FACTA UNIVERSITATIS (NIŠ)
SERIES: ELECTRONICS AND ENERGETICS VOL.13, NO.1, APRIL 2000, 39–49

PERFORMANCE OF THE IEEE 802.11 WIRELESS LANs AND INFLUENCE OF HIDDEN TERMINALS

Zoran Hadži-Velkov and Liljana Gavrilovska

Abstract. Performance of the MAC protocol for the IEEE 802.11 Wireless LANs is examined with respect to the "hidden terminal" problem. Only the ad hoc portion of the wireless network, with stations generating time - insensitive asynchronous data traffic, is considered. The simulation results have clearly shown that "hidden terminals" introduce significant impact on network performance, especially on maximum achievable throughput and delay at moderate loads. With Pareto distributed packet traffic, different level of source burstiness seems to have no considerable influence over the throughput and the delay because of the station queues acting as traffic equalizers.

Key words: IEE 802.11, "hiden terminal effect", Pareto distribution, mobile communication.

1. Introduction

The enormous growth of public mobile communications and the tendency to provide similar wireless services in indoor environment reflects on the activities in the area of wideband wireless local access, and Wireless Local Area Networks (WLAN) architectures and protocols [1]. The IEEE 802.11 WLAN standard has been developed to provide high bandwidth to mobile users in a short-range indoor environment [2]. Apart from mobility, it should provide some QoS guarantees, for certain set of services. However, it has been an uneasy task to accomplish due to unreliable physical medium and several other specific effects, most important of which is the "hidden terminal" problem. There have been certain number of papers dealing with

Manuscript received February 23, 2000. A version of this paper was presented at the fourth IEEE Conference on Telecommunications in Modern Satellite, Cables and Broadcasting Services, TELSIKS'99, October 1999, Niš, Serbia.

Authors are with Institute of Telecommunication at Faculty of Electrical Engineering in Skopje Macedonia, Karpos 2 b.b. Skopje 1000, e-mails are `[zoranhv; ljiljana]@cerera.etf.ukim.edu.mk`.

performance evaluation of the IEEE 802.11 networks [3-6]. In this paper, we evaluate throughput and delay characteristics of the MAC protocol of the IEEE 802.11 WLAN system by taking the *"hidden terminal"* problem into consideration.

The paper is organized as follows. Section II gives a brief overview of the IEEE 802.11 specification. In the next section, the simulation scenario and utilized traffic and "hidden terminal" are described. The evaluation results are presented in section IV. Finally, we provide our discussion and conclusions in the fifth section.

2. IEEE 802.11 WLAN Spec Overview

2.1. Network architecture

The stations within the WLAN are organized into distinct cells referred to as basic service areas. All stations belonging to same service area form a *basic service set (BSS)*. They can communicate directly among each other in a virtual fully meshed architecture, forming an *ad-hoc* network. The stations from different BSSs can communicate among each other through centralized *Access Points (AP)*, provided within each BSS. APs are interconnected through the common *Distribution System (DS)*. The DS is actually an infrastructure backbone network, which is implementation-independent, and usually is a legacy network with one or more gateways to the outside Internet (Fig. 1). In our simulation model, only single BSS is considered.

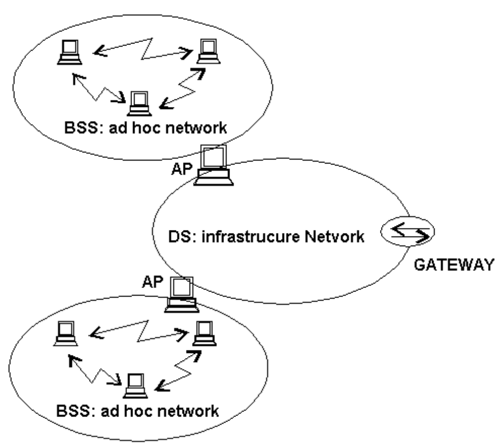


Fig. 1. IEEE 802.11 Wireless LAN architecture.

2.2 Physical layer

The physical layer at the radio-interface supports three different coding techniques: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared (IR). Our model considers DSSS coding with a DSSS preamble (144 bit) and a DSSS header (48 bits).

2.3 Medium access control

The stations within the WLAN can operate in the contention mode or alternate between the contention and the *contention-free mode* in order to provide both asynchronous (i.e. time-insensitive) and synchronous (i.e. time-sensitive) services. The contention-free mode is implemented optionally by the *Point Coordination Function (PCF)* and utilizes polling access mechanism. The mandatory *Distributed Coordination Function (DCF)* uses a random access method, which controls the contention for the channel of each station. The DCF provides services on a best effort basis in the ad-hoc network environment (i.e. within a single BSS).

2.4 Distributed coordination function

The DCF is based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol, enhanced by the use of the Network Allocation Vector (NAV) timer, which reduces the probability of "hidden terminal" occurrences. The NAV timer in each station indicates the time that must elapse before the currently transmitting station concludes its frame transmission. Upon its expiry and after sensing the channel to be idle for a DIFS period, a station can try to seize the medium by commencing transmission of a new or retransmission of a previously collided frame. The frame duration is announced by the transmitting station so other stations can update their NAV timers.

A station is unable to detect the collisions until it transmits its entire frame because of the nature of the air channel. If the generated data frames have extensive length, the collisions waste a lot of bandwidth inefficiently. In order to increase bandwidth efficiency, there is an alternative mechanism, referred to as *RTS/CTS handshaking* (Fig. 2), which is implemented by the Request to Send (RTS) and Clear to Send (CTS) control frames. The RTS/CTS handshaking mechanism is used when the length of packets, delivered from the upper layers to the MAC sublayer, exceeds a predefined *RTS_Threshold value*. If the collision has not occurred during handshaking, the source station will have successful transmission of its data frame.

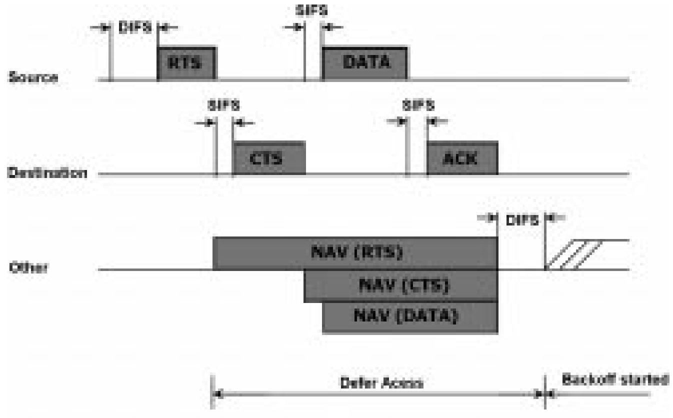


Fig. 2. Transmission of data frame using RTS/CTS handshake

The packets delivered from the upper layers are fragmented when the *Fragmentation_Threshold* value is reached. The lengths of resulting frames, except for the last one, are equal to Fragmentation_Threshold parameter. The RTS/CTS handshaking is used for the first fragment only.

Binary exponential backoff procedure (i.e. Collision Avoidance) ensures stability of network under heavy load conditions. If the station initially senses the channel to be busy, it waits for a DIFS period and then computes a random backoff time in the range between 0 and 7 Slot Times. The idle period after the DIFS interval is actually the *contention window (CW)*. After medium becomes idle, the station starts to decrement its backoff timer. If another station occupies the channel during the timer decrementation, it is temporarily freezed. When it reaches zero, the frame is transmitted. After the $i-th$ retransmission, a random integer number of slots between 0 and $(2^{2+i}-1)$ is chosen. After a certain number of retransmissions (i.e. *Retry_Limit*), the packet is dropped from the queue and the station contends for the access of a new frame as if the dropped one has been successfully transmitted.

3. System Model

3.1 Simulation scenario and performance measures

Our system utilizes the behavior of the IEEE 802.11 WLAN within single Basic Service Set (BSS). The BSS consists of 10 stations, which is a reasonable size of the wireless ad-hoc network. Each station performs access to the network using the Distributed Coordination Functionality only. Due to assumed short distances between the stations within the BSS, collisions can occur only because of simultaneous start of transmission of multiple stations, and not because of the propagation delay. The default channel transmission rate is 1 Mbps.

The queue between the upper layer and the MAC sublayer in each station (also referred to as the station queue) has limited length of 300 packets, although it can be arbitrary chosen in order to estimate its effect on the performance.

Binary exponential backoff algorithm is based on two parameters defining the maximum number of retransmissions before discarding the packet from its station queue: *Short_Retry_Limit* and *Long_Retry_Limit*. Actually, the number of retransmissions are equal to the Short_Retry_Limit unless the packet size is larger then RTS_Threshold, when they are limited to the Long_Retry_Limit value. Both parameters are adequately chosen to ensure that almost all the packets are delivered to the destination and to minimize their influence on the delay.

The parameters and its default values relevant for the system model are presented in Table 1.

Table 1. Relevant system parameters

PARAMETER	DEFAULT VALUE
Channel Rate	1 Mbps
MAC header length	34 octets
ACK length	14 octets
SIFS_Time	20 μs
DIFS_Time	50 μs
Slot_Time	10 μs
Station queue length	300 packets
Fragmentation_Threshold	800 octets
RTS_Threshold	200 octets
Short_Retry_Limit	5
Long_Retry_Limit	7

All the performance measures are observed in function of the offered load, which is defined to be the average number of bits per second submitted from the upper layers to station queues in all the stations. The observed performance measures are defined as follows. *Throughput* is the average number of successfully transmitted bits per second. *Delay* is defined to be the elapsed time between the moments of packet arrival at the station queue and positive acknowledgment reception for the corresponding frame, averaged over all successfully transmitted frames.

3.2 Traffic modeling

Because only the random access scheme is implemented, all the stations are assumed to generate delay-insensitive data traffic. While the traditional traffic-generating models (like the *Poisson* arrival process) are correlated over limited timescales (i.e. bursty over very limited timescales), real network traffic seems to be *self-similar*, i.e. long-range dependent [9] - [12]. The primary manifestation of such traffic is its burstiness over wide range of timescales. To produce such a behavior, the corresponding model should inevitably employ heavy-tailed distributions with infinite variance. The *Pareto* distribution is such a distribution with heavy tail and strong burstiness.

We used both the Poisson and the Pareto-distributed traffic generation models in order to compare their impact on the network performance.

The first approach implements the Poisson traffic model, which assumes the packet inter-arrival times from the upper layers to the station queue to be exponentially distributed with average arrival rate of λ packets per second.

Within the second model, the packet interarrival times are independent and identically distributed according to the infinite-variance Pareto distribution, determined by the *shape* parameter α $(1 \leq \alpha \leq 2)$ and *cut-off* parameter k $(t \geq k)$. Its integral distribution function is defined as follows

$$F_T(t) = P(T \leq t) = 1 - \left(\frac{k}{\alpha}\right)^{\alpha}, \quad k, \alpha \geq 0 \tag{1}$$

The average packet generation rate in each station is λ packets per second. The burstiness of each source is controlled by the shape parameter α. Modification of these two parameters implicitly alters the cut-off parameter due to the following relation

$$\lambda = \frac{\alpha - 1}{\alpha \cdot k} \tag{2}$$

All the stations are assumed to introduce identical load to the network, namely λ. Their sum actually represents previously defined total *offered load.* Therefore, the offered load in the network is controlled by the parameter λ.

The packet lengths are distributed according to the truncated geometric distribution. Truncation occurs at maximum packet length specified by the standard, i.e. 2312 octets. Average packet length is set to 1000 octets.

3.3 "Hidden Terminal" effect modeling

The "hidden terminals" are introduced by stochastically modeling their occurrences. We suppose one station can become a "hidden terminal" of another with probability P_h [4]. The reason to use the stochastic approach is to represent the user's mobility and channel dynamics adequately. The "hidden terminal" occurrence at some destination is evaluated before each frame is sent to it. If a particular station happens to be under influence of "hidden terminal" (occurring with probability P_h), the frames sent to it, by all the transmitting stations, will be lost and must be retransmitted.

4. Simulation Results

The evaluation results are presented in the following section. "Hidden terminals" are addressed by introducing different "hidden terminal" occurrence probabilities, P_h: 0 (no "hidden terminals"), 0.05, 0.1 and 0.2. P_h probabilities above 20% are not reasonable in indoor environments with relatively limited distances among stations, corresponding also to our previous assumption about the propagation delay.

4.1 Effects on throughput

In case of Pareto distributed traffic model, maximum achievable throughput of the shared channel excluding the influence of the "hidden terminal" ($P_h = 0$) is evaluated to be 74%. This value is reached at offered load of about 0.85 Mbps and remains unchanged for relatively high offered loads (Fig. 3). Such throughput stability is result of the implementation of the Binary Exponential Backoff procedure.

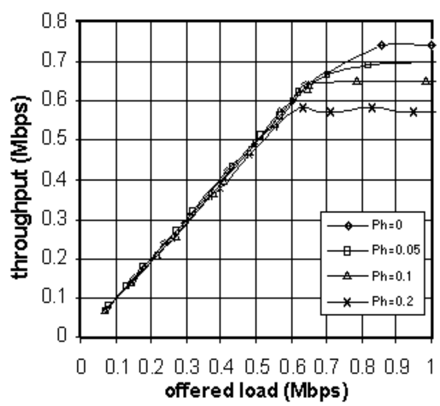


Fig. 3. "Hidden terminal" influence on throughput.

Increasing the "hidden terminal" probability reduces the maximum achievable throughput; for $P_h = 0.05$, 0.1 and 0.2, it is estimated to be 70%, 65% and 58%, respectively. Namely, "hidden terminal" occurrence introduces increased number of retransmissions, as well as the increased number of dropped packets from the station queue in each station due to reached Retry_Limit thresholds.

However, our simulation has shown that the throughput is insensitive to different level of source burstiness, i.e. the Fig. 3 remains unchanged for different values of the shape parameter, α. In addition, the curves corresponding to the Poisson traffic model are very similar, i.e. maximum achievable throughput is $1-3\%$ lower for each corresponding P_h. Actually, the station queue in each station equalizes the throughput for moderate and high traffic loads. At low loads, the curves also coincide because there are almost no collisions what so ever.

4.2 Effects on delay

It is evident from Fig. 4 that delay increases dramatically as the maximum throughput is reached. For relatively low throughput, that is at low offered load, delay is estimated to be several tens of milliseconds. For example, at throughput of 40% (corresponding to the offered load of 0.4 Mbps), under "no hidden terminal" assumption ($P_h = 0$), the estimated delay is 24 ms. As the throughput reaches its upper ceiling, delay dramatically increases up to intolerable 16 seconds ($P_h = 0$). Under such conditions, the station queues are fully occupied and the rest of the packets are being dropped. This value would continue to rise with offered load if the station queues were enlarged. Fig. 4 is almost identical for both traffic models.

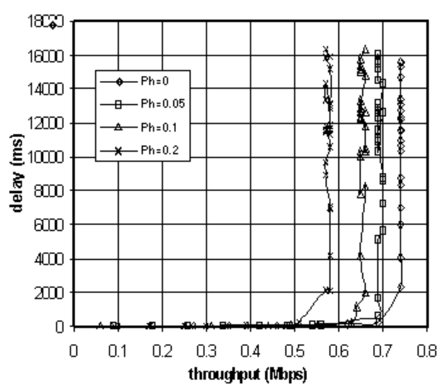
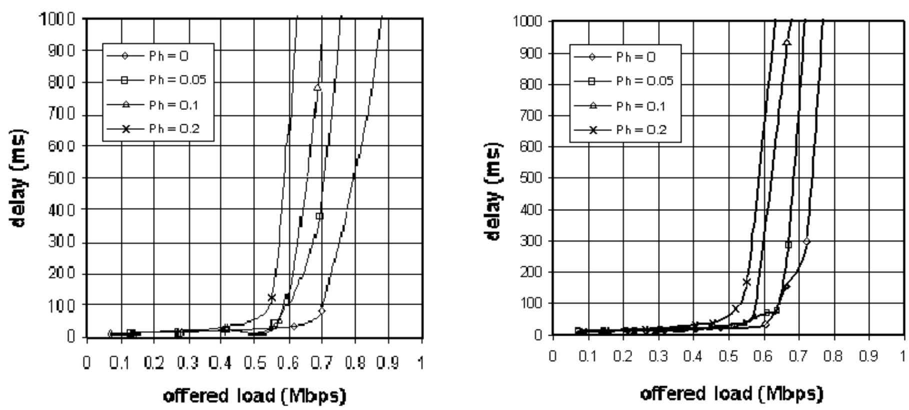


Fig. 4. Delay versus throughput

However, influence of both the "hidden terminals" and the implemented traffic model is obvious at loads between 0.5 and 1 Mbps. For example, at

0.7 Mbps, the delay is estimated to be 200 ms, 800 ms, 1400 ms and 2000 ms for $P_h = 0$, 0.05, 0.1 and 0.2, respectively if the sources utilize Pareto distributed packet interarrival times with $\alpha = 1.5$ (Fig. 5a). For Poison-like traffic, the delay is 90 ms, 380 ms, 790 ms and 2000 ms respectively for all P_h (Fig. 5b). Bursty traffic (originating from the Pareto model) causes increased delay for lower values of P_h. As P_h rises, source burstiness is suppressed by "hidden terminal" impact.

Regarding the different levels of source burstiness (controlled by the shape parameter α), the delay exhibits robustness for low and high loads, same as with the throughput. Under high loads, the station queues are overwhelmed with traffic so that both the effects of "hidden terminals" and source burstiness are of secondary importance. At low loads, there are almost no collisions so the curves also coincide.



a) *b)*

Fig. 5. "Hidden Terminal" impact on delay at moderate loads:
a) traffic distributed according to Pareto distribution;
b) traffic as a Poisson process.

However, under loads between 0.5 Mbps and 1 Mbps, increased α (in the range between 1 and 2), meaning reduced burstiness, reduces delay as depicted on Fig. 6. We conceive that increased source burstiness causes increased number of collisions, which increases the delay as well. Clearly, this behavior is obvious in case of "no hidden terminal" assumption only, since as we increase P_h, "hidden terminal" occurrence masks the effect.

5. Conclusions

The evaluation results have clearly demonstrated that the "hidden ter-

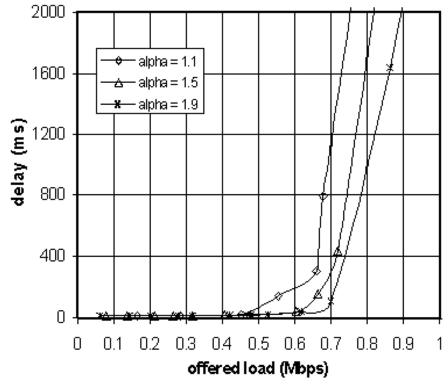


Fig. 6. Effects of source burstiness on delay at moderate loads.

minal" effect has negative impact on the overall network performance, especially on the maximum achievable throughput and the delay at moderate loads. The relatively simple CSMA/CD protocol suffers from many collisions at higher loads, generating dramatic increase in access delay as throughput capacity is slightly exceeded.

With Pareto distributed packet traffic, different level of source burstiness seems to have no considerable influence over the throughput because of the station queue acting as a *traffic equalizer*. This stand for the delay as well, except at moderate loads when the station queues are almost empty. The increased source burstiness increases the collision probability and therefore also the delay. The manifestation of this effect is suppressed as "hidden terminal" probability is increased.

Comparing the influence of two different traffic models, we conclude that all the performance measures at corresponding offered loads and P_h are almost identical within 1 – 3% boundary. Therefore, one can rightfully question justification for the use of more complex, i.e. self-similar traffic models [7], [8].

Regarding to our future endeavors in this field, it would be interesting to consider the impact of both "hidden terminals" and different traffic sources on other existing WLAN technologies, for example the second standardized WLAN, ETSI HIPERLAN Type 1. We also conceive that the influence of real air medium conditions over the performances of the WLAN would be significant [8].

REFERENCES

1. R.O. LaMaire et al.: *Wireless LANs and mobile networking: standards and future directions.* IEEE Communications Mag., vol. 34, no. 8, Aug. 1996, pp. 86-94.
2. IEEE Stds. Dept.: IEEE 802.11 D3: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* Jan. 1996.
3. K.C. Chen: *Medium access control of wireless LANs for mobile computing.* IEEE Network Mag., vol. 8, No. 5, Sept. 1994, pp. 50-63.
4. H. Kim et al.: *Performance analysis of MAC protocols for wireless LAN in Rayleigh and shadow fading channels.* Proc. GLOBECOM '97, Phoenix, Arizona, USA, 1997, pp. 404-408.
5. B. Crow et al.: *IEEE 802.11 wireless local area networks.* IEEE Communications Mag., vol. 35, no. 9, Sept. 1997, pp. 116-126.
6. G. Anastasi et. al.: *MAC protocols for wideband wireless local access: evolution toward wireless ATM.* IEEE Pers. Commun. Mag., Oct. 1998, pp. 53-64.
7. Z. Hadzi-Velkov and L.Gavrilovska: *Performance of the IEEE 802.11 wireless LANs under influence of hidden terminals and Pareto distributed packet traffic.* Proc. ICPWC'99, Jaipur, India, 1999.
8. Z. Hadzi-Velkov and L. Gavrilovska: *Influence of burst noise channel and hidden terminals over the IEEE 802.11 wireless LANs.* Proc. VTC 1999 - Fall, Amsterdam, The Netherlands, Sept. 1999, pp. 2641-2645.
9. W. Willinger et al.: *Self-similarity through high variability: statistical analysis of ethernet LAN traffic at the source level.* IEEE/ACM Trans. Networking, vol.5, no. 1, Feb. 1997, pp. 71-86.
10. V. Paxson et al.: *Wide area traffic: the failure of poisson modeling.* IEEE/ACM Trans. Networking, vol.3, no. 3, Jun. 1995, pp. 226-244.
11. M. Taqqu et al.: *Proof of a fundamental result in self-similar traffic modeling.* Comp. Commun. Rev., vol. 27, 1997, pp. 5-23.
12. C. Matarasso: *On the generation of self-similar traffic.* ACTS Mobile Summit, Sorrento, Italy, 1999