Performance analysis and simulation in wireless mesh networks

Roberto Cusani, Tiziano Inzerilli, Giacomo Di Stasio
University of Rome Sapienza
INFOCOM Dept.
Via Eudossiana 18, 00184 Rome, Italy

Abstract —Wireless Mesh Networks (WMNs) can be used as convenient replacements of wireline networks in the context of emergency scenarios. WMNs technologies can be advantageously exploited to quickly set-up a new communication infrastructure to recover from terrestrial network collapse. However, in order to enable effectively operative communications through a WMN infrastructure, traffic control measures are generally needed, as wireless communications especially in mesh network configurations can be affected by significant congestion and channel impairments problems.

In this work1, we are focusing on performance assessment and enhancement in WMNs. In particular we are examining traffic control design aided by simulation. Experimental results are presented from simulation models of IEEE802.11b technology obtained through the open source INET framework of OMNET++.

Index Terms — Wireless Mesh Networks, traffic control, IP QoS

I. INTRODUCTION

IEEE 802.11 is a largely adopted technology for deployment of wireless local area networks (LANs)[1]. In this context, IEEE 802.11 is often configured to operate in the infrastructure mode, where a set of access points (APs) serve as communication hubs for mobile stations and provide entry points to the Internet and the current role of IEEE 802.11 is limited to direct communications between mobile clients with a single AP.

As an alternative, IEEE 802.11 can be used to interconnect form a full wireless mesh network (WMN) by means of two additional modes of operation. The ad-hoc mode can be used to form a single-hop ad-hoc network where nodes communicate with each other directly without the use of APs and the wireless distribution system (WDS) mode allows forming point-to-point AP relay links where each AP acts also as a wireless relay node.

Such WMN, however, does not possess satisfactory levels of QoS, for various reasons. The intrinsic unreliability of the wireless medium along with the potentially high number of traversed hops, make it difficult to provide bandwidth guarantees as in all WMNs. In addition, the contention based MAC scheme, i.e. CSMA/CA [3] operated with the DCF (Distributed Coordination Function), poses serious challenges in the control of the end-to-end delay [4, 5], as it does not assure time-bounded access.

In order to support real-time multimedia communications in a IEEE802.11 WMN, one can compensate for the lack of effective traffic control strategy at the IP layer. Before IP traffic is relayed to the IEEE802.11 NIC (network interface card) for transmission [6] bandwidth and buffer management strategies can be applied. In addition, the alternative time-bounded PCF (Point Coordination Function) [3] MAC scheme can be adopted along with the DCF based on CMSA/CA.

In this work we are presenting traffic control analysis and design in a IEEE802.11 WMN using simulation models, which have been developed using OMNET++ tool. In particular, we are concentrating on bandwidth allocation and control of packet transfer delays in nodes receiving multiple real-time and non-real-time IP flows with a CSMA/CA MAC.

In section II we introduce the simulation models which we have used to study IEEE802.11 mesh networks. In section III a theoretical estimation of available bandwidth in a IEEE802.11 link is developed. Finally, in section IV we show experimental results obtained with the OMNET++ simulator.

II. SIMULATION MODELS

OMNeT++ [7] is an open-source simulation tool, which can be freely used for academic research. Within OMNET, the INET framework provides support for most common network protocols, including TCP/IP and ethernet networks.

Instead, the Mobility framework includes simulation models for wireless channels and mobile nodes, including IEEE802.11b (currently work in progress). We have used these two frameworks as the basis for building our traffic control models for IEEE802.11 networks.

Fig. 1 shows a possible network configuration for a WMN, obtained by interconnecting two AP nodes heading two wireless cells.

AP relay stations are critical nodes for QoS as they aggregate and dispatch traffic. In APs traffic control policies are needed in order to control end-to-end delays and bandwidth allocation. In our simulation models we have then provided such nodes with traffic control.

Fig. 2 depicts the traffic control model along with the NIC (Network Interface Card) model it interacts with. The traffic control is based on an EDFPS (Earliest Deadline First Packet Scheduler) model in the AP node consists of the following components:

---

1 This work is partially supported by the Italian National project Wireless 802.16 Multi-antenna mEsh Networks (WOMEN)[2] under grant number 2005093248.
III. ESTIMATING MAXIMUM COMMUNICATION THROUGHPUT IN
AN IEEE802.11 MULTIHOP LINK

Overall capacity experienced in a IEEE 802.11b link decreases from its nominal value on account of various factors, including

(i) channel impairments, determined by location-dependent errors due to multipath fading.
(ii) overhead introduced by control information added to each packet at the various architectural levels, which is strictly related to the packet size.
(iii) link contention, which is strongly dependent on the nodes contending the wireless medium bandwidth for transmission.

Effective capacity which is available in a IEEE802.11 link contended by N source nodes can be derived from [12], which we briefly summarize. Let us consider a single host transmitting one data frame in a IEEE802.11b link. The overall transmission time, i.e. \( T \), is given by:

\[
T = t_r + t_{\text{ov}}
\]  

where \( t_r \) is a MAC PDU (protocol data unit) transmission time and \( t_{\text{ov}} \) is a fix overhead introduced by the CSMA/CA protocol, including fixed intervals of time during which the medium is sensed prior sending a MAC frame and prior returning the corresponding acknowledgment respectively, the transmission time for an acknowledgment and the fix time for sending the PLCP preamble and header prior each MAC PDU.

When there are \( N-1 \) other hosts, further delay needs to be accounted for medium contention. In this case, an additional delay \( t_{\text{cont}}(N) \) (an analytical formula for \( t_{\text{cont}}(N) \) can be found in [13, 14]) will have to be considered, corresponding to the time spent during contention among the \( N \) nodes. The overall transmission time becomes as follows:

\[
T(N) = t_r + t_{\text{ov}} + t_{\text{cont}}(N)
\]  

Hence, the actual MAC capacity which is used for transmission in the IEEE802.11b will be given by

\[
C(N) = C_{\text{max}} \cdot \frac{t_r}{T(N)}
\]  

where \( C_{\text{max}} \) is the nominal capacity of the link IEEE802.11b, equal to 11Mbps.

We are now deriving an approximate formula for assessment of throughput in multi-hop scenario, which will be validated through simulations.

In Fig. 3 is depicted the dynamics of a multi-hop transmission from a source node \( S \) to a destination node \( D \), through intermediate relay stations \( R1, R2 \) and \( R3 \), which are used to interconnect nodes that are not in visibility.
IEEE802.11 links include an overhead order to maximize the overall throughput, each relay station should alternate intervals of transmission and reception as seen in Fig. 3 and dedicate 50% of their time for each of them. The maximum throughput at MAC layer can be then estimated at half of the link capacity in eq. (3).

In order to validate eq. (4) we have collected statistics of throughput from two scenarios where link capacity is completely saturated (Fig. 4, scenarios 1 and 2). Namely, two nodes (scenario 1, \(N_{\text{max}} = 2\)) and four nodes (scenario 2, \(N_{\text{max}} = 4\)) transmit UDP video streams to a destination node through an intermediate relay station respectively.

In both scenarios the analytical plane as for eq. (4) approximate well the simulation plane obtained through OMNET++ models. The maximum difference between the two planes is of 5% (scenario \(N_{\text{max}} = 2\), Fig. 4) and 7% (scenario \(N_{\text{max}} = 4\), Fig. 5). This provides an overall validation and assessment of eq. (4).

Eq. (4) can be used for an overall dimensioning of a multi-hop network rather then to provide accurate estimate of throughput, which in general can be hardly provided.
B. Throughput in presence of elastic and anelastic traffic

It is worth highlighting that theoretical throughput calculated as in eq. (4) can be approached only when the link is saturated with sessions running on UDP, which conveys anelastic traffic. If we instead transport TCP sessions in the link, throughput can be significantly reduced on account of packet loss due to contention as well as channel impairments. TCP, unlike UDP, react to packet loss by considerably reducing the throughput. As a consequence when bandwidth is contended between UDP and TCP sessions, UDP sessions tend to prevail over TCP sessions as their throughput is insensitive to packet loss. This behaviour has been observed and commented in the work [15].

We have then considered scenario 2 in Fig. 4 with a mix of UDP and TCP sources. Namely, we have considered two UDP video streaming sources along with an HTTP and an FTP session. The BER has been set to 10% and packet size for all the sessions set to 1024 byte. We have then observed a reduction of the throughput from 2.3 Mbps experience with 4 UDP video sources (Fig. 6) to 1.54 Mbps with mixed UDP and TCP sessions, which accounts for a loss of throughput of 33%, with video sources maintaining a mean throughput of 580 Kbps.

This result shows that in order to improve performance of TCP traffic in a IEEE802.11 link, it is necessary to separate contention of UDP sessions with TCP sessions, e.g. using PCF window for UDP flows and DCF window for TCP flows.

B. End-to-end delay performance

![Fig. 7 – Mean end-to-end (e2e) packet delay in scenario 2 with mixed UDP and TCP sources without traffic control](image)

Fig. 7 shows delay performance of the four traffic sources in scenario 2. If we compare delay statistics of the two TCP sources (FTP and HTTP flow) with the UDP ones (video1 and video2) we observe that performance of TCP transport is generally better than that of UDP transport. As no traffic control strategy is applied, delay differentiation between UDP and TCP can only depend on the interaction of UDP and TCP protocols with channel errors and the CSMA/CA MAC. This demonstrates that a traffic control strategy is required, first of all, to invert delay performance of TCP and UDP flows, so that UDP packets are generally delivered in shorter time than TCP packets.

![Fig. 8 – Mean end-to-end (e2e) packet delay in scenario 2 with mixed UDP and TCP sources with traffic control](image)

Figure 8 shows delay statistics in the previous scenario when traffic control is used in the AP node to implement differentiated QoS management of UDP and TCP flows. The traffic control which is used consists of two EDF schedulers, i.e. EDF1 and EDF2, and a PQ (priority queuing) scheduler [REF]. EDF1 is used to schedule packets of UDP flows and EDF2 packets for TCP flows. The PQ scheduler imposes that packets can be extracted from TCP queues only when UDP queues are empty. In addition, UDP flows are regulated by LB prior EDF1 so as to assure that TCP traffic is not starved by excessive consumption of resources by UDP traffic, which are given absolute priority over TCP traffic by the PQ scheduler. Table I shows priority parameters used in the simulation, which sets approximate target values to be reached by the end-to-end delay of the various traffic sources.

<table>
<thead>
<tr>
<th>EDF</th>
<th>Priority Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDF1</td>
<td>Video1 0.040 s, HTTP 0.080 s</td>
</tr>
<tr>
<td>EDF2</td>
<td>Video2 0.020 s, FTP 2.000 s</td>
</tr>
</tbody>
</table>

Table I - EDF priority parameters

It can be noticed from figure 8 that the incorporated traffic control has allowed to reduce the dependency of delay performance on the IEEE802.11 MAC and invert performance of UDP and TCP flows as required. In addition, adoption of traffic control has also resulted into performance differentiation among flows transported with the same protocol. Namely, end-to-end delay for one video source has been reduced from roughly 50 ms to 35 ms. In turn, end-to-end delay for HTTP and FTP flows from initial values of 40 ms for both has been increased to 100 ms and 2 s respectively.
The delay differentiation introduced by the traffic control has to be regarded particularly good considering that the overall load of video sources corresponds to 75% of the total traffic (i.e., throughput of each video source is roughly 580 Kbps, while the total throughput of the four sources 1.54 Mbps, as discussed in subsection A).

CONCLUSION

In this work we have dealt with performance analysis of IP flows transport over an IEEE802.11 mesh network. We have developed simulation models of traffic control for an IEEE802.11b network using the OMNET++ tool to carry out extensive simulations of various WMN scenarios.

Basing on [12] we have first developed a theoretical approach to estimate effective capacity in a IEEE802.11b link, where the medium is contended by $N$ nodes.

Statistics collected with the simulation models has shown that the throughput which is reached when using UDP sources well approximate the effective link capacity estimated theoretically. Formulas in the theoretical approach can be used for an overall dimensioning of a WMN.

As observed also in [15], when TCP sources contend the medium with UDP sources, generally exhibit lower performance. Namely, we have measured significant throughput loss in TCP flows with respect to UDP flows, which can be avoided scheduling UDP and TCP flows in separate PCF and DCF windows.

Conversely, when we observed end-to-end delay statistics, UDP flows has exhibited slightly worse performance. Using a traffic control strategy in relay nodes, we have showed how to invert UDP and TCP delay performance in favour of UDP traffic and determine further delay differentiation within UDP sources and TCP sources.

REFERENCES