Analysis of Jamming effects on IEEE 802.11 Wireless Networks

Abderrahim Benslimane
Avignon Computer Science Laboratory
Avignon University
Email: abderrahim.benslimane@univ-avignon.fr

Abdelouahid El Yakoubi and Mohammed Bouhorma
Department of Computer Science
Tangier Faculty of Sciences and Technologies

Abstract—IEEE 802.11 wireless transmissions suffer from a big security flaw as they are vulnerable to Denial of Service (DoS) attacks which can degrade severely their performance, especially their achieved throughput. One of the most harmful forms of these attacks is the jamming. In this paper, we provide an analytical model to study the effect of jamming on WLANs. Hence, we implement a physical layer jamming to show the effect at the MAC layer level (i.e. cross-layer jamming). Different jamming scenarios, with different modulation techniques such as Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM), are distinguished in order to evaluate the most accurately possible the effect of jamming on WLANs performance. Our validation model is confirmed by means of simulations under ns-3 simulation tool. We show that low rates (e.g. 1Mbps) are more resistant to jamming than high rates (e.g. 27Mbps). We also show that energy consumption when jamming depends on transmission time rather than other factors. These results allow to derive solutions for jamming.

Index Terms—DoS, Jamming, IEEE 802.11.

I. INTRODUCTION

Wireless Local Area Networks (WLANs) gain more and more popularity and they are implemented in many communication systems. The attractiveness of IEEE 802.11 technology is essentially due to its low cost and its easy deployment. However, with all advantages it offers, wireless communication suffers from security vulnerabilities due to the radio characteristics of the communication medium. Jamming is a kind of DoS which represents the most harmful risk that a wireless network may encounter [1]. A jammer is a malicious user that deliberately sends a signal from a wireless device in order to overwhelm legitimate wireless signals. Jamming may take many forms such as generating continuous high power noise across the entire bandwidth near transmitting and/or receiving nodes. In energy limited networks (e.g. sensor networks), detecting and countering jamming attacks is of critical importance [2]. In fact, energy efficient and less detectable jammers can be made using knowledge of communication protocol. Such jammers are called ”Protocol Aware Jammer” and the process is called Intelligent Jamming [3].

As jamming downgrades the successful transmissions rate of the attacked nodes, the study of its precise impact on network performance is too important because it is the first step in the design of robust solutions that improve network resiliency to DoS attacks.

Some previous works dealing with different jamming types show that intelligent jamming can have crucial effect on the network by ignoring the MAC protocol rules [3], [6]. However, those works consider ideal jamming conditions. This means that a jamming signal is able to destroy any legitimate signal once their transmissions overlap. Preventing jamming before it occurs is the subject of the work in [7]. The proposed method consists of sending fake signals by particular nodes deceiving jammers to attack them and giving time to other nodes to switch to another frequency of operation.

In this paper, we propose an analytical model to study the jamming effects on IEEE 802.11 networks with two modulation techniques namely DSSS and OFDM. In our simulations, we measure performance metrics such as Packet Delivery ratio (PDR), Received Signal Strength (RSS) and total consumed energy at each node. We consider a network acting in a saturation condition where every node has always packets to send. Most of the previous works that studied saturation throughput considered ideal channel conditions which means that transmission failures only occur because of collisions. In our work, we calculate the throughput by considering the same model as described in [4] for which several enhancements were proposed [8], [9]. Instead of considering only the collision probability, we consider also the probability of jamming and the physical channel capacity which involves the distance, the interferences and the packet length.

The remainder of the paper is organized as follows. Section II presents the background of the proposed model. In section III, we introduce our analytical model. In section IV, we present and discuss simulation results. Finally, a conclusion is given in section V.

II. MODEL BACKGROUND

A. Channel Capacity

According to Shanon, channel capacity can be defined as the maximum information that can be transmitted reliably from a source to a destination. For Additive White Gaussian Noise (AWGN) channels, the channel capacity is given by:

$$C = B \times \log_2(1 + SINR)$$  \hspace{1cm} (1)

where B represents the channel bandwidth in Hz (e.g. B = 22 MHz for DSSS) and SINR is the Signal to Interference plus Noise Ratio.
B. Throughput modeling

In order to analyze the effect of jamming on an IEEE 802.11 network, we study the impact of some jamming factors on the saturation throughput. The saturation throughput was studied in the literature in many works which consider ideal channel conditions (i.e., no hidden terminals and no capture effects) and without taking into account the effect of noise. We start our calculus with the throughput formula, given in [4], in the case of perfect conditions, to which we bring modifications to introduce the effect of jamming. In this work, Bianchi considers only the collision probability which is constant and equal for all nodes. Let $T_s$ be the time when the channel is sensed busy because of a successful transmission and $T_c$ the time when the channel is sensed busy because of a collision. Let $\tau$ be the probability of a transmission in a random slot time. For $\tau$ sufficiently small, and for $K = \sqrt{T_c/2\sigma}$ we get $\tau = \frac{1}{\sqrt{K}}$. The approximate expression of the maximum achievable throughput is given by:

$$S_{\text{max}} = \frac{E[P]}{T_s + \alpha K + T_c(K(-1 + \exp\frac{\tau}{K}) - 1)}$$  \hspace{1cm} (2)

Where $\sigma$ is the minimal amount of time needed at a station to detect a transmission from any other station, $P_s$ is the probability that a transmission occurring on the channel is successful, $P_i$ is the probability that there is at least one transmission in the considered slot time and $E[P]$ is the average payload transmitted in a successful transmission.

III. ANALYTICAL MODEL

In this section, we study the performances of a WLAN network when stations or access points (APs) are exposed to different conditions of jamming. We consider two types of jammer: continuous and periodic. We focus on jamming, at different conditions of jamming. We consider two types of network when stations or access points (APs) are exposed to interference power of the jammer is expressed as:

$$I = Q * d_r^{-\alpha}$$  \hspace{1cm} (3)

where $\alpha$ is an attenuation parameter such that $2 < \alpha < 4$.

A. Continuous jamming

1) Jamming a single node: The jammer sends a jamming pulse in each slot time to a single node. Thus, the received interference power of the jammer is expressed as:

$$C_r = B * \log_2(1 + \frac{P}{\rho + Q * d_r^{-\alpha}})$$  \hspace{1cm} (4)

where $\rho$ is the additive white Gaussian noise. To find the expression of $T_s$ given in 2, we denote by $T(\text{data})$ the time needed to transmit data information and by $\delta$ the propagation delay. For the basic access mechanism without reservation (i.e., RTS/CTS handshake):

$$T_s = T(PHY_{\text{hdr}}) + T(MAC_{\text{hdr}}) + T(E[P]) + SIFS + \delta + T(ACK) + DIFS + \delta$$

In this paper, we consider only the basic access mechanism. The derived formulas can be applied to RTS/CTS mechanism by simply changing the expression of $T_s$. Hence, for the basic access mechanism, we have:

$$T_s = T_0 + T(MAC_{\text{hd}}) + T(ACK) + T(E[P])$$

where $T_0$ is a constant value and depends only on the used modulation technique and has the expression:

$$T_0 = T(PHY_{\text{hd}}) + SIFS + \delta + DIFS + \delta$$

Due to the IEEE 802.11 anomaly as stated in [5], the transmission rate of all other nodes will be degraded and bounded by the transmission rate of the node suffering the most from interferences (i.e. the jammed node). Hence, the expression of the transmission rate $C$ will be the same as in (4). Therefore

$$T(MAC_{\text{hd}} + ACK + E[P]) = \frac{MAC_{\text{hd}} + ACK + E[P]}{C}.$$  \hspace{1cm} (5)

Assuming that the packet length $E[P]$ is the same for all transmissions and equal to a constant value $L$, and by using the approximate model, the maximum throughput would be:

$$S_{\text{max}} = \frac{L}{(T_0 + \frac{MAC_{\text{hd}} + ACK + L}{C}) + \alpha K + T_c(K(-1 + \exp\frac{\tau}{K}) - 1)}$$  \hspace{1cm} (6)

Substituting $C$ by its expression yields:

$$S_{\text{max}} = \frac{L}{(T_0 + \frac{MAC_{\text{hd}} + ACK + L}{B*\log_2(1 + \frac{P}{\rho + Q + d_r^{-\alpha}})}) + \alpha K + T_c(K(-1 + \exp\frac{\tau}{K}) - 1)}$$  \hspace{1cm} (7)

2) Jamming multiple nodes: We consider $n_{\text{jam}}$ jammed nodes in the network (i.e. $n_{\text{jam}} \in [2, n]$). As the power of interference depends on the distance between the jammer and the jammed node, we distinguish the case where the distances between the jammer and all the jammed nodes are equal and the case where the distances separating the jammer and the jammed nodes are different.

a) Equal distances: Let $d$ denote the same distance separating the jammer to the jammed nodes. Each node receives the same jammer interference power $I$. Hence, the channel capacity would have the expression:

$$C = B * \log_2(1 + \frac{P}{\rho + n_{\text{jam}} + Q * d^{-\alpha}})$$  \hspace{1cm} (8)

In this case, (7) can be rewritten as:

$$S_{\text{max}} = \frac{L}{(T_0 + \frac{MAC_{\text{hd}} + ACK + L}{B*\log_2(1 + \frac{P}{\rho + n_{\text{jam}} + Q + d^{-\alpha}})}) + \alpha K + T_c(K(-1 + \exp\frac{\tau}{K}) - 1)}$$  \hspace{1cm} (9)
expressed as:

\[ C = \log_2 \left( 1 + \frac{P}{\rho + I_1 + I_2 + \ldots + I_{\text{jam}}} \right) \]  

With the approximate model, the normalized throughput can then be expressed as follows:

\[ S_{\text{max}} = \frac{P L}{(T_0 + \frac{\text{MAC}_{\text{idle}} + \text{AC}K + L}{B \log_2 (1 + \frac{\text{MAC}_{\text{idle}} + \text{AC}K + L}{\rho + Q \sum_{r=1}^{n_{\text{jam}}} d_r^\alpha})}) + \sigma K + T_c (K(-1 + \exp \frac{K}{\delta})).) - 1} \]  

### B. Periodic jamming

1) Jamming a single node: In this case, the jammer sends a number of pulses, makes a break for some time and then restarts sending pulses, and so on. Let’s consider a time interval T that is a multiple of slot time \( \sigma \) (i.e. \( T = N \times \sigma \)). We define the jammer rate R as:

\[ R = \frac{\text{the number of emitted pulses in } T}{\text{the number of time slots in } T \text{ (i.e. } N)} = \frac{N_{\text{jam}}}{N} \]

Based on the jammer rate, if we consider a time interval T, we can define the probability that the jammer emits a pulse in a specific time slot as:

\[ P_{\text{jam}} = R \exp \left( (R-1)/T \right) \]

where \( R \in [0, 1] \). For \( R = 1 \) we have \( P_{\text{jam}} = 1 \). In the case of single node jamming, the received jamming interference will be multiplied by jamming probability. Hence, the channel capacity given in (4) will change to:

\[ C = B \log_2 \left( 1 + \frac{P}{\rho + P_{\text{jam}} \times Q \times d_r^\alpha} \right) \]

Thus, \( S_{\text{max}} \) in (11) becomes:

\[ S_{\text{max}} = \frac{PL}{(T_0 + \frac{\text{MAC}_{\text{idle}} + \text{AC}K + L}{B \log_2 (1 + \frac{\text{MAC}_{\text{idle}} + \text{AC}K + L}{\rho + P_{\text{jam}} \times Q \times d_r^\alpha})}) + \sigma K + T_c (K(-1 + \exp \frac{K}{\delta})). - 1} \]

2) Jamming multiple nodes:

### IV. Performance Analysis

In order to evaluate the performances of wireless networks under jamming according to the proposed models, we conduct simulations with ns-3 network simulator [10]. In addition to the achieved throughput, we are interested in measuring the PDR, the RSS and the consumed energy at each node. In all scenarios, we consider a network of 50 nodes. For a single node jamming and multiple nodes jamming with different distances, nodes are placed on a circle surrounding the AP. However, for multiple nodes jamming with equal distances, the AP is the center of a sphere to which all nodes belong. The safe (i.e., not jammed) nodes belong to a circle surrounding the AP on the plane. The jammed nodes belong to the intersection of the sphere with a plane parallel to the one containing the AP and the safe nodes. Fig. 1 presents a network configuration adopted for simulations. We use the same transmission power for all nodes including the jammer. In order to make sure that the jamming concerns only the desired jammed nodes, the jammer is placed sufficiently far from the other nodes. The parameters used in the simulations are presented in tables I and II. In each scenario, the simulation time is set to 100 s.
Fig. 2: Throughput achieved for a transmission rate of 36Mbps using OFDM technique with a jamming rate equal to 0.5

Fig. 3: PDR for a transmission rate of 11Mbps using DSSS with a jamming rate equal to 0.5

Fig. 4: PDR for different transmission rates with a jamming rate equal to 1

Fig. 5: Throughput of a jammed node achieved for a transmission rate of 1Mbps with different jamming rates

Fig. 6: Throughput of a node suffering from jamming attacks with an initial transmission rate of 1Mbps. For a continuous jamming, the PDR and the throughput are null when the distance between the jammer and the jammed node is small. Indeed, when the jamming rate is equal to 0.1, the PDR and the throughput are much higher than those achieved with a jamming rate equal to 0.5 or to 1. This is an expected result because a high jamming rate increases the received jamming interference power.

Fig. 6 shows the measured RSS in a network with a transmission rate of 18Mbps. The continuous jamming in this scenario starts at time 0s. When a small distance separates the jammer from the jammed node, the RSS of the latter is higher than all the other nodes. In fact, the jammer sends strong signals to the jammed node attempting to prevent it from any communication with the other nodes. So, the stronger the jamming signals are, the more the probability to destroy the received legitimate signals is high. When the distance to the jammer becomes higher, we observe that RSS of safe nodes is more important than that of the jammed node. Indeed, weakness of the signal strength measured at the jammed node has two reasons: a) weakness of the received signals from the jammer because of fading; b) long distances to the safe nodes.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings.
Fig. 6: RSS for a transmission rate of 18Mbps using OFDM under continuous jamming

The study of the impact of the distance between the jammer and the jammed nodes constitutes another key element that distinguishes our work from other works in the literature such as [6].

To study the effect of jamming on the energy consumption, we consider a network of 10 jammed nodes equidistant to the jammer and 40 safe nodes. Fig. 7 compares the effect of different jamming rates on the consumed energy for nodes using a transmission rate of 54Mbps. For a jamming rate equal to 1, nodes consume very less energy. This is because when the jammer starts its activity, communication in the network decreases: nodes transmit less often and hence their energy consumption is saved. However, for a jamming rate equal to 0.1 the curve inclination remains practically unchanged while it slightly decreases in the case of a jamming rate equal to 0.5. With small jamming rates, jamming interferences are weak which increase the communication between the legitimate nodes and hence increases the energy consumption. Fig. 8 represents the energy consumption for 5 transmission rates with a continuous jamming. After jamming starts, the energy consumption decreases severely except for 1Mbps. From these observations, we deduce that energy consumption depends on transmission time more than any other factor such as transmission rate.

V. CONCLUSION AND FUTURE WORK

In this paper, we presented an analytical model that evaluates the performance of a wireless network exposed to jamming attacks. We studied the behavior of the network under different scenarios namely single node jamming, multiple nodes jamming with equal distances to the jammer and multiple nodes jamming with different distances between the jammer and the jammed nodes. Simulation results show that the considered performance metrics depend strongly on the jamming interferences power. The throughput degrades in the same manner described in our formulas which proves the accuracy of the proposed model. Currently, we are studying some counterattack measures (such as mobility and sacrifice of particular nodes, etc.) that would help to improve networks’ resiliency against jamming.

REFERENCES