Video Streaming Performance in Wireless Hostile Environments

Alexandros G. Fragkiadakis, Elias Z. Tragos, Ioannis G. Askoxylakis
Institute of Computer Science
Foundation for Research and Technology-Hellas
Heraklion, Crete, Greece
{alfrag, etragos, asko}@ics.forth.gr

Abstract—Wireless networks have been among the main trends during the last few years. Their low-cost deployment and ubiquitous coverage have enabled the provision of numerous services to the end-users. Wireless local area networks (WLANs) are capable of providing many services with high quality of service (QoS), including not only email and web browsing, but also multimedia services. As the demand for more ubiquitous communications increases, mainly because of the rapid proliferation of the Wi-Fi enabled smart phones, wireless networks will play a crucial role in the future networks domain. Nevertheless, due to their open nature, these networks have several vulnerabilities that adversaries can exploit. In this paper, we use an adversary that violates several rules of the IEEE 802.11 protocol. We show, by collecting cross-layer measurements, how it can severely degrade the performance of an MPEG-4 encoded video streaming application. We also show that the traditional PSNR evaluation metric is not sufficient to characterize the video performance when an adversary is present.

Keywords: video streaming performance, MPEG-4, wireless networks, jamming attacks, peak signal-to-noise ratio, packet loss, CRC errors, PHY errors

I. INTRODUCTION

Wireless networks are unreliable by nature, since wireless transmissions are vulnerable to interference, fading, multi-path propagation and attacks. This work focuses on the effect of MAC-layer jamming attacks on the performance of a video streaming application over a wireless network and to the best of our knowledge; no previous work has investigated this issue. We show how an adversary called as Jammer can severely disrupt the network operation and degrade the performance of a video streaming application. Jammer violates some basic principles of the IEEE 802.11 protocol, such as the contention and back-off mechanisms. For the measurements we used a real IEEE 802.11 network collecting cross-layer data.

Previous research has focused on investigating the reliability of data transmission over current wireless networks, such as 802.11-based networks, in different scenarios, especially focusing on the impact of interference on the performance of wireless links [1][2][3][4][5]. These works mainly focus on investigating the behavior of the wireless links in various topologies (laboratory, outdoor experiments, etc.) and they show how much the presence of interference degrades the performance of the links. Common metrics used for the performance measurements are the signal-to-noise-plus-interference ratio (SINR), received throughput, packet delay, jitter, and packet loss. The results, under any conditions and settings, show that interference can cause severe performance degradation.

Special attention has been given on multimedia delivery over wireless networks and many previous works have dealt with measurements of the ability of wireless links to support efficiently the transmission of multimedia flows [6][7][8][9][10]. These works emphasize mostly on the delivery of video over wireless links and most of them investigate how many video flows (with specific characteristics) can be supported by a wireless link. The metrics used in these cases are mostly the same as before, since the requirements of the video flows are mainly in terms of data rate, delay, and packet loss.

Closely related to the concept of this paper are the previous contributions that focus on the performance of video streaming delivery over wireless links, with the presence of interference at the links. In [11], the authors present the different metrics that are used to evaluate the quality of a video and discuss the effect of packet loss on the evaluation of the video quality. Packet loss is one of the main problems that degrade the performance of video streaming, which is delivered using UDP applications. UDP, by nature, provides unreliable transmissions, but is used to satisfy the delay requirements of video streaming. In [12], the authors discuss the issues and problems of providing multimedia in multi-hop wireless networks, using as an example a video streaming application. They use a real test-bed with different interference scenarios and they measure several performance indicators, such as the Peak Signal-to-Noise Ratio (PSNR), throughput, packet loss ratio, delay and jitter, in order to show the effects of interference on video streaming delivery over a multi-hop mesh network. The authors in [13] investigate the performance of video streaming applications, based on MPEG-2 video codec, in the presence of interference from blue-tooth devices and AWGN noise. The results include measurements for packet loss ratio, video quality metric (VQM) and jitter for different levels of the SINR. In [14], the authors have performed extensive measurements in various topologies of an ad-hoc network, but they focus only on PSNR measurements. In [15],
the authors measure the performance of a video application over a high data rate wireless link, but they also focus only on the perceived quality, measuring mainly the mean opinion score (MOS) of the received video and the packet loss for different settings of the experiments.

An area that has not gained much research attention so far is related to the impact of security attacks on the performance of multimedia applications over wireless links. The general performance of wireless networks under jamming attacks has been investigated in various works, but, to the best of our knowledge, no previous work has focused specifically on how jamming can affect the performance of wireless video streaming, which has strict quality of service (QoS) requirements. In [16], the authors investigate the performance of the IEEE 802.11 MAC protocol under two different jammers, namely a periodic and a memory-less jammer. At first, the authors present a theoretical analysis and then, they present experimental and theoretical results that show clearly that the throughput of the network can degrade severely due to jamming. In [17], the authors present various jamming attacks and their effects on the performance of wireless networks, providing also solutions for detecting such attacks. The authors in [19] investigate how the performance and capacity of the IEEE 802.11 medium access control (MAC) layer is affected by pulse jamming. The authors use a VoIP application to show the performance degradation due to jamming, but they do not conduct real experiments; they provide simulation results only. Finally, the authors in [18] discuss the problem of the physical layer jamming and propose several algorithms for its detection.

The rest of this paper is organized as follows. In Section II we describe the attack model and the hardware used to implement it. Section III describes the network test-bed used for running the experiments. In Section IV we present the results. Finally, the conclusions and further work appear in Section IV.

II. ATTACK MODEL

This section describes the model we use to perform the jamming attacks. Attacks are realized by a single machine (called as Jammer throughout the paper) that violates several features of the IEEE 802.11 protocol. In general, DCF (Distributed Coordinated Function) is the common method used for access in the wireless medium. Each station has to sense the medium first, before transmitting any data. If the medium is idle, at least for a specific amount of time, the station transmits its data; otherwise it has to wait for an additional time called as back-off time before attempting to transmit again. The back-off time is an integer multiple of a basic slot duration that is randomly chosen in the range [0, CW-1], where CW is the current contention window. This integer is randomly chosen so as to randomize the access to the medium for the several contending stations; hence with this random access mechanism, the collision probability is reduced. Our Jammer violates this principle by transmitting even when the medium is occupied. Its scope is to cause denial-of-service (DoS) attacks:

- by causing collisions as it transmits even when the channel is occupied by other stations,
- by occupying the channel so other nodes continuously enter the back-off stage and defer from transmission.

Generally, regarding the jamming implementations, there is always the trade-off between jamming intelligence and cost. A sophisticated jammer can cause severe performance degradation with the lowest energy consumption. On the other hand, a less intelligent jammer, based on off-the-shelf hardware can severely disrupt the network operation, however consuming more energy, but its cost is significantly lower. Hence, it can be used by individuals without any expert knowledge about network protocols and functions. Our jammer is realized by using a single mini-ITX board carrying 512 MB of RAM and an 80 GB hard disk. Furthermore, this board is equipped with an Atheros 802.11a/b/g CM9-GP mini-PCI card, controlled by Ath5k, an open source IEEE 802.11 driver [20], running on Gentoo Linux. The protocol violations (disabling of the back-off procedure and the medium sensing) became feasible by modifying the values of several hardware registers of the Atheros wireless card, through the Ath5k driver. Jammer is now oblivious of any other transmissions and thus it can freely jam the channel. Note that Jammer operates on the same channel that legitimate stations use to communicate; thus it can be considered as a MAC-layer jammer.

Several types of jammers have been described in the literature (e.g. periodic, memory-less etc). In this work, Jammer operated periodically, alternating between sleeping and jamming, emitting energy for \( a \) seconds, followed by \( b \) seconds of inactivity, and so on. We define as attack duty cycle (ADC) the ratio: \( \text{ADC} = \frac{a}{a+b} \). For the experiments, we kept \( b \) constant (10 seconds) modifying the time \( a \) that Jammer was active. Table I shows the ADCs we used for the different experiments we conducted. The ADC with the zero value (No Jam) corresponds to the case where no jamming was performed during the experiment.

<table>
<thead>
<tr>
<th>Symbolic name</th>
<th>ADC value ((a)/(a+b))</th>
<th>Jamming time (secs)</th>
<th>Sleeping time (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Jam</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jam #1</td>
<td>0.67</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Jam #2</td>
<td>1.33</td>
<td>40</td>
<td>60</td>
</tr>
<tr>
<td>Jam #3</td>
<td>2</td>
<td>60</td>
<td>10</td>
</tr>
<tr>
<td>Jam #4</td>
<td>2.67</td>
<td>80</td>
<td>10</td>
</tr>
</tbody>
</table>

III. MEASUREMENT TESTBED

We performed measurements in a real IEEE 802.11 network consisting of a Video Sender (VS), a Video Receiver (VR), two wireless gateways (WGWs), and the Jammer (Figure 1).
As shown in Table I, there are five different experiments, each with a different attack intensity. The attack intensity is controlled by the jamming time (the sleeping time is constant to 10 seconds). For each experiment, an MPEG-4 encoded video was transferred using RTP/UDP datagrams flowing from VS to VR. The characteristics of the video are: (i) the duration is 100 seconds, (ii) the file size is 6.8 Mbytes, (iii) there are 2100 frames (8.33% of I frames and 91.67% of P frames), (iii) the frame rate is 30 fps, (iv) the video bitrate is 762 Kbps, and (iv) the total number of packets is 6818.

We executed each experiment several times, recording data from multiple layers. Data were collected in the physical (PHY), medium access (MAC) and application layers, at the VR. Also, the packet loss was measured in the WGW1.

A. Data collection at the physical and the medium access layers of the VR

1) Cyclic Redundancy Check (CRC) errors

At the MAC layer of the VR we recorded the number of the arrived packets having a CRC (cyclic redundancy check) error. This type of packets have one or more of their bits corrupted and as the MAC layer uses no error correction codes, they are discarded. For each experiment, we computed the CRC ratio given by the number of the packets with CRC errors over the correctly decoded packets (packets with no errors), within the duration of the experiment.

2) Physical (PHY) errors

Furthermore, we recorded the number of the arrived packets having PHY error. During frame reception and before the MAC header is decoded, for several reasons (e.g. interference), the wireless card may become unable to continue with the reception process, so the corresponding frame is rejected. We computed the PHY ratio that is the ratio of the packets with PHY errors over the correctly decoded packets.

All the above information was collected directly in the wireless driver (Ath5k) in the VR. For this purpose, we implemented a software module that resides in the heart of the Ath5k driver (Figure 2).

B. Data collection at the application layer of the VR

As the aim of this paper is to study the performance of the video streaming application under jamming attacks using multi-layer information, we also collected experimental data referred to the application layer. These are categorized as follows:

1) Packet delay

The packet delay is defined as the difference between the arrival time and the transmission time. We recorded the time-stamps of the transmitted packets in the VS and the received packets in the VR. Each packet is uniquely identified by an id number carried by its IP header. VR and VS were synchronized using an NTP server [21].

2) End-to-end packet loss

By recording the packet ids in both the VS and VR, we were able to compute the packet loss at the end of each experiment.

3) Peak Signal-to-Noise Ratio (PSNR)

PSNR is an objective quality metric widely used to measure video performance. In general, PSNR is defined as the ratio of the maximum possible power of a signal and the noise power that corrupts the fidelity of its representation. For video evaluation, the signals are the images and noise is the distortion caused by a codec and/or the medium used for transmission (e.g. a wireless network). Supposing there are two m x n images S and D, where S is the original image and D the reconstructed image, the PSNR of this image is given by the following formula:

\[
\text{PSNR} = 20 \log_{10} \frac{V_{\text{peak}}}{\sqrt{\text{MSE}}} \label{eq:1}
\]

where \(V_{\text{peak}}\) is its maximum value (e.g. 255 for 8-bit encoding) and \(\text{MSE}\) is the mean squared error given by:

\[
\text{MSE} = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [S(i, j) - D(i, j)]^2 \label{eq:2}
\]

Consequently, PSNR gives the reconstruction quality of an image. The higher the PSNR is, the higher the fidelity of the reconstructed image. For each of our experiments, we
measured the PSNR for each of the received frames that comprised the transmitted video. We used Evalvid [22], a software tool that at the VS, it packetizes the video to be transmitted in RTP/UDP packets. At the VR, using the raw received packets, it reconstructs the received video. Then, by using the original transmitted video and the reconstructed video, it computes the PSNR in a per frame basis. For each lost frame we assigned a PSNR equal to zero.

C. Packet loss at the MGW1

We also measured the packets loss at the MGW1, which operates as a wireless gateway. Packet loss mainly takes place in the Linux ring buffer that resides between its IP layer and the driver software. This buffer operates in a first-in-first out queue, used to temporarily store the packets before handled by the wireless driver. The ring buffer has a constant size and so, if packets are stored in it faster than they are pulled-out by the wireless driver (for transmission), the previous packets are overwritten; hence they are lost. There are two reasons that can make the wireless driver unable to follow the rate packets are stored in the buffer, when jamming takes place. As mentioned in Section II, Jammer has its sensing and back-off mechanisms disabled. This means that it transmits even if the medium is occupied by the MGW1. This causes packet losses because:

- there is a large number of collisions at the VR; hence MGW1 has to retransmit multiple times each packet. Consequently, this slows down the rate driver reads packets from the ring buffer, resulting in losses within it (overwritten packets).
- MGW1 continuously defers from transmissions while Jammer is active, as the access to the medium is not fair. As MGW1 is trapped in the back-off process, packets are lost within its ring buffer.

IV. RESULTS

Using the network layout shown in Figure 1, we ran the experiments displayed in Table I several times, recording the information described in the previous section.

A. PSNR

We start our analysis by presenting the measurements collected at the application layer regarding the video quality. Figure 3 shows the PSNR for each received video frame, for two of the experiments: (i) when no jamming was used (No Jam), and (ii) when the Jammer was active for 80 seconds (Jam #4). As the duration of the experiment is 90 seconds, the second experiment can be regarded as a high intensity attack. During the high intensity attack, the PSNR reduces for a significant number of frames; therefore, the overall video quality significantly deteriorates. To better highlight the impact of jamming on video quality, Figure 4 shows the cumulative distribution function (cdf) of the PSNR, for the different attack intensities. As the intensity of the attack increases, the probability that the PSNR deteriorates, increases. As mentioned in [23], when the PSNR is over 37, the fidelity of the reconstructed frame is very high (excellent). Based on this and on Figure 4, observe that the probability of a frame to have PSNR lower than 37 is: (i) almost zero when no jamming is present, (ii) 8% in the case of Jam #1, (iii) 46% for Jam #2, (iii) 57% for Jam #3, and (iv) over 65% for Jam #4. Therefore, as the attack intensity increases, the probability that the video quality degrades, increases dramatically.

B. End-to-end packet delay

Except PSNR, the packet delay also affects video quality. According to [24], the recommended minimum delay for acceptable video quality with MPEG-4 encoding without error concealment and/or correction to be necessary, is 1 second. Figure 5 shows the cdf of the end-to-end packet delay, measured using the packet time-stamps at the VS and the VR. The packet loss when no jamming was used (No Jam) is almost zero, therefore its cdf equals 1, laying on the vertical axis of this figure. Observe that as the jamming intensity increases, the probability that the packet delay is smaller than the recommended 1 second; substantially decreases. For the
lowest intensity attack (Jam #1) the probability is about 60%. For Jam #2 it falls to 52%, while for Jam #3 is about 47%. For the highest intensity attack, the probability falls to 40%.

Figure 5. CDF of the end-to-end packet delay for the different attack intensities

C. MAC-PHY results and the packet loss

At this point, we present the measurements collected at the MAC layer, along with the packet loss measured at both the MGW1 and the VR. The packet loss measured between the VS and the MGW1, and between the MGW2 and the VR (Figure 1), is almost zero for all attack intensities. This is not surprising as these devices are interconnected through 10/100 Mbps wired Ethernet links; hence packets are exclusively lost during the wireless transmissions.

Table II shows that the packet loss at the MGW1 increases, as the attack intensity increases. This is because MGW1 does not have a fair access to the medium; it back-offs for longer times, and so packets are lost in its Linux ring buffer. Furthermore, when MGW1 finally manages to gain access to the medium and transmits packets, these can be corrupted at the VR, because Jammer successfully causes collisions. This is shown in the fourth column of Table II, where the CRC ratio (packets with CRC errors over the correctly received packets) dramatically increases. Observe that during the highest intensity attack (Jam #4), for about every 44 packets, only one is correctly received. Of course, the high CRC ratio affects the average end-to-end delay as for every not acknowledged packet, MGW1 has to retransmit it, probably several times.

Note that almost 6.7% of the packets are lost during Jam #1 and 72.3% during the highest intensity attack. As mentioned in [24], a maximum packet loss of 0.1% is recommended when MPEG4 coding is used without error concealment and/or correction to be necessary. Even for the lowest intensity attack (Jam #1), the average packet loss is much higher than 0.1%.

The excessive packet loss, as our results show, is caused by the large number of the corrupted packets at the VR, combined with the inability of the MGW1 to transmit packets as Jammer monopolizes the medium when it is active. The main problem however is packet corruptions as the CRC ratio shows. This makes us to revisit the PSNR cdf shown in Figure 4. In this figure is clear that PSNR deteriorates when Jammer is present. However, it does not reliably represent the degradation that video quality has suffered. In numerous contributions, is referred that when the PSNR is at least 31, the fidelity of the reconstructed video is at least good. Our experimental results show that even if the PSNR is relatively high (Figure 4) when a Jammer is present, the packet loss is mainly caused by packet collisions and this severely degrades video quality.

Table II. MAC-PHY layer measurements and the packet loss

<table>
<thead>
<tr>
<th>Attack type</th>
<th>Average packet loss at the MGW1 (%)</th>
<th>Average (end-to-end) packet loss at the VR (%)</th>
<th>CRC Ratio</th>
<th>PHY Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Jam</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.02</td>
</tr>
<tr>
<td>Jam #1</td>
<td>1.21</td>
<td>6.65</td>
<td>10.94</td>
<td>0.61</td>
</tr>
<tr>
<td>Jam #2</td>
<td>4.78</td>
<td>45.61</td>
<td>21.41</td>
<td>0.62</td>
</tr>
<tr>
<td>Jam #3</td>
<td>10.79</td>
<td>57.41</td>
<td>26.60</td>
<td>0.96</td>
</tr>
<tr>
<td>Jam #4</td>
<td>20.77</td>
<td>72.35</td>
<td>43.96</td>
<td>1.22</td>
</tr>
</tbody>
</table>

In Table II we also show the PHY ratio, that it is the number of the packets with PHY errors over the correctly decoded packet. The PHY ratio does not significantly increase when Jammer is present. However, if Jammer was operating in a neighboring channel we would expect a high number of PHY errors and fewer CRC errors.

V. CONCLUSIONS-FURTHER WORK

In this paper we show how an adversary can severely disrupt the operation of a wireless network, reducing dramatically the performance of a video streaming application. Collecting cross-layer data using a real IEEE 802.11 network, we identified the main causes for the performance degradation as: (i) the excessive losses due to the unfair access to the medium by the legitimate stations, and (ii) the large number of the collisions at the video receiver. We also show that the traditional method for video quality estimation using the PSNR does not reliably reflect the fidelity of the reconstructed video when an attacker is present. This can be explained by considering that PSNR only measures the quality of the reconstructed (at the receiver) video in relationship to the original video and it is not related to the video transmission. For real-time video streaming applications, not only PSNR, but also end-to-end delay and jitter are also very important quality metrics, since high delay and jitter results in higher buffering times at the receiving video player, which furthermore degrades the users’ quality of experience (QoE), since they are waiting more (than expected) time to view a video and during buffering, the video image stands still. Further work includes the investigation of the performance of
VI. REFERENCES


