Fair Sharing of Bandwidth in VANETs

Marc Torrent-Moreno
Institute of Telematics
University of Karlsruhe
Germany
torrent
@tm.uni-karlsruhe.de

Paolo Santi
Istituto di Informatica e
Telematica del CNR
Pisa, Italy
paolo.santi
@iit.cnr.it

Hannes Hartenstein
Institute of Telematics
University of Karlsruhe
Germany
hartenstein
@rz.uni-karlsruhe.de

ABSTRACT

We address the challenge of how to share the limited wireless channel capacity for the exchange of safety-related information in a fully deployed vehicular ad hoc network (VANET). In particular, we study the situation that arises when the number of nodes sending periodic safety messages is too high in a specific area. In order to achieve a good performance of safety-related protocols, we propose to limit the load sent to the channel using a strict fairness criterion among the nodes. A formal definition of this problem is presented in terms of a max-min optimization problem with an extra condition on per-node maximality. Furthermore, we propose FPAV, a power control algorithm which finds the optimum transmission range of every node, and formally prove its validity under idealistic conditions. Simulations are performed to visualize the result of FPAV in a couple of road situations. Finally, we discuss the issues that must be taken into account when implementing FPAV.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]: Wireless communication

General Terms

Algorithms, design

Keywords

Ad hoc networks, fairness, power control, vehicular safety

1. INTRODUCTION

We have witnessed a wide spread of mobile technologies during the last decade. Their rapid evolution and cost reduction have made them to be considered as a suitable solution for a wide spectrum of applications. Recently, the promises of wireless communications to support vehicular safety applications have led to several research projects around the world: the Vehicle Safety Communications Consortium [1] developing the DSRC technology [2] (USA), the Internet ITS Consortium [3] (Japan), the PReVENT project [4] (Europe) or the 'Network on Wheels' project (Germany) [5], to name a few. All these projects have as a main goal to improve safety in vehicular environments by the use of wireless communications, but also consider transport efficiency, comfort and environment. The results achieved so far by the various projects together with the efforts of car manufacturers and standardization bodies, e.g., [6], invite to optimism. Although many problems are not yet solved, the general feeling is that vehicles could benefit from spontaneous wireless communications in a near future, making VANETs (Vehicular Ad-Hoc Networks) a reality.

In this paper we analyze a problem arising in VANETs with high vehicle densities with respect to the channel reserved for the exchange of safety-related information. In this context, it is likely that the limited capacity of the so called control channel is not enough to support the safety-related load generated by a large number of vehicles unless the offered load is carefully controlled. More specifically, in this paper we consider a fairness problem that arises in situations in which vehicles send periodic beacon messages to inform other vehicles in the surrounding of their current state (velocity, direction, and so on) in order to improve safety conditions. The motivations for studying this problem are thoroughly discussed in Section 2. After presenting our fairness problem and formally defining it in terms of a max-min optimization problem with an extra condition on per-node maximality, we propose an approach to solve this problem based on power control, and we provide an optimal algorithm, called FPAV (Fair Power Adjustment for Vehicular environments) – see Section 3. We then verify the validity of our approach by simulation. The results show FPAV's fairness and effectiveness in confining the network load generated by the beaconing activity below a certain desired threshold (Section 4). In Section 5 we discuss the issues that must be dealt with when bringing FPAV into a real scenario. Section 6 presents some related work, and Section 7 concludes the paper.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
VANET'05, September 2, 2005, Cologne, Germany.
Copyright 2005 ACM 1-59593-141-4/05/0009 ...$5.00.

2. MOTIVATION FOR FAIR POWER ADJUSTMENT

In a VANET every vehicle will be able to send and receive data packets into/from a shared medium. One of the decisions already taken in the USA (FCC ruling report [7]) is that the frequency spectrum will be divided in 7 different channels, 1 control channel and 6 service channels. The control channel will be utilized for the exchange of safety messages, and will contain few service messages, e.g., announcing services, if feasible. Therefore, all vehicles will have to monitor the control channel often enough to receive all safety related information so that the safety applications achieve their goal.

In this paper, we are concerned with the utilization of the control channel. In particular, we assume that two types of safety messages circulate in the control channel and classify them depending on how they are generated: *event driven* and *periodic*. The first ones are the result of the detection of an unsafe situation, e.g., a car crash, the proximity of vehicles at high speed, etc. Periodic messages instead can be seen as preventive messages in terms of safety, and their information can also be used by other (non-safety) applications (e.g., traffic monitoring) or protocols (e.g., routing). Periodic message exchange (also called *beaconing* in the following) is needed to make vehicles aware of their environment. Thus, they will be able to avoid emergency or unsafe situations even before they appear.

We assume, therefore, that beacon messages essentially contain the state of the sending vehicle, i.e., position, direction, speed, etc., and also aggregated data regarding the state of their neighbors. It is reasonable to assume that these periodic messages will be sent in a broadcast fashion since the messages' content can be beneficial for all vehicles around. Finally, it is our strong belief that the amount of load resulting from beaconing should be limited, i.e., the medium should not be working permanently near the maximum load limit. This is because it is desirable to leave some bandwidth available to handle unexpected emergency situations with a reasonable reliability. Emergency packets should be able to access the control channel with short delay, and they should have low probability of collision even when targeting large areas, i.e., when being transmitted with high power.

In the context described above, a fundamental design decision is to choose a strategy for sending the periodic safety messages. We assume that some communication parameters (e.g., transmission range, packet generation rate) can be appropriately set depending on the situation and/or the vehicles' state. An example of such strategy could be to increase the transmission power of beacons depending on the vehicle's speed. Therefore, we expect different transmission power requirements among the nodes.

When VANETs are fully deployed, they might encounter situations where the technology limitations become a challenge. Scenarios with high vehicle densities can be easily found in real life, e.g., highways at the entrance of big cities or a traffic jam due to a temporal working area. Due to a large number of vehicles sharing the medium, it is not clear whether the channel capacity is sufficient in these scenarios to support the data load generated by beaconing while at the same time leaving enough available bandwidth for event-driven safety messages.

Now, let us consider the following assumptions: *a)* the lower layer technology used in VANETs will be a variant of IEEE 802.11a technology [2] and *b)* there will be only one control channel, 10MHz wide [7], for the exchange of both types of safety messages. Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA), i.e., 802.11 Link Layer protocol, is a totally asynchronous approach. Although it is widely used in commercial applications, it

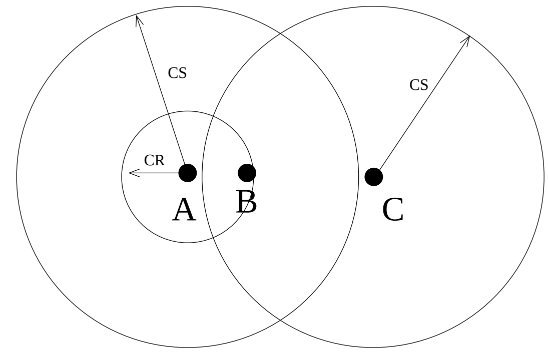

Figure 1: Hidden Terminal Problem: In a CSMA/CA scenario, node B is inside the Communication Range of A and node C is placed outside of the Carrier Sense range (CS) of A, i.e., C can not sense ongoing transmissions from A. In that case, the hidden terminal problem occurs when B can not receive a message from A because it collides with one from C.

is known for not being able to manage the medium resources very efficiently, especially in case of broadcast messages. Then, a 10MHz channel can offer half the data-rates of 802.11a, and lower rates are preferred because of their robustness to noise and interference. With such configuration, we conducted a simulation work [8] where broadcast reception rates were evaluated. For instance, we observed that in a scenario with a high node's density and an offered load to the channel (2.56 Mbps) lower than half of the channel's ideal capacity (6Mbps), the probability that a node receives a broadcast message at the edge of the intended communication range[1] drops below 40%. Basically, the main reason for such low reception rates is the well-known hidden terminal problem (see Figure 1)[2]. Hidden nodes have a severe impact on these scenarios, since no channel reservation process is performed in the targeted area when sending a broadcast packet.

Therefore, we are concerned with situations where the overall load generated by beaconing is too high, i.e., packet collisions are too high, and thus the information obtained by a node cannot be updated frequently enough to prevent possible emergency situations in a vehicle's surrounding. To avoid such situations, we need to design a congestion control mechanism which is able to keep the periodic messages' load under the aforementioned maximum load in all points of the network. This threshold, called *MaxBeaconingLoad* (*MBL*) in the following, represents a limit where safety protocols can achieve a reasonable performance. Since *MBL* represents a network load threshold it is measured in Mbps, however, if we assume a fixed packet generation rate, it might be equivalently measured as maximum number of cars whose

[1]The intended Communication, or Transmission, Range is the distance up to where a transmission would be received successfully in ideal conditions and in the absence of any interference.

[2]The Carrier Sense range, in ideal conditions, is the distance to which a node's transmissions can be sensed, or in other words, the distance to which a node can interfere with other transmissions.

CS range cover a specific point in the network, when appropriate.

We propose to adjust the transmission range of all nodes using power control in order to keep the load in the medium below a certain threshold. We are aware that before decreasing the transmission power of safety messages other steps should be taken, for example, implementing an admission control mechanism to drop all non-safety related packets before being sent to the control channel, or minimizing the packet generation rate. Although these strategies can also be utilized as a first step, there will be situations where decreasing the transmission range of certain nodes is necessary. By adjusting the transmission range once the packet generation rate is fixed to the minimum requirement of the safety applications, the load on the channel can be reduced while at the same time high-accuracy information of neighboring vehicles is still available.

Although power control has been a deeply studied subject in the mobile networks field already (see related work in Section 6), vehicular environments present new challenges. As argued above, safety application designers may decide that the beacon's transmission power of a node depends on its state. Since these different power settings should be respected also among neighboring nodes, we introduce the concept of **fair power control** in VANETs: all vehicles in a certain area must restrict their beacons' (potentially different) transmission power *by the same ratio* to satisfy *MaxBeaconingLoad*. Basically, in a high dense cloud of vehicles, our proposal is to decrease the transmission ranges of all nodes by the same ratio until there is no spatial area where the load overcomes the pre-fixed maximum *MBL*. We present in the following section a detailed and formal definition.

3. THE FPAV ALGORITHM

3.1 The reference application scenario

We are considering a scenario in which a set of vehicles (also called *cars*, *users*, or *nodes*, in the following) is moving along a road. Periodically, users send beacon messages to inform the nodes in their vicinity of their current position, direction, velocity, etc. For clarity reasons in the problem formulation, we assume that the beaconing frequency is the same for all the nodes in the network. However, the power used to transmit beacons can be adjusted, so that the overall network bandwidth used for beaconing can be kept under control.

In principle, a node will send its beacon at maximum power, as this in general guarantees that more nodes will receive the beacon, resulting in increased safety conditions. On the other hand, the higher the power used to send beacons, the higher is the network load generated by the beacon exchange activity.

We recall that in the envisioned application scenario, the above described beaconing activity is assigned with a *limited portion* of the available network bandwidth *MBL*, the remaining bandwidth being available for event-driven safety messages. Thus, the 'node optimal strategy' of sending the beacon at maximum power in general conflicts with the network-wide task of keeping the network load offered by beaconing below a certain threshold. As a consequence of this, we need a strategy for setting the node transmit power levels such that the beaconing network load does not exceed the threshold, and the beaconing transmit power levels are maximized.

3.2 The BMMTxP problem

Assume a set of nodes $N = \{u_1, \ldots, u_n\}$ is moving along a road. To simplify the problem statement, we assume that the road is modeled as a line[3] of unit length, i.e., $R = [0, 1]$, and that nodes can be modeled as points in $[0, 1]$. Given a node $u_i \in N$, $x(i, t)$ denotes the position of u_i in R at time t. To simplify the notation, in the following we drop the argument t, focusing our attention on a snapshot of the system at a certain time instant t. Mobility is later addressed in Section 5.

Each of the network nodes sends a beacon with a predefined beaconing frequency F, using a certain transmit power $p \in [0, P_{max}]$, where P_{max} is the maximum transmit power. In order to simplify the presentation, we assume that all the nodes have the same maximum transmit power level. We remark that this assumption is made only to simplify the notation, and that the framework described in this paper can be applied also when the nodes have different maximum transmit power levels.

DEFINITION 1. *Power Assignment:*
Given a set of nodes $N = \{u_1, \ldots, u_n\}$, a power assignment PA is a function that assigns to every network node u_i, with $i = 1, \ldots, n$, a ratio $PA(i) \in [0, 1]$. The power used by node u_i to send the beacon is $PA(i) \cdot P_{max}$.

DEFINITION 2. *Interference Range:*
Given a power assignment PA and any node $u_i \in N$, the interference range of u_i under PA, denoted $IR(i, PA)$ is defined as the intersection between the CS range of node u_i at power $PA(i) \cdot P_{max}$ and the deployment region R.

The above definition of interference deserves some explanation. In general, assuming that the CS range can be modeled as a 1/0 situation (either a transmission at a certain power interferes with a node, or it does not interfere at all) is a simplification of what occurs in practice, where the wireless channel conditions (which have a strong influence on the quality of the received signal) fluctuate over time. It is not difficult to extend our definition of interference to account for variable channel conditions: essentially, it is sufficient to associate a certain probability density function over [0,1] to each pair $(u_i, PA(i))$. However, in order to simplify the presentation of our framework, we assume that the notion of interference range is deterministic.

Besides the 0/1 interference assumption described above our notion of interference range is very general, as we do not assume that the CS range is regular – e.g., a segment centered at $x(i)$ – nor that it is contiguous – due to the presence of obstacles, there might exist 'holes' in the interference region. The only other assumption which is needed for the correctness of the proposed framework is a monotonic property, namely that the interference range of node u_i at power $(PA(i) + \epsilon) \cdot P_{max}$ contains the interference range of node i

[3]Modeling the road as a line is a reasonable simplification in our case since we assume the communication ranges of the nodes to be much larger than the width of the road.

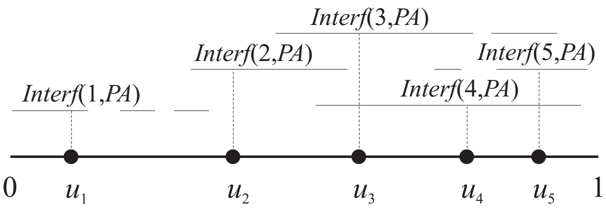

Figure 2: Network load based on interference: the maximum load is experienced in those subregions of $R = [0,1]$ where the number of intersecting interference ranges is maximal. In the example, we have $BL(PA) = 3$.

at power $PA(i) \cdot P_{max}$, for every $\epsilon > 0$. We remark that this assumption is very reasonable in a realistic setting.

Given a power assignment PA, the network load generated by the beaconing activity under PA is defined as follows:

DEFINITION 3. *Beaconing Load under PA:*
Given a set of nodes N and a power assignment PA for the nodes in N, the beaconing network load under PA is defined as

$$BL(PA) = \max_{x \in [0,1]} Interference(x, PA) \ ,$$

where $Interference(x, PA)$ is the number of nodes which have point x in their CS range under PA. Formally,

$$Interference(x, PA) = |\{u_i \in N : x \in IR(i, PA)\}| \ .$$

An example clarifying our notion of network load based on interference is reported in Figure 2. The intuition is the following: since the beaconing frequency is pre-determined, the network load depends on the transmit power levels used for beaconing – the higher these levels, the higher the network load[4]. Assuming that nodes are not allowed to transmit while they *sense* some message in the channel, the maximum load is experienced in those subregions of R where the number of intersecting interference ranges is maximal.

We are now ready to define the beaconing with max-min transmit power problem addressed in this paper:

DEFINITION 4. *Beaconing Max-Min Tx Power Problem (BMMTxP):*
Given a set of nodes $N = \{u_1, \dots, u_n\}$ in $R = [0,1]$, determine a power assignment $\overline{PA}$ such that the minimum of the transmit powers used by nodes for beaconing is maximized, and the network load remains below the beaconing threshold MBL. Formally,

$$\begin{cases} \max_{PA \in \mathbf{PA}} \left(\min_{u_i \in N} PA(i)\right) \\ \text{subject to} \\ \quad BL(PA) \leq MBL \end{cases}$$

where **PA** *is the set of all possible power assignments.*

Informally speaking, we are interested in finding the power assignment such that the minimal 'quality of service' guaranteed to the network nodes is maximized, i.e., is fair to all nodes, while not exceeding the portion of network bandwidth assigned to the beaconing activity. Notice that in our problem formulation we are assuming that the portion of bandwidth assigned for beaconing can be expressed in terms of the maximal number of overlapping nodes' interference ranges in a single point. This assumption is reasonable under our working hypothesis of fixed beaconing frequency.

[4]Here, we use the assumption of monotonic interference range.

Observe that in general there exist several power assignments that can be regarded as optimal solutions to BMMTxP. For instance, assume a certain power assignment $\overline{PA}$ is optimal for BMMTxP, and assume there exists a node $u_i \in N$ such that the power assignment $\overline{PA}(i,\epsilon)$ obtained from $\overline{PA}$ by increasing u_i's transmit power to $(PA(i) + \epsilon) \cdot P_{max}$, for some $\epsilon > 0$, does not violate the condition on the network load. It is immediate to see that also $\overline{PA}(i,\epsilon)$ is an optimal solution to BMMTxP.

In general, we are interested in finding an optimal solution to BMMTxP which is *per-node maximal*, i.e., a power assignment $\overline{PA}_M$ such that increasing the transmit power of any single network node results in exceeding the assigned network bandwidth.

DEFINITION 5. *Per-Node Maximal Power Assignment:*
A power assignment $\overline{PA}_M$ for node set $N = \{u_1, \dots, u_n\}$ is per-node maximal if and only if:

i) it is an optimal solution to BMMTxP; and

ii) for each $u_i \in N$, and for any $\epsilon > 0$, we have that $BL(\overline{PA}_M(i,\epsilon)) > MBL$, where $PA(i,\epsilon)$ denotes a power assignment where node u_i increases its transmit power by $\epsilon \cdot P_{max}$.

Our interest in finding a per-node maximal power assignment is motivated by the fact that, as long as the condition on the network load is not impaired and the minimum of the nodes' transmit power levels is maximized, the higher a node transmit power the better the safety conditions of the vehicle.

3.3 An optimal algorithm for BMMTxP

In this section we present a centralized algorithm for solving BMMTxP and computing a per-node maximal power assignment. The algorithm, called FPAV (Fair Power Adjustment for Vehicular environments), is composed of two stages: stage 1 computes an optimal solution to BMMTxP, and stage 2 augments this solution into a per-node maximal power assignment.

Stage 1 of FPAV, which is summarized in Figure 3, is very simple: every node starts with the minimum transmit power, and all the nodes increase their transmit power simultaneously of the same amount $\epsilon \cdot P_{max}$ as long as the condition on the beaconing network load (*MBL*) is satisfied. Note the strict fairness achieved at the end of this stage where all nodes increase their power the same number of steps k and end up with a power of $p = (k\epsilon) \cdot P_{max}$.

The next theorem shows that this simple strategy results in producing an optimal solution to BMMTxP. Technically, the power assignment computed by stage 1 of FPAV is an $\epsilon \cdot P_{max}$-approximation of the optimal solution to BMMTxP. Since the step size ϵ is an arbitrarily small constant, the solution computed by BMMTxP can be regarded as optimal for all practical purposes.

```
ALGORITHM FPAV, STAGE 1:
INPUT:    a set of nodes N = {u_1, ..., u_n} in [0, 1]
OUTPUT:   a power assignment PA which is an
          (ε · P_max-approximation of an) optimal solu-
          tion to BMMTxP

          ∀u_i ∈ N, set PA(i) = 0
          while (BL(PA) ≤ MBL) do
            ∀u_i ∈ N, PA(i) = PA(i) + ε
          end while
          ∀u_i ∈ N, PA(i) = PA(i) − ε
```

Figure 3: Stage 1 of the FPAV algorithm.

THEOREM 1. *Stage 1 of FPAV computes an $\epsilon \cdot P_{max}$-approximation of the optimal solution to BMMTxP for any constant $\epsilon > 0$.*

PROOF. First, we observe that the power assignment PA computed by the stage 1 of FPAV, with a power level $p = (k\epsilon) \cdot P_{max}$, is the minimal assignment among all the power assignments with minimum power level p, since in PA *all* the nodes have the same power level p. Thus, if a power assignment PA' with minimum power level p does not violate the condition on the network load, then also PA does not violate the condition on the network load because the nodes' interference ranges under PA' are at least as large as under PA (this is true because of the assumption of monotonic interference range).
Let $\overline{p}$ be the minimum of the node transmit powers in an optimal solution to BMMTxP, and assume $(k\epsilon) \cdot P_{max} < \overline{p} \leq ((k+1)\epsilon) \cdot P_{max}$ for some $k \geq 0$. The following cases can occur:

(*i*) $\overline{p} = ((k+1)\epsilon) \cdot P_{max}$. In this case, given the observation above it follows immediately that the power assignment computed by FPAV-stage 1 is optimal;

(*ii*) $(k\epsilon) \cdot P_{max} < \overline{p} < ((k+1)\epsilon) \cdot P_{max}$. In this case, given the observation above and the assumption of monotonic interference range we can conclude that the power assignment PA computed by FPAV-stage 1 is a feasible solution to $BMMTxP$, which is at most $\epsilon \cdot P_{max}$ away from the optimal solution.

This concludes the proof of the theorem. □

Observe that we had to introduce the constant ϵ in our algorithm to discretize the process of increasing the nodes' transmit power. The smaller ϵ, the more accurate the solution computed by FPAV, the longer the running time of the algorithm. On the other hand, in a practical setting we expect that nodes can set the transmit power only to a limited number of different levels, and discretizing the transmit power increase process is not an issue. It is immediate to see that, under the assumption that all the nodes use the same power levels $\{p_1, \ldots, p_h\}$, stage 1 of FPAV computes an optimal solution to BMMTxP (subject to the constraint that the possible power levels for the nodes are $\{p_1, \ldots, p_h\}$).

Once BMMTxP is satisfied, let us now consider two approaches for the stage 2 of FPAV. The first approach, summarized in Figure 4, is a straightforward strategy to achieve

```
ALGORITHM FPAV, STAGE 2:
INPUT:    an optimal solution to BMMTxP, denoted PA
OUTPUT:   a power assignment PA which is a
          (ε · P_max-approximation of a) per-node maxi-
          mal power assignment

          for (i = 1 to n) do
            while (BL(PA) ≤ MBL) do
              PA(i) = PA(i) + ε
            end while
            PA(i) = PA(i) − ε
          end for
```

Figure 4: Stage 2 of the FPAV algorithm, alternative 1.

per-node maximal power assignment (also called *alternative 1* in the following): given an optimal solution to $BMMTxP$ (provided by stage 1 of the algorithm), each node is considered in turn, and its transmit power is increased by $\epsilon \cdot P_{max}$ steps as long as the condition on the beaconing network load is satisfied. Notice that although the minimum power has been maximized in stage 1 in a fair manner, some nodes could benefit from starting to increase earlier in stage 2 and reach a higher transmission power with respect to their close neighbors. To respect the fairness constraint, we propose a slightly more complex approach that requires a tighter synchronization and a complete global knowledge from all nodes in the network (also the ones far away) to achieve the per-node maximal power. We would like to remark though, that our main intention in this paper is to understand, formulate and solve the problem from a clear and conceptual point of view. Figure 5 summarizes a stage 2 approach with strict fairness constraints (also called *alternative 2* in the following): given an optimal solution to $BMMTxP$ (provided by stage 1 of the algorithm), each node sequentially increases its transmit power by $\epsilon \cdot P_{max}$ (only one step) if the condition $BL(PA) \leq MBL$ is not violated, repeating the sequence after all nodes have been given a chance and until no node is able to increase without violating the condition on the beaconing network load. Intuitively, this algorithm provides a higher fairness than the previous one. It ensures that any node will increase at maximum $\epsilon \cdot P_{max}$ its transmission power before letting the others try it.

The next theorem shows that both approaches of stage 2 of FPAV compute a per-node maximal (technically, an $\epsilon \cdot P_{max}$-approximation to a per-node maximal) power assignment.

THEOREM 2. *Assume PA is an optimal solution to BMMTxP; then, stage 2 of FPAV computes an $\epsilon \cdot P_{max}$-approximation to a per-node maximal power assignment for any constant $\epsilon > 0$.*

PROOF. The proof is along the same lines as the proof of Theorem 1. Let PA be an optimal solution to BMMTxP; this power assignment is augmented by FPAV-stage 2 considering each node u_i in turn (and in different sequences in alternative 2), which is assigned with a power level that is at most $\epsilon \cdot P_{max}$ away from the maximal power level for

```
ALGORITHM FPAV, STAGE 2:
INPUT:    an optimal solution to BMMTxP, denoted PA
OUTPUT:   a power assignment PA which is a
          (ε · P_max-approximation of a) per-node maximal power assignment following strict fairness constraints

∀u_i ∈ N, set ReachedTop(i) = false
while !(∀u_i ∈ N, ReachedTop(i) = true) do
  for (i = 1 to n) do
    PA(i) = PA(i) + ε
    if (BL(PA) > MBL) then
      PA(i) = PA(i) − ε
      ReachedTop(i) = true
    end if
  end for
end while
```

Figure 5: Stage 2 of the FPAV algorithm, alternative 2.

node u_i which does not violate the condition on the network load (MBL). It follows that the power assignment computed by FPAV-stage 2 at the end of this augmentation process is such that the power assigned to each node is at most $\epsilon \cdot P_{max}$ away from the per-node maximal transmit power level. We can then conclude that FPAV-stage 2 computes an $\epsilon \cdot P_{max}$-approximation to a per-node maximal power assignment. □

For reasons similar to the ones discussed above, the power assignment computed by FPAV-stage 2 can be regarded as per-node maximal for all practical purposes.

4. EXPERIMENTS

To illustrate the performance of FPAV and as a 'proof of concept' we have implemented the algorithm in C (both stage 2 approaches) and simulated it under two different traffic situations.

Since many decisions regarding the technology to be used in VANETs are not yet taken, we are forced to do additional assumptions or approximations. To define the load that every node periodically intends to offer to the control channel we should fix two parameters (the third parameter, transmit power, is managed by FPAV): packet generation rate and packet size. We assume that broadcasting a few packets per second is sufficient to maintain an accurate knowledge of position and state of all cars. On top of that, the number of transmitted packets may be increased due to retransmissions or to the use of mechanisms for improving transmission reliability. We take 10 packets per second as a reasonable rate for periodic messages. To come up with a packet size value we consider that every packet will contain several parameters composing the state of the sender. Also, the beacon could contain some aggregated and very valuable information about the sender's neighbors. If we finally consider some necessary security fields it does not look too pessimistic to take 250 Bytes as the packet size. These two parameters set the offered load of every node to 20Kbps inside their CS range. To facilitate interpretation of the results we fix the same intended communication range for all nodes, i.e., we assume that the radio coverage area is regular (no holes), and that the maximum CR is 250m. Similarly, we assume that the interference range of a node has a regular shape (no holes). Also, a maximum load accepted for the control channel should be defined. Taking into consideration all arguments from Section 2 we set the maximum load for beaconing to 50% of the channel capacity. For the physical layer we choose one of the lower 802.11a rates, 6Mbps, since this rate is more robust against interferences, i.e., nodes will have a shorter CS minimizing the effect of hidden terminals. Then, assuming a required SNR of 6dB and that idealistically the power decreases with the square of the distance we will have a CS of 500m approximately (at maximum transmit power). The final parameter we have to fix is the resolution of PA's increase in FPAV, i.e., the step size ϵ. We fix this parameter to 0.01, resulting in a CS increase of 5 meters for each increase of PA.

On the other hand, we also have to specify a vehicular traffic scenario to run our simulations. We choose a straight linear road with an average vehicle density of 20 vehicles per 100m modeling a congested traffic situation[5]. We recall that even higher vehicle densities can be easily found every day on real roads. Finally, we must consider that in most situations both directions of the traffic will share the same communication medium.

A summary of the configuration parameters of our simulations can be found in Table 1.

Packet generation rate	10 pckts/s
Packet size	250B
$\text{Load}_{vehicle}$	20Kbps
Data Rate	6Mbps
Maximum beaconing load	3Mbps
Communication range	250m
Carrier Sense range	500m
Step size ϵ	0.01
Vehicle density	20vehicles/100m

Table 1: Configuration parameters

Let us now define the metrics used to evaluate FPAV performance:

- **Offered Load:** Load, accumulated from all nodes, offered to the control channel [Mbps] in a specific point x on the road *before* applying FPAV. This metric shows the resulting load offered to the channel if no power control is performed (i.e., all vehicles have $PA(i) = 1$).
- **Adjusted Load:** Load, accumulated from all nodes, offered to the control channel [Mbps] in a specific point x after all nodes have adjusted their transmit power according to FPAV.
- **MaxBeaconingLoad (*MBL*):** Maximum load allowed for beaconing [Mbps].

[5]As in Section 3 we model the road as a line (1-D). Thus, our densities will be given in [vehicles/m] instead of [vehicles/m^2] adding up all vehicles circulating in the different lanes. For example, in a 4 lanes road, to have 20 vehicles/100m results in 1 car every 25m in each lane.

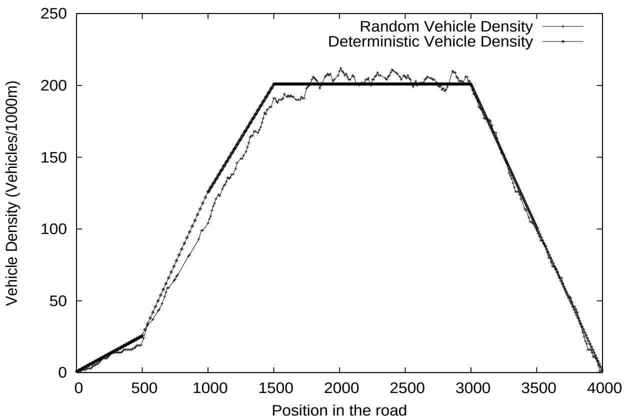

Figure 6: Traffic Cloud Densities. Vehicle densities at each point for both deterministic and random scenarios.

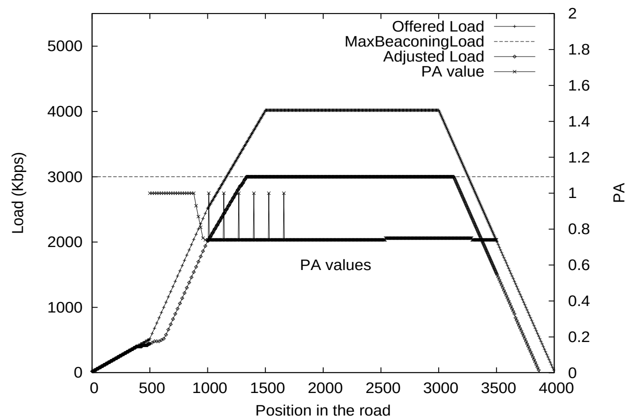

Figure 7: Deterministic Traffic Cloud. Load on the channel at every point of the deterministic scenario before and after applying FPAV with alternative 1 of stage 2.

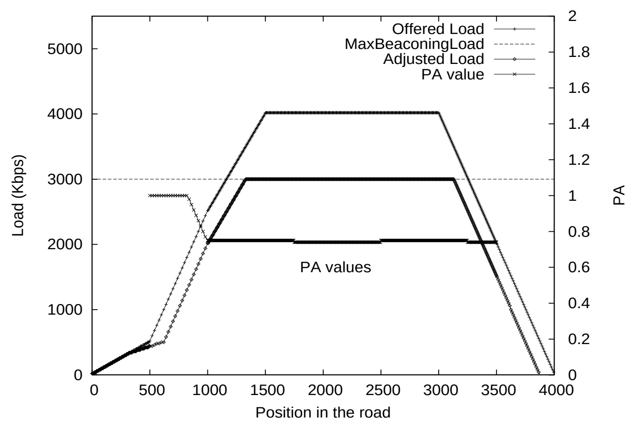

Figure 8: Deterministic Traffic Cloud. Load on the channel at every point of the deterministic scenario before and after applying FPAV with alternative 2 of stage 2.

- PA **value:** Value of $PA(i)$ after FPAV execution, expressed as a function of the node position x. Note that all vehicles placed on the same position x (if any) will have the same value of PA due to the same configuration values.
- **Vehicle Density:** Number of vehicles in a range of 1000m [vehicles/1000m] centered in a specific point x. 1000m is selected to give an estimation of the number of cars a node has inside its maximum CS range (when $PA = 1$).

We present the results obtained from applying FPAV to two different traffic scenarios. Both of them model the same piece of road (4km long) and have the same overall car density. However, in the first one cars are placed in a deterministic, equally-spaced fashion (*Deterministic Vehicle Density* Fig. 6). On the other hand, in the second scenario, vehicles are placed somehow randomly (*Random Vehicle Density* Fig. 6). In the following, we will refer them as deterministic or random scenario, respectively. In order to facilitate presentation and comprehension of results, both scenarios model a static situation.

The deterministic scenario models a cloud of cars in a straight road (starting at $x = 500m$) where the first 0.5 kilometer ('rear part' of the cloud) is populated with 1 car every 20 meters and the following 2.5 kilometers with 1 car every 5 meters ('front part' of the cloud). To populate the second scenario we make use of a discrete uniform random number generator. In particular, we place every 10m either 0 or 1 car along the first 0.5 km, and a number of cars ranging between 0 and 4 along the following 2.5 kms. Notice that in the plot reported in Figure 6 we do not report the parameters' values if at a certain point x there are no cars. This explains the missing points, e.g., around $x = 800m$ in the random scenario curve due to the result of the random generator being 0 in that point.

Figures 7 and 8 provide some insight into how FPAV works. The original *Offered-Load*, which exceeds *MBL*, has been adjusted right below this threshold. The values of PA at the end of FPAV's execution look fairly distributed in case the alternative 2 of stage 2 is used (Fig. 8). On the other hand, in Figure 7 it can be observed how some nodes are allowed to transmit with much higher power than their neighbors since once BMMTxP was achieved no fairness constraint was considered. If we take a close look and compare both plots we can appreciate how nodes around this few high power nodes (from 1000m to 1750m in Fig. 7) can not increase the assigned power at the end of stage 1 of FPAV ($PA = 0.74$ as, e.g., $x = 2000m$ in both plots). However, nodes placed at the same region can increase their PA value one step further (to 0.75) when using alternative 2 of FPAV-stage 2 (Fig. 8).

Let us now take a closer look to Figure 8 to better understand FPAV's behavior. First, we notice that curves in Figure 8 represent the result from the car distribution plotted as *Uniform Vehicle Density* (Fig. 6). Since we computed the *Vehicle Density* over a range of 1000m, the *Offered Load* matches Figure 6 scaled up by a factor of 20Kbps/car (this also applies for the random case). Now, we can observe how the channel load increases with the car density in the rear side of the cloud (lower xs). At the same time, the increase of the vehicle density causes the PA values to start decreas-

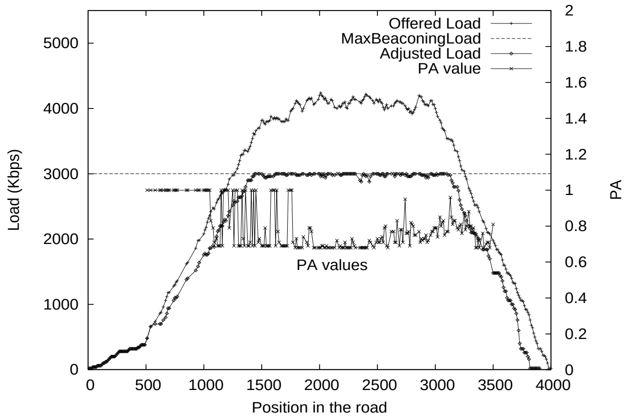

Figure 9: Random Traffic Cloud. Load on the channel at every point of the random scenario before and after applying FPAV with alternative 1 of stage 2.

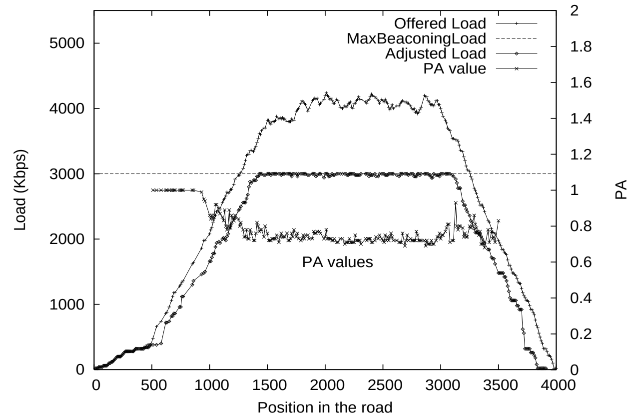

Figure 10: Random Traffic Cloud. Load on the channel at every point of the random scenario before and after applying FPAV with alternative 2 of stage 2.

ing (at $x = 840m$). At this point too many vehicles intend to transmit inside this specific region, and the value of PA decreases from 1 (where density is still 1car/20m) to 0.75 (where density starts being 1car/5m). Then, the values of PA remain almost constant (0.74 or 0.75) up to the first car of the cloud ($x = 3500m$). The value of PA as computed at the end of the first stage of FPAV in the denser region of the road, i.e., the lowest PA value at the end of both stages, can be easily calculated as follows:

$$PA = \frac{MaxBeaconingLoad}{2 * CS_{max} * Vehicle\_Density * Load_{vehicle}} - \epsilon$$

Note that if we would not subtract ϵ from PA the resulting load would exceed *MaxBeaconingLoad* since in our discrete scenario in a range of, e.g., 500m there are 101 cars and not 100. Thus:

$$PA = \frac{3Mbps}{2 * 500m * 1car/5m * 20Kbps/car} - 0.01 = 0.74$$

The reason for $PA = 0.75$ in some regions of the road is that $PA = 0.74$ is not a per-node maximal solution. Therefore, some nodes can increase their transmission power one step further without violating the condition on the network load $BL(PA) \leq MBL$.

Very interesting are also the results obtained from the random scenario (Fig. 9 and 10). Observe how FPAV achieves a good channel utilization in both cases, i.e., the *Adjusted Load* stays very close to *MBL* whenever possible. Contrary to the deterministic scenario and due to the random distribution of the nodes, cars in the front part of the cloud do not, in general, have the same value of PA (or one ϵ difference) after executing FPAV. The main difference when comparing Figures 9 and 10 is the higher deviation that PA values present in the former one. Since nodes do not sequentially increase their transmission power by one single step one after each other there exist many more nodes achieving high PA values (the maximum, 1) as well as low values (the minimum in this scenario, 0.68). On the other hand, addressing fairness during the whole FPAV process (Fig. 10) results, in general, in a perfectly balanced distribution of the PA values of all nodes with respect to their surrounding neighbors. These results might demonstrate that one must be strict when applying design constraints in all steps of a process in order to achieve the desired results, i.e., fairness in our case.

5. DISCUSSION

We have presented a power control approach that achieves fairness when adjusting the channel load in VANET environments. In this section, we discuss the feasibility of our approach and outline open issues we have to consider when specifying an implementation for real environments.

Determining the MaxBeaconingLoad threshold. The determination of the *MaxBeaconingLoad* threshold depends on safety requirements of the applications that must be fixed by application designers. We expect that, in order for the safety system to be reliable, safety applications should be updated with new information *a)* within a specific time and *b)* with some minimum reliability. Hence, issues to consider when determining the *MaxBeaconingLoad* are the accuracy of the positioning devices, the reaction time of the potential drivers, the efficiency of the breaking system, etc. Also, a very important issue to address is how to balance the accuracy and amount of information. The trade-off situations spans between using low transmission power for *accurate* state information only from nearby nodes to using high transmission power to acquire *less accurate* state information from more nodes including further ones.

Once safety related issues are addressed, communication challenges come into play. Note that, as commented in Section 3, we assume a constant packet generation rate for all cars performing beaconing. Nevertheless, accurately estimating the maximum load in the channel that guarantees a minimum performance level is not straightforward in our environments. In fact, wireless medium access control protocols have to deal with the hidden terminal problem, with non-deterministic channel characteristics, and mobility. Therefore, a thorough study of this issue will be needed when technology requirements will be defined.

Implementation issues. Our goal is to implement FPAV (with alternative 2 of stage 2, Fig. 5) in a fully distributed, localized and asynchronous fashion. Note that the current version of FPAV is centralized and requires synchronization between nodes. In principle, we can think about two approaches to solve this problem. The first one is a mere distributed implementation of FPAV, i.e., the same protocol is executed at each node, and nodes increase their PA value synchronously until the *MaxBeaconingLoad* threshold is reached. Implementing this approach would require a tight synchronization among the nodes and a 'global knowledge' of the channel load to determine whether the condition on the maximum allowed load is satisfied in the entire network. We believe this approach is not feasible in VANETs where the high degree of mobility renders the goals of ensuring tight synchronization and of quickly assessing global information too ambitious (at least with current technology).

The second approach is to let every node execute FPAV 'internally' (i.e., without synchronization and network-wide check of maximum offered load), assuming nodes have some knowledge about their environment. Observe that, if nodes would know the state of the other nodes (e.g., their exact position, speed) and their communication parameters (e.g., CS range, packet generation rate), they could run FPAV by themselves and compute the resulting PA values of all nodes for that specific situation, and this set of values would be the same for all the nodes (assuming all the nodes have the same knowledge). Clearly, the performance of this approach depends on how accurate the knowledge about the state of other vehicles is, and whether the nodes have *complete* knowledge of the environment (as it is assumed above), or only a *partial* knowledge of the environment. In the latter case, the computed solution (i.e., setting of the PA values) would probably be sub-optimal, but the induced load needed to maintain environment information would be minimized. A careful study of this approach, and of the tradeoff between computing an optimal solution with global knowledge (but high overhead to maintain the environment information) and computing a suboptimal solution with only local knowledge is left to future work.

Real channel characteristics. The unreliability of the wireless channel due to, e.g., fading, will affect the accuracy of the state information acquired from the other vehicles on the road. In reality, the probability that a packet is successfully received does not only depend on collisions but also on the SINR (Signal to Interference and Noise Ratio). In absence of collisions, the higher the received power the lower the BER (Bit Error Rate), see for example the curves that Yin et al. provide in [9]. The trade-off between lower BER and higher interferences must be taken into account when designing any wireless system, specially in VANET's environments, i.e., in highly populated broadcast scenarios.

6. RELATED WORK

Channel capacity and power control are broadly studied concepts in ad hoc networks. We can find studies since the early years, Kleinrock and Tobagi [10] analyze the throughput of CSMA transmission protocols already in 1975. Since then, a large number of studies tried to optimize the channel throughput or capacity adjusting the transmission power. Up to now, though, no study addressed our specific situation. The particularity of having safety as main goal brings to VANETs new constraints not considered before. Most of the studies address unicast environments and try to improve the spatial reuse minimizing the interference or energy consumption. These studies find the path to the destination that minimizes energy consumption and/or maximizes the overall throughput. In the category of 'energy concerned protocols' would fit most of the topology control proposals such as [11], [12] and [13] that propose adaptive algorithms that make use of only local information to adjust their power or [14] that considers non-uniform transmission ranges. A slightly different approach is given in [15], [16] and [17] where the authors agree that the minimum transmission power does not always maximize throughput and then propose an adaptive algorithm as a function of the traffic load. Although we can find related issues and methodologies in all these works we have to remember that energy efficiency is not an issue in VANETs where nodes have unlimited power supply. In addition, another common goal of these approaches is to keep the network connected for unicast flows, which is a totally different approach than the one we are considering. For FPAV the goal is to make sure that nodes close to the sender will receive its messages with high probability while ensuring fairness in the overall system.

Maybe the most related piece of work to our study is performed by Li *et al.* in two steps [18] and [19]. The authors propose, first, an analytical model able to find a transmission power that maximizes 1-hop broadcast coverage and, second, an adaptive algorithm that converges to the beforehand fixed transmission power. Although they focus on a pure broadcast environment their assumptions make their approach infeasible for VANETs: *a)* all nodes are static and *b)* all nodes use the same transmission power.

Last, early this year appeared a study [20] where the effect of power control is identified in many wireless parameters. Although they had also in mind the before mentioned classical wireless networks goals, i.e., energy consumption, connectivity and throughput, their explanations can help understand some of the situations considered in former sections.

7. CONCLUSIONS

In this paper we studied a problem that VANETs will face when achieving high penetration rates in dense traffic roads, i.e., the limited channel capacity to support the exchange of safety-related information. In these scenarios we consider that all nodes can send two types of safety related messages: *a)* periodic messages to make the other cars aware about their state and *b)* emergency messages triggered by the detection of a non-safe situation. In order to ensure that both types of messages can be handled efficiently with the existent resources we propose to limit the wireless channel load resulting from the periodic messages. Moreover, we require a strict fairness among the vehicles because of the safety nature of VANET applications.

With the constraints commented above, and assuming a constant packet generation rate, we formally defined the challenge in terms of a max-min optimization problem and extend it to obtain per-node maximality. Additionally, we proposed FPAV, a centralized power control algorithm that provides an optimal solution to the defined problem in two stages. In stage 1 FPAV maximizes the minimum transmission range for all nodes in a synchronized approach. For the stage 2 of FPAV we have considered two different approaches to achieve a maximum transmission range for all nodes individually while satisfying the condition of keeping the channel load under a certain limit. We proved the validity of FPAV formally and visualized the performance of both approaches with simulations under idealized conditions. Simulations have shown how the desired results are achieved when strict fairness constraints are applied to all steps of the algorithm.

Finally we discussed all issues that will have to be dealt with when bringing the algorithm into a real scenario: *a)* finding the proper maximum load threshold that ensures a good performance of the safety protocols, *b)* optimizing the performance of the algorithm with only local information and *c)* fighting against the adverse and uncertain wireless channel conditions. In our future work we will perform a detailed study of these issues. Our goal is to come up with a fully distributed, localized and asynchronous implementation of the protocol and to validate its performance comparing it with the optimum computed by FPAV as defined in this paper.

8. ACKNOWLEDGMENTS

The authors would like to thank Prof. Raja Sengupta and his team at U.C. Berkeley, Qing Xu, Tony Mak, Jeff Ko and Anthony Patire, for useful and stimulating discussions on earlier versions of this paper.

Marc Torrent-Moreno acknowledges the support of the German Ministry of Education and Research (BMB+F) within the “Network-on-Wheels” project under contract number 01AK064F.

9. REFERENCES

[1] Vehicle Safety Communications Consortium. http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm.

[2] Dedicated Short Range Communications Project. http://www.leearmstrong.com/DSRC/DSRCHomeset.htm.

[3] Internet ITS Consortium. http://www.internetits.org.

[4] The PReVENT Project. http://www.prevent-ip.org.

[5] The NOW: Network on Wheels Project. http://www.network-on-wheels.de.

[6] Dedicated Short Range Communications working group. http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[7] Federal Communications Commision. FCC 03-324. FCC Report and Order, February 2004.

[8] M. Torrent-Moreno, Daniel Jiang, and Hannes Hartenstein. Broadcast Reception Rates and Effects of Priority Access in 802.11-Based Vehicular Ad-Hoc Networks. In *Proceedings of ACM International Workshop on Vehicular Ad Hoc Networks, Philadelphia, Pennsylvania*, October 2004.

[9] J. Yin, T. ElBatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, and T. Talty. Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks. In *Proceedings of ACM International Workshop on Vehicular Ad Hoc Networks, Philadelphia, Pennsylvania*, October 2004.

[10] L. Kleinrock and F. Tobagi. Packet Switching in Radio Channels: Part I–Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics. *IEEE Transactions on Communications*, December 1975.

[11] Y. Chen, E.G. Sirer, and S.B. Wicker. On Selection of Optimal Transmission Power for Ad hoc Networks. In *Proceedings of Hawaii International Conference on System Sciences (HICSS), Waikoloa, Hawaii*, January 2003.

[12] M. Kubisch, H. Karl, A. Wolisz, L.C. Zhong, and J. Rabay. Distributed Algorithms for Transmission Power Control in Wireless Sensor Networks. In *Proceedings of IEEE Wireless Communications and Networking (WCNC)*, March 2003.

[13] X. Chen, M. Faloutsos, and S.V. Krishnamurthy. Power Adaptive Broadcasting with Local Information in Ad hoc Networks. In *Proceedings of the International Conference on Network Protocols (ICNP), Atlanta, Georgia*, November 2003.

[14] W. Song X. Li and Y. Wang. Efficient Topology Control for Wireless Ad Hoc Networks with Non-uniform Transmission Ranges. In *Proceedings of ACM Wireless Networks (WINET)*, 2003.

[15] S. Park and R. Sivakumar. Quantitative Analysis of Transmission Power Control in Wireless Ad-hoc Networks. In *Proceedings of International Conference on Parallel Processing Workshops (ICPP), Vancouver, Canada*, August 2002.

[16] S. Park and R. Sivakumar. MobiHoc Poster: Adaptive Topology Control for Wireless Ad hoc Networks. *ACM SIGMOBILE Mobile Computing and Communications Review (MC2R)*, July 2003.

[17] J. Liu and B. Li. MobileGrid: Capacity-aware Topology Control in Mobile Ad Hoc Networks. In *Proceedings of IEEE International Conference on Computer Communications and Networks (ICCCN), Miami, Florida*, October 2002.

[18] X. Li, T. Nguyen, and R. Martin. An Analytic Model Predicting the Optimal Range for Maximizing 1-HopBroadcast Coverage in Dense Wireless Networks. In *Proceedings of International Conference on Ad-Hoc Networks and Wireless (ADHOC-NOW), Vancouver, Canada*, July 2004.

[19] X. Li, T. Nguyen, and R. Martin. Using Adaptive Range Control to Maximize 1-Hop Broadcast Coverage in Dense Wireless Networks. In *Proceedings of IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON), Santa Clara, CA*, October 2004.

[20] V. Kawadia and P.R. Kumar. Principles and Protocols for Power Control in Wireless Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications (JSAC)*, January 2005.