

MPEG-4 video transfer over IEEE 802.11 WLAN

Ivan Gagro, B.Sc.E.E.; Riko Luša, B.Sc.E.E.; Vanesa Čačković B.Sc.E.E.

Ericsson Nikola Tesla d.d.

Krapinska 45, 10000 Zagreb, Republic of Croatia

Tel: +385 91 3654322, E-mail: ivan.gagro@ericsson.com

Tel: +385 91 3653127, E-mail: riko.lusa@ericsson.com

Tel: +385 91 3653588, E-mail: vanesa.cackovic@ericsson.com

Abstract - In this paper we explore the possibilities of using existing IEEE 802.11b and 802.11g networks to stream video content. The objective is to evaluate WiFi network as a mean to transport video services. Experiment performed on a private network show some issues that manifest as breaks in transmission and unstable throughput and quality of a streamed video. Also, we discuss several other factors that can have effect on a quality of a video stream. We conclude that WiFi networks can be used to stream video content with recommendation to use point-to-point connections and avoid access points that serve more clients to achieve maximal transmission quality.

I. INTRODUCTION

In last few years Wireless Local Area Networks (WLAN's) have become very popular, especially IEEE 802.11 standard [1], which became almost standard network equipment in every household or company premises. 802.11 standard is mostly used as extension to Ethernet (IEEE 802.3) [2], which used as backbone part of LAN networks. However, WLAN can also be used as an alternative to wired LAN in case that physical interconnection is not possible.

With introduction of new multimedia contents, including streaming of high quality audio/video signal over IP networks and the emergence of internet TV services have put huge demands on bandwidth, which has to be provided to end user. There are two major methods of delivering streaming audio and video content over the Web. The first method uses a standard Web server to deliver the audio and video data to a media player. The second method uses a separate streaming media server specialized to the audio/video streaming task.

Wireless systems based on 802.11 technology became very affordable today, and allow end-users to connect to the network without cables. As most of multimedia devices have 802.11 interface cards already built-in, or it can be added at very low cost, it seems that we have technology that fulfills our needs. Unfortunately, these sounds too good to be true.

802.11b standard, with maximum physical data rate of 11 Mbit/s should be able to support Standard Definition (SD) MPEG-2 (Moving Picture Experts Group) encoded video stream, while faster 802.11g/a networks (with 54 Mbit/s) support High Definition (HD) video stream. There is also relatively new standard, which is not officially released yet (only in draft version), 802.11n, with theoretical maximal throughput of 300 Mbit/s, but we are not evaluating this one, as it's not as popular as 802.11a/b/g yet.

Multimedia applications should be able to run in physically heterogeneous environment, consisting of both wired and wireless component. There are two major problems for wide deployment of wireless LAN networks regarding real-time applications, and those are very limited Quality of Service (QoS) support and unstable quality of radio interface. Non-real time applications are more reliant on difference between playbacks and download rate at the client premises. In this paper we will focus on the later, often called "progressive download" method of delivering media over Internet.

In this paper we will present some tests, which were done in real 802.11b/g networks.

II. VIDEO OVER WIFI REQUIREMENTS

To better understand how characteristics of an WiFi link affect the streaming video, we will review the metrics that are usually used to define quality of a video session: IPDV, packet loss rate, out-of order delivery, throughput, end-to-end delay. IP performance parameters are defined in [3], and network performance levels are defined in [4].

Inter-packet delay variation (IPDV) is difference between the one-way-delay of the selected packets. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably.

Packet loss rate also effects video quality, as decoded video will show artifacts (blocks) that are associated with the lost packets. Loss of packets occurs in routers along the path if their buffers are full when the packet arrives. The receiving application may ask for a retransmission causing severe delays in the overall transmission. It has little effect on "progressive download" type of streaming, unless mayor loss happens that causes buffered part to be spent.

Out-of order delivery can happen when packets travel on different routes, resulting in different delays. The end result is that the packets arrive in a different order than they were sent. This problem requires special additional protocols responsible for rearranging out-of-order packets to an isochronous state once they reach their destination. This has serious effect in video streams where quality is dramatically affected by both delays and lack of isochronicity. It has little effect on "progressive download" type of streaming.

Throughput is the bandwidth required by a single video stream to ensure that minimum level of quality is maintained. Typical DVD video is coded in MPEG-2 standard and achieves maximum bit rate of 15Mbit/s, MPEG-4 streams (encoded in ITU-T H.264 [5]) that have

become common way of encoding any video content can achieve up to 56 Mbit/s for a High definition video. As shown in Section III, our evaluation will be based on video encoded using MPEG-4 codec, which consumes up to 75KB/s of bandwidth.

At the first look, IEEE 802.11b seems to be appropriate for the video streams of standard definition video. As the following sections will show, some characteristics of WiFi networks induce significant barriers for video streaming in existing networks.

III. VIDEO TRANSPORT TRACES

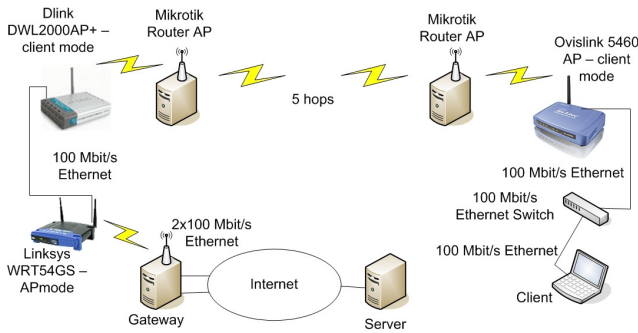


Fig. 1. Network layout used

Our testing environment is actually live network in Zagreb (ZNET), based mostly on 802.11b standard. We collected data traces on transport of media between two network nodes and measured packet delays. Figure 1 presents part of the network used for experimental purposes. Data was collected using network monitoring program called Wireshark [6].

Backbone of the network is based on Point-to-Point links between Mikrotik routers. There were 8 wireless hops between client side and gateway connected to internet. We assumed that local 100Mbit/s switches don't degrade quality.

Gateway is connected to the Internet service provider with two 100Mbit/s network interfaces, providing connection toward the Joost Internet TV service, stated as Server on Fig. 1 [7]. Joost service uses a web interface to connect the user with multimedia content (movies, shows, music, etc.) using a Flash embedded player in client browser. The streaming client starts playing the video while it is downloading, after only a few seconds of buffering, the process of collecting the first part of a media file before playing. This small backlog of information, or buffer, allows the media to continue playing uninterrupted even during periods of high network congestion. With this delivery method, the client retrieves data as fast as the Web server, network and client will allow without regard to the bit-rate parameter of the compressed stream. Service model that is used in the process is QoS class 5 or better known as "best effort" [4].

Connection to video server was provided by HTTP protocol, and video was being transported using TCP/IP. Connection is secured using Transport Layer Security (TLS), ensuring data security and integrity (Figure 2).

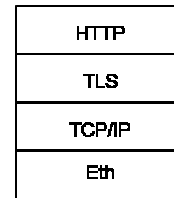


Fig.2. Connection protocol stack

Timestamp and sequence numbers in headers were used to monitor time the packet is sent and received, to measure packet loss. Arrival of each packet is noted to calculate the delay between arrivals of each packet.

We performed testing of Linksys Access Point to measure parameters which could have impact on final result and quality of video stream (Table 1).

TABLE 1
SNR TESTING OF LINKSYS

	SNR (dB)				
	<=10	10-20	20-30	30-40	>=40
Max. Throughput, Mbit/s	0,31	1,07	3,52	4,21	4,71
Average Throughput, Mbit/s	0,21	0,95	3,38	4,16	4,62
Jitter, ms	130,91	30,24	4,57	4,21	4,17

After that we performed measurement in testing environment, measuring same parameters.

TABLE 2
SNR IN TESTING ENVIRONMENT

	SNR (dB)				
	<=10	10-20	20-30	30-40	>=40
Max. Throughput, Mbit/s	0,23	0,91	3,31	4,05	4,52
Average Throughput, Mbit/s	0,18	0,79	3,18	3,98	4,41
Jitter, ms	274,37	74,27	26,58	24,31	23,56

As it can be seen from measured parameters in Table 2, Linksys AP was not a bottleneck in the network. As other nodes are in actual network, we didn't have any influence on their parameters.

Round trip time (RTT) is shown in Figure 2. Average RTT for our experiment does not go above 50ms. But the video stream is not so much affected with the RTT; its quality is more influenced by variations in one way delay. Bigger variations of one way delay could be subjectively confirmed as small glitches in the video scene that, if this continues decreases the experience in watching the video.

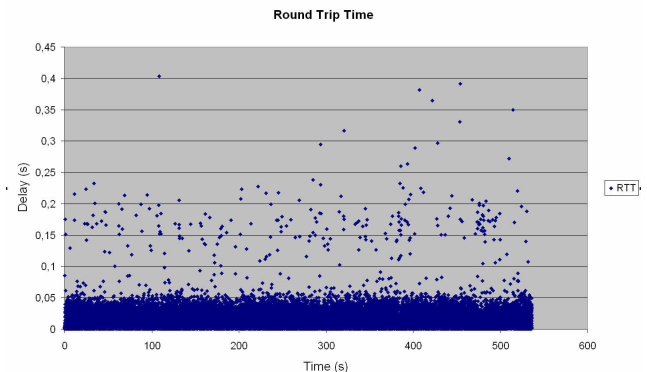


Fig.2. Round Trip Time

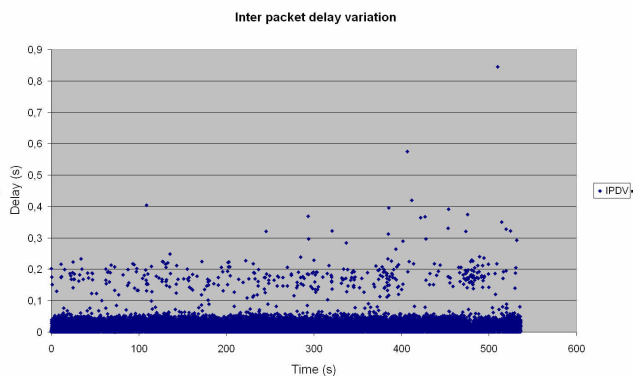


Fig.3. Inter packet arrival times

For this purpose we have measured inter packet arrival times to obtain this relative measure. Figure 3. shows how arrival times were distributed over a measuring period.

Subjectively, the quality of the video being watched is good as long as it is shown in small display sizes. As the bit-rate of the video was consuming 75KB/s of bandwidth, it was not intended to be displayed on large screens, where video encoder low bit-rate compression would seriously jeopardize normal viewing.

IV. MAJOR OBSTACLES TO VIDEO OVER WIFI

We can identify 2 major obstacles of streaming video over WiFi: pollution with overlapping channels, and throughput. Also, we look at other obstacles such as fairness.

A. Channel pollution and overlapping

IEEE 802.11 a/b/g all communicate in their respective operational frequencies by splitting their frequencies into 13 channels of 25MHz. A major difference between 802.11b/g and 802.11a is that the channels in 802.11b/g overlap (Figure 4), creating interference whereas the channels in 802.11a do not. In general, channel 1 on an 802.11b/g network overlaps with channels 2, 3, 4, and 5. This means that if a home network is on channel 1, but neighbor's home network is on channel 2, our WiFi signals may interfere, causing a degradation of performance for both networks (WiFi pollution).

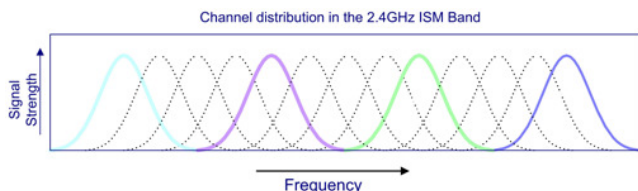


Fig.4. Channel distribution in 802.11b/g

In order to reduce the interference from nearby channels, there are 4 channels that do not overlap and can be used increase performance: 1, 5, 9 and 13.

Contrast to this is 802.11a which has 13 clear channels meaning there's less of a chance that degradation will occur. Recently many countries of the world are allowing operation in the 5.47 to 5.725 GHz Band as a secondary user using a sharing method derived in 802.11h. This will add another 12/13 Channels to the overall 5 GHz band

enabling significant overall wireless network capacity enabling the possibility of 24+ channels in some countries.

Connected to this overlapping issue is channel pollution. Wi-Fi pollution, or an excessive number of access points in the area, especially on the same or neighboring channel, can prevent access and interfere with the use of other access points by others, caused by overlapping channels in the 802.11g/b spectrum, as well as with decreased signal-to-noise ratio (SNR) between access points. This can be a problem in high-density areas, such as large apartment complexes or office buildings with many Wi-Fi access points. Whilst it poses a problem, overlap does not completely preclude wireless communications. The Media Access Control (MAC) specification for 802.11b networks implements a CSMA/CA (Carrier Sense Multiple Access Collision Avoidance) mechanism, which effectively means that each AP listens on its channel before attempting a transmission. In the overlap scenario described above, the multiple APs would end up sharing the available channel resource (with some further reduction in throughput due to collisions). WiFi was designed to support many interfering, overlapping networks and handling the resultant packet collisions. So rather than entirely disrupting a wireless LAN, overlapping channel assignments 'merely' greatly reduce its efficiency. This is clearly not desirable, and so in order to reduce overlapping effect is to select one of the four non-overlapping channels for adjacent cells, allowing all APs to operate at their peak throughput.

Additionally, other devices use the 2.4 GHz band: microwave ovens, security cameras, Bluetooth devices and (in some countries) amateur radio, cordless phones and baby monitors, all of which can cause significant additional interference.

B. Throughput

Throughput of IEEE 802.11b/g should be enough for transmission of video stream encoded in standard definition. However, in practice, an IEEE 802.11b wireless network can hardly accommodate a video streaming service and additional network traffic at the same time, especially if the access point in the receiving end has multiple clients connected (explained in more detail in IV-C.). This, together with half duplex mode of operation of WiFi devices also means that video streaming will hit the bottlenecks quite often if network is working in its peak performance.

Additional retransmissions of packets caused by hidden node effect and multi-path are greatly reducing the capacity of the wireless medium causing throughput degradation. Approach that can reduce the hidden node effect in wireless networks is called Collision avoidance and uses Distributed Coordinated Function (DCF), which is simply that a transmitting node negotiates to reserve the channel with the receiving node prior to sending its packet. This is done by exchanging small RTS (Request to Send) and CTS (Clear to Send) packets. There's still a risk that a RTS or CTS packet from node 'A' could collide with one from node 'B' before either has reserved the channel, but as these packets are very small, there is much less chance of this happening than having big packets collide otherwise.

Unfortunately, the down side is that it uses up a fair bit of the available bandwidth, particularly when the packets are small. For example, when sending large 1,500 byte IP

packets on DCF-enabled Wi-Fi at an air-speed of 11Mbps, maximum speed that can be achieved is less than 60%. The rest of the bandwidth is taken up in signaling, including the RTS/CTS packets [8].

Multi-path propagation occurs when an RF signal takes different paths when propagating from a source (e.g., a radio NIC) to a destination node (e.g., access point). While the signal is en route, different objects and walls get in the way and cause the signal to bounce in different directions. A portion of the signal may go directly to the destination, and another part may bounce from an object, and then to the destination. As a result, some of the signal will encounter delay and travel longer paths to the receiver. Multi-path delay causes the information symbols represented in an 802.11 signal to overlap, which confuses the receiver. This is often referred to as intersymbol interference (ISI). Because the shape of the signal conveys the information being transmitted, the receiver will make mistakes when demodulating the signal's information. If the delays are great enough, bit errors in the packet will occur. The receiver won't be able to distinguish the symbols and interpret the corresponding bits correctly. The receiving station will detect the errors through 802.11's error checking process. The CRC (cyclic redundancy check) checksum will not compute correctly, indicating that there are errors in the packet. In response to bit errors, the receiving station will not send an 802.11 acknowledgement to the source. The source will then eventually retransmit the signal after regaining access to the medium. DSSS (direct sequence spread spectrum), which is used in 802.11b is more susceptible to multi-path effect. DSSS transmits information continuously over a relatively wide channel, nearly 30MHz. This leaves enough room for lower frequency elements of the DSSS signal to reflect off obstacles much differently than the higher frequency elements of the signal. The differences in reflectivity will cause a wider range of signal paths. Thus, 802.11b systems are more susceptible to multi-path delays. OFDM (orthogonal frequency division multiplexing) that is used by 802.11a and 802.11g transmits information on many narrow sub-channels, which also reduces the impacts of multi-path.

C. Fairness

It is difficult to achieve fairness in IEEE 802.11 networks. Capacity of an access point is limited and must be shared among other clients, thus greedy client can negatively affect other clients. IEEE 802.11 MAC layer was designed to give approximately equal probability of channel access to all clients, disregarding their packet size, signal quality, or transmission rate. So a client transmitting at 1Mbit/s can negatively affect other clients that are transmitting at a higher rate [9].

The main problem in fairness is the Automatic Rate Control (ARC) mechanisms [10]. These mechanisms use different coding schemes to adapt data rate to error rate. Meaning, if signal strength is low, ARC will choose a more resilient modulation decreasing its transmission rate in order to reduce frame loss rate and expand transmission range. Criteria's used by ACR mechanisms are not defined in the standard, so each supplier implements own strategy and defines own thresholds. This has effect in unpredictable and unfair equilibrium of the bandwidth sharing among wireless clients [11].

D. Connection quality

Quality of the connection is usually measured by different performance parameters [3], where some will have more effect on the quality of media being transported. But, these metrics are not reliable indicators. For example, packet loss rate is affected by automatic retransmission mechanism of IEEE 802.11 MAC layer. Before MAC layer notifies application layer, it may request retransmission of frame up to 7 times if its ACK message is not received. Application layer may not perceive that packet losses are happening until the loss is too great for it to recover from errors.

Metrics such as signal strength and SNR are also unreliable due to variation based on their susceptibility to interferences.

In summary, there is no definite measure for connection quality and current metrics are unstable and may not reflect the real connection quality.

V. CONCLUSION

After close monitoring of the video in the private WiFi network, we can conclude that existing WiFi networks can be used as a transport mechanism to deliver video content. Several notes have to be taken into account:

- The user is not connected to a same access point as the video server. This will have enormous impact on the quality of the receiving video stream;
- Signal strength is good without major disturbances;
- Preferably, receiving client will not share the access point with other clients. This is especially affecting the quality of video encoded in higher bit rate.

It has to be pointed out that even with all above restrictions, video stream is likely to show some quality degradation if transmitted over several wireless hops. Nevertheless, due to high popularity of WiFi, this might appear quite appealing to many users.

REFERENCES

- [1] IEEE 802.11, "Local and metropolitan area networks. Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", Piscataway, NJ, 1999.
- [2] IEEE 802.3, "Local and metropolitan area networks. Specific requirements. Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specification", Piscataway, NJ, 1999.
- [3] ITU-T Recommendation Y.1540, "Internet protocol data communication service – IP packet transfer and availability performance parameters", November 2007.
- [4] ITU-T Recommendation Y.1541, "Network performance objectives for IP-based services", February 2006.
- [5] ITU-T Recommendation H.264, "Advanced video coding for generic audiovisual services", November 2007.
- [6] Wireshark, network analyzer, <http://www.wireshark.org/>
- [7] Joost, Internet TV, <http://www.joost.com/>

- [8] A. Rahman, P. Gburzynski, "Hidden Problems with the Hidden Node Problem", *23rd Biennial Symposium on Communications*, p. 270 - 273, 2006,
- [9] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda, "Performance anomaly of 802.11b", *IEEE INFOCOM*, San Francisco, CA, 2003.
- [10] I. Haratcharev, J. Taal, K. Langendoen, R. Legendijk, and H. Sips, "Automatic IEEE 802.11 rate control for streaming applications", *Wireless Communications and Mobile Computing*, p. 421-427, June 2005.
- [11] G. Tan and J. Guttag, "The 802.11 MAC protocol leads to inefficient equilibria", *IEEE INFOCOM*, Miami, FL, March 2005.