A Differentiated Services QoS Scheme Preventing Malicious Flow Behavior in Mobile Ad hoc Networks

Margaritis Margaritidis, Christopher N. Ververidis, George Xylomenos, George C. Polyzos
Mobile Multimedia Laboratory
Department of Informatics
Athens University of Economics and Business
Patision 76, Athens 104 34, Greece
Email: {margarit,chris,xgeorge,polyzos}@aueb.gr

***Abstract*— The design of an efficient Quality of Service (QoS) scheme for a Mobile Ad hoc Network requires addressing all the challenging characteristics of such a network. Specifically, a QoS scheme for such an environment must have a light-weight implementation, in terms of both storage and processing requirements, must be scalable and keep the signaling overhead to a minimum, must focus on differentiated services instead of "hard" guarantees, and must provide the necessary incentives for the flows to be cooperative. This paper describes such a QoS scheme which manages to meet all the aforementioned requirements while still having a simple, yet effective, implementation.**

I. Introduction

Designing an efficient and effective QoS scheme for a *Mobile Ad-Hoc Network* (MANET) is a very challenging task, due to the unique characteristics of these networks. A MANET consists of numerous small, fast moving devices, interconnected in an unstructured manner, and having a wide range of communication, storage and processing capabilities. This differs dramatically not only from a typical wired network, but also from a hierarchical, base-station based, wireless network. The latter type of network is somewhat similar to a MANET, but the fact that it is a single-hop network coordinated by base-stations, significantly simplifies the design of appropriate QoS schemes.

The most important factors that should be taken into account when designing a QoS scheme for a MANET are the following:

1) Due to the distributed control in MANETs, every node must be able to implement the QoS scheme. Considering the wide range of devices that may participate in a MANET, we can see that the processing and storage requirements of the supporting scheme should be minimal.
2) The dynamic and unstructured layout of a MANET causes frequent changes in the connectivity of each device and, consequently, in the paths taken by each flow. As a result, the QoS scheme should periodically refresh the state of each flow, with a frequency directly proportional to the instability of the end-to-end path. This requirement induces signaling overhead and, therefore, the scheme should be designed to be as light-weight as possible.
3) The size of a MANET can grow arbitrarily, since it is not hierarchically structured. Therefore, any QoS scheme applied in such an environment must be scalable in order to be effective.
4) A typical MANET layout consists of many devices with small transmission ranges that move frequently, interfere with each other and are affected by the presence of physical obstacles. This causes frequent and severe variations to the quality and capacity of the shared wireless medium. Thus, the provision of "hard" resource guarantees in such an environment is extremely difficult.
5) The admission control procedures of a QoS scheme require accurate estimation and allocation of the link resources. The shared access to the wireless link by several devices however, coupled with the fluctuating link quality, allows only coarse estimations or predictions to be made regarding the available resources of a MANET.
6) The high traffic volumes expected in a MANET cause relentless contention for resources between the existing flows, which may occasionally lead some sources to exhibit malicious behavior in order to gain an unfair advantage over the competition. A typical behavior of this sort is the declaration of false information regarding the transmission rates and the adaptation capabilities of the flow.

In order to address these factors, an effective QoS scheme for a MANET should exhibit the following characteristics:

1) Distributed and light-weight implementation.
2) Minimum per flow storage and processing requirements at each node.
3) Minimum signaling overhead.
4) Scalability.
5) Soft resource guarantees, based on differentiated services.
6) Incentives to prevent malicious behavior by non-cooperative flows.

In this paper, we propose a QoS scheme that meets all the

aforementioned requirements in order to provide service differentiation for adaptive flows in a MANET. The contribution of the proposed scheme is that it addresses all the factors that uniquely characterize a MANET, paying special attention to the prevention of malicious behavior by non-cooperative flows.

The remainder of this paper is structured as follows. Section II provides essential background on QoS schemes for MANETs by presenting related research efforts along with their advantages and disadvantages. Section III describes our proposed QoS scheme and presents a qualitative evaluation of it. Section IV concludes and summarizes this work and refers to our future research directions. Finally, the Appendix provides an initial theoretical estimation of the operational parameters of the proposed QoS scheme.

II. Related Work

Many QoS schemes that have been proposed in the literature are specifically designed to fit the characteristics of a MANET. They typically follow a cross-layer architecture, which is more effective, albeit more difficult to implement and deploy [1], [2], [3]. A few QoS schemes take a pure end-to-end approach [4], while others concentrate solely on the local wireless link of each node [5], [6], [7]. Most schemes however prefer an intermediate approach, where the edge nodes cooperate with the intermediate nodes, in order to provide the best QoS possible for each flow [2], [3], [8], [9], [10], [11], [12].

The main drawback of existing schemes is that they usually address only a subset of a MANET's parameters. As a result, they either restrict their applicability into specific MANET topologies or suffer from degraded performance due to their neglect of the impact of the remaining parameters. For example, some schemes attempt to provide "hard" guarantees, an extremely difficult task since they can rarely make accurate estimations of the available resources; unfortunately, admission control procedures based on available bandwidth are inaccurate over the shared wireless links of a MANET [3], [8], [9], [10], [11], [12]. Other schemes attempt to provide "hard" guarantees by throttling down the unaware best effort traffic [6], [10], [11]. However, when the demanding real-time traffic overwhelms the link, they arbitrarily drop flows in order to resolve the congestion, indiscriminately penalizing both old and new flows [6], [8].

Several other schemes implement a differentiated services scheme, implemented by the MAC or link layer of intermediate nodes [5], [8], [13]. There are two main approaches. The first is per-flow queuing, typically with a different queue for each traversing flow and some kind of prioritized or balanced interleaving of the wireless medium [2], [3], [5], [7]. In this approach, each node selects the best candidate for transmission from the packets on the head of all the existing queues and then contends for the channel. The problem is that such scheduling requires a powerful processor and a large amount of storage space per-flow from potentially small and light intermediate nodes.

The second approach is to modify the behavior of the MAC protocol. 802.11 does not provide any guarantees since the *Distributed Coordination Function* (DCF) commonly implemented in 802.11 devices avoids any coordination between the competing nodes. Lately, 802.11e was designed, with an *Enhanced DCF* (EDCF) that alters the contention windows of each flow according to its requirements [14]. Similarly, other QoS schemes alter the parameters of the MAC protocol, in order to provide structured, prioritized or temporal fair sharing of the wireless medium [7], [10], [13], [15], [16]. The drawback of these solutions is that they provide neither resource guarantees nor fair sharing of the wireless medium, while imposing high processing and storage requirements.

Moving up the layers, there are many QoS schemes attempting to solve the problem end-to-end. Although most of them use local information from the intermediate nodes to make decisions, their main functionality lies at the edges of the path [3], [11], [17]. These are mostly cross-layer schemes which probe the end-to-end path for a bottleneck. They then adapt the flows according to the bottleneck's resource availability. Due to the dynamic nature of a MANET, these schemes only provide "soft" reservations that are periodically refreshed. This approach has two main drawbacks. First, the per-flow reservations in each node require excessive storage, coupled with excessive signaling over the end-to-end path in order to periodically refresh them [9], [17], [18]. Second, the refresh frequency must be precisely and carefully tuned for the scheme to work effectively. Otherwise, the adaptation process cannot follow the variations in path quality (too low frequency) or the incurred signaling overhead becomes too high (too high frequency) [9], [17].

III. A Differentiated Services QoS Scheme

A. Scheme Framework

The scheme that we present below is designed to address all the previously described aspects of a MANET. It has a simple, yet effective, implementation, based on a cross-layer approach that splits the QoS functionality between edge and intermediate nodes in the transmission path (Figure 1). The scheme's goal is to provide differentiated services at the intermediate nodes without imposing significant overhead either to them or to the network. Therefore, it is designed so that nodes do *not* store any per-flow state and do *not* perform per-flow queuing. In addition, admission control is not required at the initiation of the flow or throughout its lifetime. The scheme is applicable to adaptive flows that can modify their transmission rate between a minimum and a maximum value depending on the available resources. For example, a video or an audio source could adapt their transmission rate by modifying the compression ratio, so as to avoid excessive losses due to congestion. Besides adaptive flows, the scheme is designed to be TCP-Friendly, since it transparently accommodates traditional unaware Web/TCP and CBR/UDP traffic.

The service differentiation in our scheme consists of altering the way packets are dropped at intermediate nodes when congestion occurs: instead of simply dropping packets from

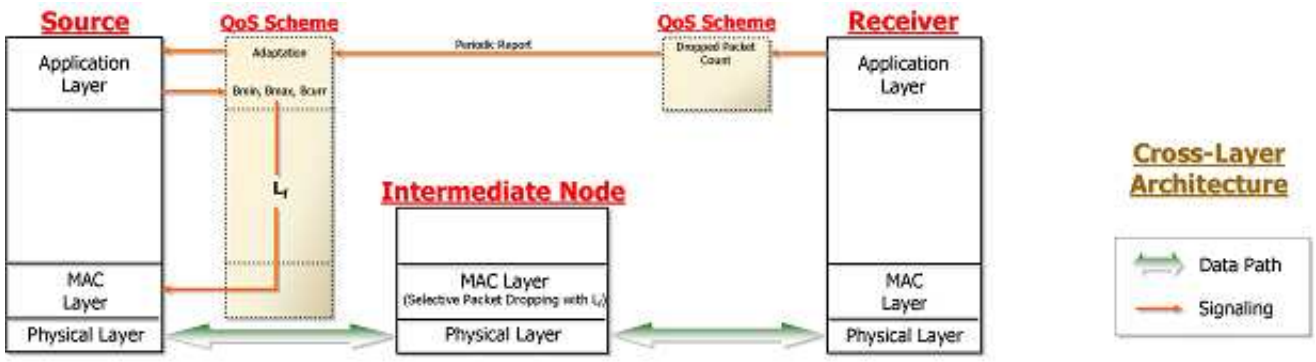

Fig. 1. Cross-Layer Architecture of the proposed QoS Scheme

the tail of the queue when it becomes full, our scheme defines an algorithm to select the best candidate packet for dropping from all packets currently in the queue. The selected packet belongs to the flow that is the best candidate for adaptation. The receiving node in the proposed scheme collects information about dropped packets and uses it as hints informing the appropriate source when it is time to adapt.

Specifically, each packet carries an identifier that is calculated at the source based only on local information. This value reflects the minimum and maximum resources that this flow can operate with, as well as the percentage of resources that the flow currently uses in excess to the minimum required. When this value is high, the likelihood that this flow enjoys resources close to its maximum requirement is also high. Thus, if the packet carries the highest value in a queue, the flow that it belongs to is most likely the best candidate for adaptation during congestion. The formula used to produce this identifier for each flow is presented and analyzed in a subsequent paragraph.

When an intermediate node experiences congestion, it must decide which packet to drop from the queue. At this point it compares the identifiers of all the packets in the queue and selects the one with the higher value as the victim. In case of a tie, the most recently arrived packet is selected. If the congestion is not resolved, the packet with the second higher identifier is selected, and so on. This loss eventually becomes apparent at the destination, which, in turn, notifies the source via a periodically sent quality report. The source then identifies a potential bottleneck along the end-to-end path and adapts the flow to a lower quality and transmission rate. The adaptation mechanism is triggered with a certain hysteresis, in order for short-term variations to be gracefully absorbed. This is important, in order for the scheme to differentiate between congestion losses and short-term link quality variation losses, since it should react only to the first type of them.

When the congestion is resolved, or when additional resources become available, the sources must attempt to adapt to higher levels of quality. This is triggered independently at the source of each flow after it receives a number of consecutive quality reports indicating zero losses. The actual number of successful reports needed to trigger this upward adaptation depends on the flow's current level of quality and a certain hysteresis defined by the application: the lower the current level of the flow's quality, the fastest the flow will attempt to grasp more resources; however, the more susceptible the perceptual quality of the flow is to variations, the higher the hysteresis will be. Again, the presence of the hysteresis factor is important, in order for the QoS scheme to differentiate between actual resource availability and short-term link quality variations.

In order to clarify the operation of our scheme, we now present the formula that produces the packet identifier L_f that is inserted in each packet of a flow f:

$$L_f = \alpha_{f,t} \cdot (k_1 \cdot \frac{B_{\text{curr},f} - B_{\min,f}}{B_{\max,f} - B_{\min,f}} + k_2 \cdot \frac{B_{\min,f}}{B_{\max,f}} + k_3 \cdot \frac{B_{\max,f}}{C_{\max}})$$

$B_{\min,f}$ and $B_{\max,f}$ correspond to the minimum and maximum bandwidth requested by the flow, respectively. $B_{\text{curr},f}$ is the bandwidth that the flow f requires in order to operate with its current level of quality. The parameter $C_{\max}$ is a global constant, common to all nodes, which corresponds to the maximum requested $B_{\max}$ by all existing flows. In other words:

$$C_{\max} = \max\{\text{for all} \quad f, B_{\max,f}\}$$

To simplify the implementation by avoiding signaling to determine $C_{\max}$, and without any loss of generality, we set this value to be equal to the raw bandwidth of the slowest wireless device in the particular MANET. This value can be easily communicated between devices during setup time, when a new wireless device enters the MANET. We discuss the k_i and $a_{f,t}$ factors below.

B. The Weighting Factors

The identifier formula consists of three parts, each with a relative weight k_1, k_2 and k_3, common to all the flows that participate in a particular MANET. These factors can be adjusted depending on the MANET, in order to better reflect its dynamic behavior, its resource availability and the type of flows that traverse it. The three parts contribute to the value of L_f in different ways. Recall that the larger the value of L_f, the higher the possibility that the flow is the best candidate for adaptation, and therefore the one whose

packets are dropped. Starting with the first part, the fraction reflects the percentage of resources that the flow is currently using in excess to the minimum resources needed, in order to operate with its base quality. If this percentage is high, it means that the flow most likely enjoys a level of quality higher than all the other flows traversing the same congested node. Therefore, this flow should release some resources first in order to relieve a potential congestion. The higher this value (and, consequently, the value of L_f), the larger the distance between the minimum and the current resource levels, hence the higher the probability that this flow will be penalized first.

The second part represents how flexible is the flow in adapting its transmission rate, while the third part indicates the relative fraction of the resources required by the flow to operate at peak quality. Their presence is needed in order to provide incentives against potentially malicious behavior from certain flows. Each part prevents one of two types of possible malicious behavior that may force the QoS scheme to malfunction. First, consider a flow that declares a $B_{\min}$ very close to its $B_{\max}$, even though it could operate at lower transmission rates. When it adapts its transmission closer to $B_{\min}$, the percentage of excessive resources used (first part of the identifier formula) will become very low, even though the flow has practically released no resources. This *virtual* adaptation allows the flow to keep operating at very high rates, while never again becoming a candidate for adaptation. In order to prohibit such malicious behavior, the second part of the identifier formula is added. When a flow declares a $B_{\min}$ close to its $B_{\max}$, the value of the second part of the formula approaches k_2. Thus, by selecting a proper value for k_2, the value of L_f will be high enough to prevent this form of *virtual* adaptation.

Second, consider a flow requesting an extremely large $B_{\max}$ without really needing it. Then, the first part of the formula will always be very small, even if the flow uses a lot of resources. This will also be the case for the second part of the formula, even for relatively high B_{min} values. As a result, the flow may effectively take over the congested link and force all other flows to adapt. In order to prevent this type of malicious behavior the third part of the identifier formula is added. For well behaved flows, this value will be negligible in comparison to the first two parts and, thus, its presence will not affect the functionality of the scheme. However, if a flow decides to cheat by arbitrarily increasing its $B_{\max}$, the third part of the formula will approach k_3 for it. By selecting an appropriate value for k_3, the identifier for this flow becomes high enough, in order to prohibit it from effectively dominating the congested link.

In conclusion, both the second and the third part of the formula are necessary for the integrity of the QoS scheme. They keep the flows honest by rewarding them for requesting reasonable values for $B_{\min}$ and $B_{\max}$ and by penalizing them for subverting the first part of the formula with artificially high values.

Besides adaptive flows, the proposed QoS scheme is designed to be TCP-Friendly, in order to transparently accommodate traditional unaware Web/TCP and CBR/UDP traffic. For Web/TCP applications, $B_{\min}$ is set to zero, while $B_{\max}$ is calculated based on the estimated RTT and the maximum allowed window. For CBR/UDP application, $B_{\min}$ is equal to $B_{\max}$ and the first part of the identifier's formula is omitted.

The selection of the parameters k_1, k_2 and k_3 is extremely important. Intuitively, the first part should be the dominating part of the formula, but the values of the other two parts should be significant enough in order to factor in the identifier's value when malicious behavior is exhibited. However, if they become too high, they may hinder the effectiveness of the QoS scheme. Thus, the decision about the actual values of the three parameters must be made according to the characteristics of each particular MANET.

As a point of reference, in future work we will assess several sets of parameters for different types of MANETs based on simulation results. The Appendix presents a first theoretical estimation of the operational parameters of the proposed QoS scheme. The estimated values will be the starting point for the simulation experiments.

C. The Aging Factor

The parameter $a_{f,t}$ ($0 < a_{f,t} \leq 1$) in the identifier's formula is an aging factor reflecting the duration of the flow up to time t. The rationale for its presence is to prevent newly initiated flows from forcing older flows to termination. Since there is no admission control in the proposed scheme, if at a certain moment a new flow is initiated over a congested link, there might not be enough resources for all of them to operate with their minimum level of quality. At this point, one or more flows must be selected to suspend or terminate their transmission. It is widely accepted that newly initiated flows should be the ones to be terminated, in favor of older flows that have been using the network for some time. This is guaranteed by the presence of the aging factor $a_{f,t}$ in the identifier's formula.

In order to clarify the importance and the role of $a_{f,t}$, consider a point where all existing flows operate with their $B_{\min}$ and a new flow is initiated also requiring $B_{\min}$ resources. The first part of the formula for all flows will be 0, while the other two parts will not reflect the relative age of the older flows compared to the new one. By adding the aging factor $a_{f,t}$, the identifier for the older flows will be smaller, forcing the newly initiated flow to terminate.

As long as a flow retains a certain level of quality, $a_{f,t}$ is periodically updated to smaller values, down to a minimum $a_{f,\min}$. The value of $a_{f,\min}$ is decided at the initiation of the flow and is selected so as to not interfere with the functionality of the QoS scheme. The exact formula for the current value of $a_{f,t}$ at a certain point in time t is:

$$a_{f,t} = \ max\{(a_{f,t-d} \cdot a_f), a_{f,\min}\}$$

where a_f ($0 < a_f < 1$) is the aging parameter of the flow f, and d is the duration between updates of the aging factor. This formula is used to recalculate $a_{f,t}$ only if a flow f has zero losses during the last time period d. Otherwise, the aging factor remains unchanged. It is important to notice that a change in the end-to-end path doesn't affect the aging factor. Thus, an old flow entering a new path is not mistakenly treated as a newly initiated flow. The Appendix presents a first theoretical

estimation of a value for the aging factor. This will be the basis for our simulation experiments, which will provide us with more accurate values for it.

D. Qualitative Evaluation

Since $a_{f,t}$, the sum of k_1, k_2 and k_3 and the three fractions in the formula are all less than 1, it is easily derived that $0 \leq L_f \leq 1$. L_f is re-calculated only when a flow adapts to a new level of quality, when the aging factor changes or (rarely) when $C_{\max}$ changes. The intermediate nodes simply compare the identifiers of the existing packets, in order to decide which to drop, without maintaining any state on the flows traversing them. Summarizing the characteristics of the proposed QoS scheme, we observe the following:

1) The signaling overhead is minimal.
2) Per-flow processing and storage requirements at each node are negligible.
3) The scheme is very scalable.
4) Admission control procedures or bandwidth estimates are not required.
5) Routing changes and mobility are transparent.
6) Malicious flow behavior is prevented.

In conclusion, the scheme follows all the guidelines given at the beginning of this paper for the design of an effective QoS scheme for MANETs.

We have identified two potential issues that might affect the effectiveness of our scheme. The first is the frequency and reliability with which quality reports are sent from the destination to the source. If the congested link varies too often, then the frequency of the reports should be high, in order for the scheme to "capture" in time the behavior of the link. The hysteresis factor at this point should be carefully tuned, in order to avoid triggering the adaptation process too frequently, since this would have a negative effect to the perceived, by the user, quality of the flow. This frequency, as well as the weighting and aging factors, will be assessed via simulations in our future work.

The second potential issue with our proposed scheme is the truthfulness of the participating wireless nodes. Although the scheme itself prevents individual flows from behaving maliciously, it is not able to prevent nodes from using hacked versions of the QoS scheme. With such an alteration, a node may allow flows to fake their L_f and, subsequently, gain an advantage over the competition. We currently expect lawful cooperation from all participating nodes, while we investigate ways to alleviate the problem in future versions of the proposed QoS scheme.

IV. Conclusions

We presented a simple, yet effective, QoS scheme for MANETs, which was designed in order to address the specific characteristics of such networks. The approach is based on differentiated services at intermediate (forwarding) nodes by adding intelligence in the packet dropping process during congestion. The framework is based on a single value, an identifier for each packet, which represents the likelihood that the associated flow is the best candidate for adaptation at a certain node during congestion. The design is light-weight in storage and processing requirements and operates without an admission control algorithm. It is also extremely scalable, since its computational complexity is not related with the size and the layout of the MANET. Finally, and most importantly, the scheme provides the necessary incentives for the flows to truthfully declare their characteristics by prohibiting the malicious behavior of non-cooperative flows.

Our plans for future work include the implementation of the proposed QoS scheme in a simulation environment using the Network Simulator ns2 [19], [20]. Three types of experiments will be conducted. One set of experiments will evaluate several suggested values for the parameters of the scheme in different network topologies. A second set of experiments will evaluate the effectiveness of the proposed approach in providing differentiated services. Finally, the last set of experiments will assess how well the proposed QoS scheme prevents the malicious behavior of non-cooperative flows.

Acknowledgment

This research is supported by the project "Mobile Services" (EP-1221-06), funded by the research program "Pythagoras-Support for Research Groups at the AUEB," which is co-financed by the Ministry of Education of Greece and the European Union, through the program "EPEAEK II."

References

[1] K. Nahrstedt, S.H. Shah, and K. Chen, *Cross-Layer Architectures for Bandwidth Management in Wireless Networks*, in Resource Management in Wireless Networking, Kluwer Academic Publishers, 2004.

[2] I. Akyildiz, Y. Altunbasak, F. Fekri, and R. Sivakumar, *AdaptNet: An Adaptive Protocol Suite for the Next-Generation Wireless Internet*, IEEE Communications Magazine, vol. 42, no. 3, pp. 128-136, Mar. 2004.

[3] N. Nikaein, C. Bonnet, Y. Moret, and I.A. Rai, *2LQoS - Two-Layered Quality-of-Service Scheme for Routing in Mobile Ad Hoc Networks*, Proc. 6th World Multiconference on Systemics, Cybernetics and Informatics, 2002.

[4] P.M. Ruiz and E. Garcia, *Adaptive Multimedia Applications to Improve User-Perceived QoS in Multihop Wireless Ad-Hoc Networks*, Proc. PIRMC 2002, vol. 3, pp. 1467-1471, Sept. 2002.

[5] M. Gerharz, C. de Waal, M. Frank, and P. James, *A Practical View on Quality-of-Service Support in Wireless Ad Hoc Networks*, Proc. 3rd Workshop on Applications and Services in Wireless Networks, July 2003.

[6] S. Gulder and M. Deziel, *Quality of Service Mechanism for MANET using Linux*, Proc. INSC Symposium, NATO C3 Agency, Nov. 2003.

[7] V. Kanodia, C. Li, A. Sabharwal, B. Sadeghi, and E. Knightly, *Distributed Multi-Hop Scheduling and Medium Access with Delay and Throughput Constraints*, Proc. ACM MobiCom 2001, July 2001.

[8] K. Xu, K. Tang, R. Bagrodia, M. Gerla, and M. Bereschinsky, *Adaptive Bandwidth Management and QoS Provisioning in Large Scale Ad Hoc Networks*, Proc. MILCOM, 2003.

[9] M. Mirhakkak, N. Shult, and D. Thomson, *Dynamic Bandwidth management and adaptive applications for a variable bandwidth wireless environment*, IEEE JSAC, vol. 19, no. 10, Oct. 2001.

[10] Y. Tang and R. Kravets, *Distributed QoS guarantees for realtime traffic in ad hoc networks*, Proc. IEEE SECON, Oct. 2004.

[11] G.-S. Anh, A.T. Campbell, A. Veres, and L.-H. Sun, *Supporting service differentiation for real-time and best-effort traffic in stateless wireless ad hoc networks (SWAN)*, IEEE Transactions on Mobile Computing, vol. 1, no. 3, pp. 192-207, Sept. 2002.

[12] H. Xiao, W.K.G. Seah, A. Lo, and K.C. Chua, *A flexible quality of service scheme for mobile ad-hoc networks*, Proc. IEEE Vehicular Technology Conference, pp. 445-449, May 2000.

[13] Y. Yuan, D. Gu, W. Arbaugh, and J. Zhang, *Achieving Packet-Level Quality of Service Through Scheduling in Multirate WLANs*, Proc. IEEE Vehicular Technology Conference, 2004.
[14] S. Mangold, S. Choi, P. May, O. Klein, G. Hiertz, and L. Stibor, *IEEE 802.11e Wireless LAN for Quality of Service*, Proc. European Wireless, 2002.
[15] H. Zhu, M. Li, I. Chlamtac, and B. Prabhakaran, *A Survey of Quality of Service in IEEE 802.11 Networks*, IEEE Wireless Communications, Aug. 2004.
[16] C.R. Lin and M. Gerla, *MACA/PR: an asynchronous multimedia multi-hop wireless network*, Proc. IEEE INFOCOM, 1997.
[17] S. Lee, G. Ahn, X. Zhang, and A. Campbell, *INSIGNIA: An IP-based quality of service framework for mobile ad hoc networks*, Journal of Parallel and Distributed Computing (JPDC), vol. 60, no. 4, Apr. 2000.
[18] L. Zhang, S. Deering, and D. Estrin, *RSVP: A new resource reservation protocol*, IEEE Network, 1993.
[19] *The Network Simulator - ns2*, http://www.isi.edu/nsnam/ns/
[20] CMU Monarch Project, *Wireless and Mobility Extensions to ns-2*, http://monarch.cs.cmu.edu:80/cmu-ns.html

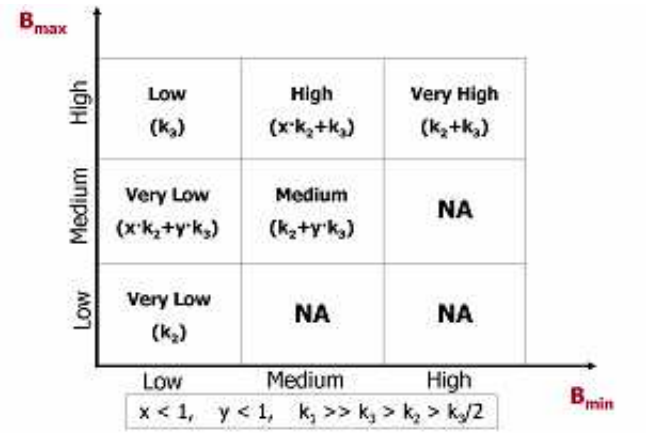

Fig. 2. Impact of the k_i parameters on L_f for various $B_{\min}$ and $B_{\max}$

APPENDIX

For implementation purposes, it is important that the value of L_f is bounded and, in particular, we want:

$$0 \leq L_f \leq 1 \tag{1}$$

We already know that $a_{f,t} \leq 1$ and that the fraction in each of the three parts of the formula is also less than 1. Thus, for (1) to hold we only need to make sure that:

$$0 < k_1 + k_2 + k_3 \leq 1 \tag{2}$$

The next step is to clarify the relationship between the k_i parameters. We start with k_2 and k_3. Consider a simple scenario where a wireless node represents a bottleneck in the MANET. Assume that all the flows traversing it currently transmit with their base quality, thus the first part in their formula is zero. Also assume for simplicity that all flows started around the same time, so the aging factor doesn't play a significant role in this case. Now consider a moment when the link quality of the node deteriorates in a degree that the node becomes congested and that a victim for adaptation must be selected. At this point, the way that the QoS scheme *expects* the k_2 and k_3 parameters to affect the identifier L_f of each flow is presented in Figure 2.

Analyzing the results of the graph, we composed the following relationship between k_2 and k_3:

$$k_3/2 < k_2 < k_3 \tag{3}$$

Let's now alter the previous scenario so that one of the flows transmits with a quality higher that the rest of the flows. In this case, the QoS scheme *expects* this flow to be the best candidate for adaptation when congestion occurs. Remember that the first part of the formula for this flow is not zero any more, which means that the k_1 parameter should be the dominating factor in the comparison of different identifiers. As a result we conclude that:

$$k_2, k_3 << k_1 \tag{4}$$

Putting (3) and (4) together we end up with the following relationship between all the k_i parameters:

$$k_3/2 < k_2 < k_3 << k_1 \tag{5}$$

Using (2) and (5) we selected a set of values for all k_i parameters, which we intent to use as a starting point in our simulation experiments:

$$k_1 = 0.8, k_2 = 0.08, k_3 = 0.12 \tag{6}$$

We also selected the following initial values for the two parameters, $a_{f,t}$ and $a_{f,\min}$, of the aging factor:

$$a_{f,t} = 0.985, \quad a_{f,\min} = 0.5 \tag{7}$$

The simulation experiments with ns2 will assist us in further understanding the relationship between all the parameters of the proposed QoS scheme and in evaluating the effect that they have on different types and sizes of MANETs.