages of τ = 10 ms that occur on average every T = 1.5 s. A simple interpretation for a leaky bucket model is to consider that between outages the bucket fills with rate ρ_v . When it is full, a link outage "drains" the bucket at link capacity, C. Thus we have $\sigma_v = C\tau$ when the bucket drains during outage at full link rate, and $\sigma_v = \rho_v\ (T - \tau)$ when the bucket is "filled in" between two consecutive outages. We derive:

$$\sigma_v = C\tau \text{ and } \rho_v = C\tau\ /(T-\tau). \quad (8)$$

For a 2.5 Gbps link, the virtual traffic burst size is σ_v = 3,125,000 bytes and the data rate is ρ_v = 25 Mbps.

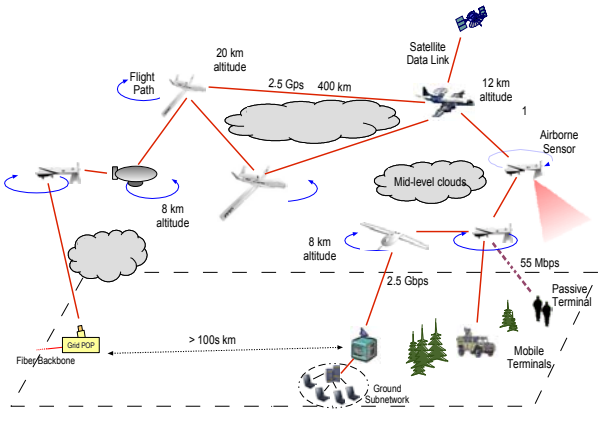

Fig. 2. Notional MOFS network topology.

In general, measuring the effective data link capacity $C(t)$ may not be practical since it requires the link to be continuously active at full load. A better approach is to have the link layer record link outages and their duration. Let the set of faults be $\langle t_i, \tau_i \rangle_{i=1..m}$, where t_i represents the time when fault i - 1 has completed and τ_i represents fault i duration. Assuming that prior fault history is a predictor for the future behavior, a leaky bucket model envelope can be defined as follows:

$$\sigma_v = C \max_{i=1..m} \tau_i \text{ and } \rho_v = \max_{i=1..m} \frac{\sigma_v}{t_{i+1} - t_i - \tau_i} \quad (9)$$

III. QoS Architecture

A. The Network Model

A notional MOFS topology is depicted in Fig. 2. The objective for this network is to connect to the optic fiber backbone (e.g. the Global Information Grid) remote and mobile ground terminals/subnetworks using high speed wireless laser links (e.g. speeds higher than 2.5 Gbps). A multihop path is established from one or more fiber backbone points of presence (POP) to the communication end points. Each air vehicle carries aboard a router and multiple wireless optical I/O interfaces (apertures), implementing an ad-hoc multihop topology. These vehicles can also generate traffic from sensors such as radars or cameras.

Point to point links are established when two nodes point a transmitter to each other's optical aperture. Wireless laser links will soon achieve data rates between 45 Mbps for passive terminals and 2-10 Gbps for active terminals, on distances for up to hundreds of kilometers for links deployed at high altitudes where adverse atmospheric effects are minimal. A thorough review of emerging technologies relevant to MOFS networks and supported by DARPA is given in [2].

When a link is obscured by clouds or terrain, an airborne relay node reroutes traffic on another link already established. If no alternate links are available, the relay node points the laser beam to another node within line-of-sight (LOS) to establish a new connection. The network topology configuration process and the PAT procedure are conducted with a secondary RF network. The network availability increases with higher connectivity, which is enabled by relay nodes with multiple apertures. Some airborne nodes may have the main mission of routing traffic. Their flight trajectory is planned to improve LOS connectivity and to avoid beam obscuration. Aircraft passing through the area of network operation can temporarily assist relaying data if equipped with compatible optical terminals. Ref. [17] presents an approach for topology control in MOFS networks.

The admission control algorithm needs access to routes and

link state. In our implementation EIGRP [18] exports routes and reports node reachability to the bandwidth broker. The QoS architecture is capable to support other routing protocols.

B. The QoS Model

This section describes how packet flows are provisioned QoS in the MOFS network with NetEx. We start by defining a few terms. A *managed* flow is a packet flow that went through admission control and for which the networks provides statistical delay guarantees. A *legacy* application is ported from existing networks to the MOFS network without modifications in code. A *QoS-aware* application requires real-time communication services from the network and is dependent on bounds to end-to-end packet delay and bandwidth.

An admission request request has a series of parameters to be processed by the bandwidth broker:

- o protocol type (TCP, UDP)
- o source, destination IP addresses
- o flow priority
- o a descriptor for end-to-end network QoS:
  - maximum burst size M
  - delay interval $[D_{min}, D_{max}]$
  - average transmission rate interval $[R_{min}, R_{max}]$
  - delay violation probability interval $[E_{min}, E_{max}]$.

The delay violation probability (DVP) is $P\{D_i \geq D_{max}\} \in [E_{min}, E_{max}]$. Using intervals for QoS allows the admission control algorithm to be flexible in assigning resources, as most real-time applications tolerate a range of network performance anyway. These applications are capable to *adapt* to a variation in bandwidth and delay and to continue to operate satisfactory. The *current operational point* (COP), defined by <*M, D, R, E*>, describes the instantaneous values of the flow QoS measures perceived by the application.

The network manager defines the set of traffic classes and assigns for each class an operational point in QoS parameter space (*M, D, R* and *E*). An IP queuing policy is set that maps the packet class (DSCP) to a scheduling priority. For the simulation study, we assigned higher priority for traffic classes that require lower delay. As a condition for providing probabilistic delay guarantees, connection admission control assisted by traffic policing at the network edge routers keep

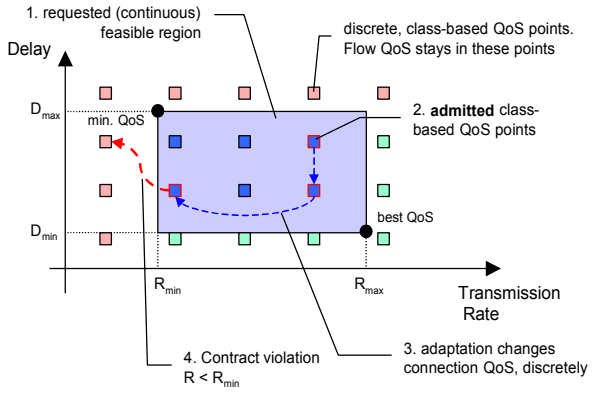

Fig. 3. QoS mapping to traffic class and adaptation.

the total managed traffic data rate from class i below $\nu_k \alpha_i C_k$ on each link k, where $\Sigma_{class\ i} \alpha_i \leq 1$, C_k is the (unidirectional) link k data rate capacity, including effects from coding and ARQ, and ν_k is the safe bandwidth utilization boundaries for link k. The difference to 1 is available for best effort traffic. A sample traffic class configuration is shown in Table I. IPv6 packets larger than 64KB (*jumbograms)* are described in [19].

C. Admission and Adaptation

Applications or network management components submit admission requests to the bandwidth broker. The admission control algorithm selects one class from the set of classes whose corresponding <*M, D, R, E*> parameters fall within the requested QoS region. If not such class exists, than admission

TABLE I
SAMPLE CLASS QOS SPECIFICATION.

Class	Prio-rity	M (kB)	R (Mbps)	D (ms)	α_i	E	Descrip-tion
0	8	128	10	80	5%	0.5%	10 Mbps Sensors
1	7	128	20	100	5%	0.8%	MPEG2 20 Mbps
2	6	521	45	100	15%	1.0%	CDL 45 Mbps
3	5	521	100	100	25%	1.0%	VPN
4	4	1024	274	100	45%	1.0%	CDL 274 Mbps

control selects a class i with $R_i \geq R_{min}$, $D_i \leq D_{max}$, $E_i \leq E_{max}$, $M_i \geq M$, and for which there exists bandwidth available within $\nu \alpha_i C_k$ for all links k on the source to destination path. In case no class exists with these parameters, admission is denied and the negotiating party can resubmit the request with a different QoS demand. If admission control cannot find a feasible class with enough bandwidth available along the source-destination path, then some other flows with a lower priority may be preempted or switched to other classes. The QoS architecture performs this *adaptation* in order to accommodate more flows of higher priority. The applications (or network management agents) owning the modified flows are being notified of the adaptation and can react accordingly. An admission/adaptation scenario is shown in Fig. 3.

The admission request is valid for a specific time interval and must be renewed using a lease mechanism. A negotiated flow for which the lease expires ceases to receive QoS. Its packet classification policy will be revoked from the ingress router and it will be marked with a best effort priority.

Admission and adaptation are controlled by a set of policies designed to meet certain objectives. For instance, selection of flows to adapt/preempt in order to admit a higher priority flow can be based strictly on priority, or on a combination of priority, endpoint address, and packet content type. These policies depend on the network's main mission and are not addressed in this paper.

D. Protocol Architecture

The NetEx QoS architecture works with the standard IP protocol stack and routing protocols. Core routers are not directly connected to managed traffic endpoints. The only

specific requirement for them is to have static-priority packet scheduling at the IP layer. Fig. 4 illustrates the protocol architecture of a node in the MOFS network involved in routing and also executing managed applications. Such a node could be aboard of an aircraft, assisting with traffic relay and also transmitting sensor data to ground nodes.

The **NetEx Resource Management** component includes:

- an API library for negotiation and adaptation with the bandwidth broker.
- policies and configuration for controlling IP packet classification, policing and queuing. .
- monitoring of link and routing state. Non-transient changes to node connectivity (e.g. new link established, or link down) are reported to the bandwidth broker to speed up QoS reconfiguration.

The NetEx components communicate with the bandwidth broker using TCP connections.

The **Network Management** component interfaces NetEx with network management applications, or other QoS configuration platforms. Configuration tasks include a setting policies (e.g. for admission/adaptation) and configuration (class flow specs, link capacity partition per class). A network manager or an "application manager" can submit flow admission requests on behalf of legacy applications that need delay guarantees.

The **Applications** component represent any application that transmits managed flows. QoS-aware, adaptive applications are designed to interface with NetEx. Legacy QoS-aware applications, such as H.323 video conferencing, are provisioned managed flows through application configuration tools that translate application specific QoS metrics (e.g. frame rate, video frame size) into the QoS parameters understood by NetEx. Ref. [20] presents an example for QoS translation. Applications communicate using the standard socket libraries.

The **IP** component includes classification, policing and scheduling. The **classifier** is used to mark packets from managed flows at network ingress with the right DSCP corresponding to the negotiated class of service. The packet **policer** enforces flow bandwidth according to the leaky bucket specification associated to the flow class (a packet metering component is not shown). The packet **scheduling** block implements a static-priority scheduling policy.

The **IP Routing Protocol** does routing and exports routing information to the bandwidth broker. Routes are used both for computing the safe utilization level during QoS reconfiguration, and for admission control, when bandwidth availability is checked along the flow source-destination path. Currently, our architecture only supports single-path routing. Multi-path routing with load balancing would require a tighter integration of our architecture with the routing protocol.

Not shown in Fig. 4 is the bandwidth broker (BB). This is executed as a TCP service, preferably on a router node with high-bandwidth and good connectivity. The BB needs current routing information to determine the network topology. The next section proposes approaches for improving bandwidth broker scalability and fault tolerance.

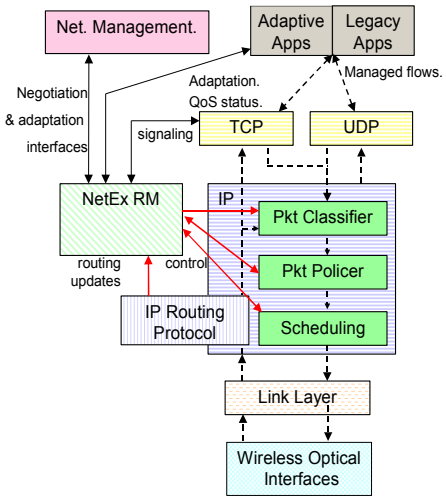

Fig. 4. Architecture of a MOFS node / edge router.

Bandwidth Broker Scalability

The QoS reconfiguration process and the admission control need access to routing information and link capacities. In the current stage of our research these are executed on a central server, the bandwidth broker, implemented as a TCP service. A distributed implementation for admission control is a challenging problem that deserves attention.

To improve the scalability of centralized admission control, we propose to partition a large MOFS network into *QoS domains*, each with a bandwidth broker managing resources and providing end-to-end probabilistic delay guarantees withing its boundaries. For a flow that spans multiple QoS domains, the BB from the source QoS domain would divide the end-to-end admission request into individual requests sent to BBs from QoS domains traversed by the flow path. This protocol is similar to the admission/adaptation protocol from DYNAMIQUE [21].

The MOFS network dynamic topology may get partitioned. To provide a degree of reliability we consider implementing the bandwidth broker service as a replicated service using the HydraNet-DS framework for fault tolerant TCP services.

E. Provisioning Support for Legacy Applications and Subnetworks

One of the objectives of the QoS architecture was to support real-time communications for legacy applications – existing applications, ported to the MOFS network, that do not directly negotiate with NetEx, or are not QoS-aware. Since the mechanisms for delay guarantees are implemented in the IP layer (classification/policing/scheduling), any IP packet flow can be effectively managed, provided the above IP components are properly configured. We next describe three mechanisms designed for QoS provisioning:

1.*QoS request negotiation*. Application/controller negotiates a request for the duration of the flow. The request will be renewed periodically using the lease mechanism.

2.*Automatic flow provisioning (policy-based)*. Application controller/network manager sets up policies for QoS with the

BB. When an edge router classifier identifies a flow according to some policy rules, it asks the NetEx components to submit a corresponding admission request to the BB. If admission succeeds, then the flow will have delay guarantees. Otherwise, the flow will be assigned to a "best effort" class or denied admission. A managed flow that is idle for a configurable amount of time will cause deallocation of resources. Consequently, its packets will be marked "best effort".

3.*Persistent flow provisioning.* This is similar to automatic provisioning, except that the flow resources are assigned permanently. Persistent flows do not "expire" and do not require lease renewal. This mechanism can be used for low data rate, low latency flows, for which negotiation overhead must be avoided. The NetEx signaling protocol TCP flows are preallocated.

All three mechanisms can be used for legacy applications. In addition, using automatic or persistent flow provisioning, traffic generated from a subnetwork that is not part of a BB QoS domain can be managed starting from the ingress router. Classification policies at the ingress router allow association of packets to flows. Through marking with the proper class DSCP, these packets will be provisioned the same degree of QoS as for flows of the same class managed by a negotiation process.

IV. Performance Evaluation

A. Simulation Scenarios

We present in this section a summary for performance results measured using OPNET simulations. We defined MOFS topologies similar to the one in Fig. 5. All links have a 2.5 Gbps capacity and experience intermittent link faults of variable duration. The network runs the EIGRP routing protocol, configured to test neighbor reachability every 250 ms. The IP forwarding code has been modified to hold off transmitting packets to the link layer when the outgoing link is interrupted. This is feasible in practice, since the optical aperture can detect when the signal breaks down and in general the outage affects connectivity in both directions.

We ran the bandwidth broker on node *air2* and submitted admission requests for managed flows between the *ground* nodes. The network was also loaded with best effort traffic (http and email). In all, we focused on application performance under heavy load, as this is when a QoS architecture provides most value.

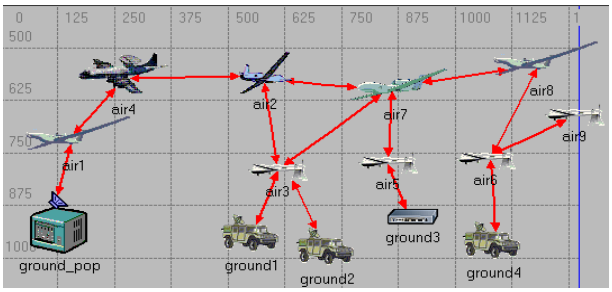

Fig. 5. Simulation scenario topology.

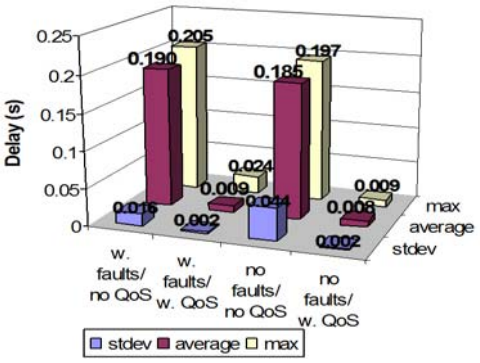

Fig. 6. End-to-end delay for managed flows.

Safe utilization bound

The safe utilization bound for real-time flows with 10 ms independent link faults (1.5 s inter-arrival time) was 80.55%. With 25 ms faults, the utilization limit decreased to 74.98%. With faults longer than 50 ms, the utilization limit drops gradually from 72% to 0%.

End-to-end Delay

The average, maximum end-to-end delays and the standard deviation are shown in Fig. 6 for 4 scenarios combining enabled/disabled QoS, and link fault presence (10 ms duration/1.5 s average interarrival time). When QoS is disabled all traffic flows (including NetEx signaling) are scheduled with FIFO policy and delay cannot be guaranteed. The maximum delay dropped from 205 ms to 24 ms when NetEx was enabled (with link faults). Similar improvement scale can be noticed for both average delay and jitter (*stdev*). All scenarios were run with the network saturated with best effort traffic. Per class average delay is shown in Fig. 7.

For a video conferencing application (500 kbps CBR 20 fps), configured as a legacy application, the average delay dropped from 221 ms to 6.95 ms when NetEx automatically provisioned a flow with class 0. The jitter dropped 8 times to 4.46 ms with QoS.

Reconfiguration Delay

The bandwidth broker was set to do a QoS reconfiguration whenever routes changed, as indicated by the routing tables exported by EIGRP. During reconfiguration, the BB recomputes the safe utilization bounds for all links, recomputes admission for all flows and signals QoS adaptation

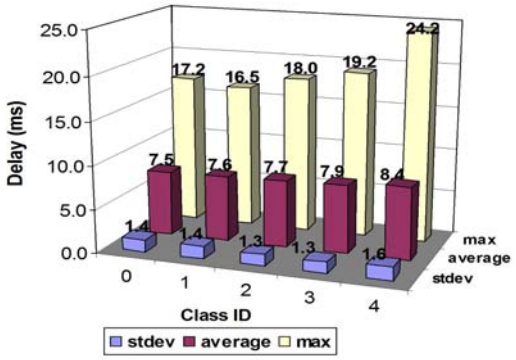

Fig. 7. Per class end-to-end delay.

to NetEx components on hosts and edge routers. We measured an average reconfiguration delay of 337 ms, including EIGRP route convergence overhead.

Admission Delay and Protocol Overhead

The average admission delay was 115.89 ms, with 10 ms link faults, and 10.1 ms with no link faults, respectively. The NetEx signaling protocol overhead was measured in sustained load conditions with 68 admission requests per second. The measured aggregated peak overhead reached 3540 kbps (1.5% of link capacity), while the average overhead was 206 kbps (0.0082% of link capacity). The overhead included flow lease renewals every 60 s. We notice that the mean protocol overhead for signaling is very low when compared to the link capacity.

V. Conclusion

Mobile Optical Free Space networking is an exciting new technology that would close the connectivity gap between high speed ground fiber networks and mobile users deployed in remote or inaccessible areas. The variable nature of the wireless optical link raises barriers to deployment of real-time distributed applications that need low-latency communication with delay guarantees.

In this paper we present a QoS architecture that provides statistical delay guarantees for end-to-end communication in the optical wireless network. The delay model uses statistical service curves to represent link capacity and traffic arrival. During QoS reconfiguration, a safe bound for capacity utilization by real-time traffic is computed, using routing information and traffic class QoS specifications. This capacity utilization bound limits the number of real-time packet flows during the Utilization Based Admission Control procedure. A model of virtual traffic arrival estimates the capacity variation of the wireless optical links. The virtual traffic service curve is included in the delay computation algorithm as traffic with the absolute highest scheduling priority.

We also describe how QoS reconfiguration and admission control are implemented, and how legacy applications and subnetworks could be provisioned QoS using IP packet classification at the ingress routers. We present performance results that validate our approach.

NetEx can be further improved. The centralized bandwidth broker architecture can be replaced with a distributed architecture, possibly using RSVP or MPLS for enforcing link utilization limits. As an alternative, we consider implementing the bandwidth broker service as a replicated TCP service using the HydraNet-DS mechanism.

References

[1] DARPA, THOR Program, http://www.darpa.mil/ato/programs/THOR

[2] B. Stadler, G. Duchak, "Terahertz operational reachback (THOR) a mobile free space optical network technology program", in *Proc. of IEEE Aerospace Conference*, 2004

[3] G. Ortiz et al., "Design and development of a robust ATP subsystem for the Altair UAV-to-Ground Lasercomm 2.5 Gbps Demonstration*", Proc. of the SPIE*, Vol. 4975, 2003

[4] V.V. Ragulsky, V.G. Sidorovich, "On the Availability of a Free-Space Optical Communication Link Operating Under Various Atmospheric Conditions", *Proc. of SPIE*, 2003

[5] S Choi, KG Shin, "A Class of Adaptive Hybrid ARQ Schemes for Wireless Links", *IEEE Trans on Vehicular Technology*, vol. 50, 5/2001

[6] S. Blake, et al. "An Architecture for Differentiated Services", RFC 2475

[7] S. Wang, D. Xuan, R. Bettati, W. Zhao. "Providing absolute differentiated services for real-time applications in static-priority scheduling networks. *Proc. IEEE Infocom*, Anchorage, AK, USA, 2001.

[8] OPNET, http://www.opnet.com

[9] S. Wang, R. Nathuji, R. Bettati and W. Zhao, "Providing Statistical delay Guarantees in Wireless Networks." *Proc. IEEE International Conference on Distributed Computing Systems*, Tokyo, 03/2004

[10] E. Knightly, "Enforceable quality of service guarantees for bursty traffic streams," *Proc. of IEEE Infocom*, San Francisco, CA, USA, 3/1998.

[11] J. Liebeherr, D. Wrege, and D. Ferrari, "Exact admission control in networks with bounded delay services," *IEEE/ACM Transactions on Networking*, vol. 4, no. 6, pp. 885–901, December 1996.

[12] P. Chaporkar, S. Sarkar "Providing stochastic delay guarantees through channel characteristics based resource reservation in wireless network", *Proc. of 5th ACM Int. Workshop on Wireless Mobile Multimedia*, 2002.

[13] S.B. Lee, G.S. Ahn, A.T. Campbell, "Improving UDP and TCP performance in mobile ad hoc networks with INSIGNIA", *IEEE Communications Magazine*, Vol. 39 , Issue 6 , 6/2001, pp. 156 – 165

[14] C. Shigang; K. Nahrstedt, "Distributed quality-of-service routing in ad hoc networks", *IEEE JSAC*, Vol. 17, Issue 8, 08/1999, pp. 1488 – 1505

[15] Z. Chenxi, M.S. Corson, "QoS routing for mobile ad hoc networks", INFOCOM 2002. *Proc. 21st Annual Joint Conference of the IEEE Computer and Communications Societies*. , Vol. 2 , 23-27 June 2002.

[16] Communication from ITT Industries, 10/2002.

[17] J.Zhuang, M.J. Casey, S.D. Milner, S.A. Gabriel, G. Baecher. "Multi-Objective Optimization Techniques In Topology Control Of Free Space Optical Networks", *Proc. IEEE MILCOM*, November, 2004.

[18] Cisco, "Enhanced Interior Gateway Routing Protocol", http://www.cisco.com/warp/public/103/eigrp-toc.html

[19] RFC 2675 - IPv6 Jumbograms, http://www.faqs.org/rfcs/rfc2675.html

[20] I. Cardei, R. Jha, M. Cardei, A. Pavan, "Hierarchical Architecture For Real-Time Adaptive Resource Management", *The IFIP/ACM International Conference on Distributed Systems Platforms and Open Distributed Processing*, April 2000.

[21] I. Cardei, S. Varadarajan, A. Pavan, L. Graba, M. Cardei, M. Min, "Resource Management for Ad-hoc Wireless Networks with Cluster Organization, *Journal of Cluster Computing in the Internet*, Kluwer Academic Publishers, Vol. 7, Issue 1, pp. 91-103, 01/2004.