

A New Approach for the Throughput Analysis of IEEE 802.11 in Networks with Hidden Terminals

Athanasia Tsertou, David I. Laurenson, John S. Thompson
Signals and Systems Group
School of Engineering and Electronics
The University of Edinburgh
EH9 3JL, Edinburgh, UK
Email: {a.tsertou, dave.laurenson, john.thompson}@ed.ac.uk

Abstract—The dominance of IEEE 802.11 in the area of single-hop wireless networks is self-evident and has been supported by both simulation results and analytical modeling. On the contrary, the question as to whether the Distributed Coordination Function (DCF) performs satisfactorily enough in multi-hop networks still remains open. In this paper, we aim to give an initial view of this by introducing an analytical framework for the evaluation of DCF in networks exhibiting hidden terminals. The accuracy of our model is determined by comparison with simulations.

Keywords : IEEE 802.11, DCF, saturation throughput, hidden terminal.

I. INTRODUCTION-RELATED WORK

In recent years there is growing interest in modeling the performance of ad hoc networks analytically. A milestone paper that set the basis for this research direction was [1]. The author develops a mathematically accurate model for calculating the throughput of IEEE 802.11 DCF under the assumption of a fully-connected network. The assumption of every terminal being within the transmission range of each other means that there are no hidden terminals in this analysis. When there is a transmission between a transmitter, T_x , and a receiver, R_x , all the nodes of the network that are inside the transmission range of R_x but cannot hear T_x are called hidden to T_x .

The problem of hidden terminals is a major issue in the performance of ad hoc networks. In order to prevent DATA packet collisions due to hidden nodes, IEEE 802.11 [2] supports the RTS/CTS mechanism. In this mode of DCF operation, a pair of small control packets, called RTS and CTS, are transmitted initially in order to avoid costly DATA packet collisions (for a detailed description of DCF we refer the reader to [2]). However, this scheme is not perfect. There are a number of papers, [3]–[6], that report cases when the RTS/CTS handshake fails to prevent the DATA packet corruption because of a collision. Reasons that are shown to be the cause of this problem are different transmission and carrier-sensing areas [3], [6], non-negligible propagation delay [4], node mobility [5], different transmission rates [6] for control packets (RTS/CTS) and DATA packet. However, as the recent paper [7] shows, there are cases when the RTS/CTS mechanism fails even under perfect channel conditions and zero mobility. [7] defines nodes that receive an RTS or a CTS packet, but cannot interpret it correctly because of another on-going transmission,

as masked nodes and uses a queueing-theoretic approach to evaluate their effect in the performance of a such a network.

Although there has been a considerable amount of research that provides sufficient analytical models for IEEE 802.11 in fully-connected networks, there is only a recent interest in multi-hop networks [8]–[12]. In particular, [8] takes into account the nodes that are hidden to T_x , but can be ‘heard’ from R_x and makes an interesting initial analysis of the problem. Furthermore, [9] introduces a modeling framework for multihop ad hoc networks, but concentrates on the impact of the PHY layer on the performance of the MAC layer. In addition, in [10] the authors define the ‘deferral set’ of neighbours that interfere with the T_x - R_x transmission (which are actually the one-hop plus the two-hop neighbours that want to communicate with the one-hop neighbours), and define the possible interferers (‘equivalent competitors’). Their main simplification is that the equivalent competitors should defer transmission for a certain time interval Δt when the T_x - R_x transmission is taking place. In our analysis it is clear that this is not entirely true, as the effect of the transmission of an interfering pair on an active transmission can vary and is dependent upon a) the relative position of the conflicting pairs and b) the relative time difference of their transmissions. Finally, the authors of [11] concentrate on enhancing the Markov chain presented in [1] by transforming it into a Semi-Markov Process which can model time between state transitions.

The paper is outlined as follows: In Section II we describe the problem of analysis of hidden terminals and present our model. In Section III we apply it to the RTS/CTS scheme and calculate saturation throughput. In Section IV we compare it to simulation results and in Section V we present our conclusions.

II. MOTIVATION-FRAMEWORK FOR THE ANALYSIS

In order to evaluate the performance of any MAC protocol in a multi-hop environment, an accurate analysis of the effect of hidden terminals is mandatory. The slotted model used in [1] is based on a simple equation for the conditional collision probability

$$p = 1 - (1 - \tau)^{n-1}. \quad (1)$$

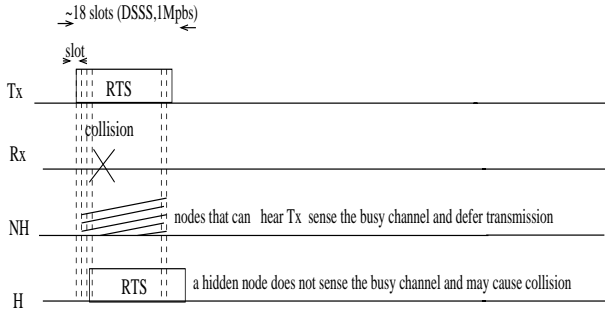


Fig. 1. Collision of RTS due to hidden terminal.

This equation implies that the transmitted packet collides if at least one of the $n - 1$ one-hop neighbours of the transmitter transmits in the same slot. Note that τ is the probability that a station transmits in a given time-slot. In a fully-connected network this is accurate, because the critical period during which a collision may occur is the period $\text{Propagation_Delay} + \text{aCCATime}^1 + \text{R}_x\text{-T}_x\text{-Turnaround_Time}$, in other words the duration of the time-slot σ . One cannot claim the same for a situation where there is a terminal hidden to T_x . In Fig. 1 the RTS packet that is sent by T_x may collide in any of the slots during which RTS is being transmitted, so (1) is not valid, even if we substitute $n - 1$ with the appropriate sum of immediate neighbours and hidden nodes.

In order to address this problem we propose the following model which is novel in that it enumerates all the possible ways in which two communicating pairs can interact for the contention of the wireless medium. In particular, we assume that there is a $\text{T}_x\text{-R}_x$ pair that starts an RTS/CTS/DATA/ACK handshake at time $t = 0$. This communication can be disturbed in several ways by another communicating pair ('interfering pair', hereafter referred to as IP). The effect depends on both the relative location of $\text{T}_x\text{-R}_x$ and the IP and also on the relative time difference of their handshakes. Moreover, we consider a time-window that extends one RTS/CTS/DATA/ACK transmission duration before and after the moment that T_x started sending the RTS control packet to R_x (i.e. $t = 0$). At any time during this time-window the interferers can initiate their transmission and influence (or not) the correct reception of DATA from R_x . The system is assumed to be in steady-state.

To make our analysis tractable, we assume that for each case considered only one IP that causes collisions to $\text{T}_x\text{-R}_x$ can exist. Moreover, we ignore channel capture, as do the majority of research papers. Other usual assumptions are the free-space model, zero propagation delay and the lack of network terminal mobility. We would also like to stress that the analysis presented in this paper takes the RTS/CTS scheme as a case-study but the methodology could be used to evaluate other CSMA/CA MAC schemes as well.

¹physical carrier sense requires aCCATime to determine the channel state.

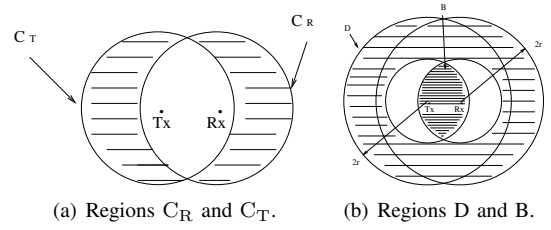


Fig. 2. All the possible interferers of $\text{T}_x\text{-R}_x$ transmission pair.

III. APPLICATION OF THE MODEL TO RTS/CTS SCHEME

The impact on the $\text{T}_x\text{-R}_x$ handshake of the fact that an IP initiates transmission within the 'time-window' can be classified as follows :

— **Success:** In this situation, the handshake between $\text{T}_x\text{-R}_x$ is not affected by the interferers, the DATA packet can be delivered to R_x without errors and the communication is completed at time $\text{RTS} + \text{SIFS} + \text{CTS} + \text{SIFS} + \text{DATA} + \text{SIFS} + \text{ACK}$.

— **Control Packet Collision:** This state happens in the case that T_x does not get a response (CTS) within CTS_Timeout after it finished transmitting the RTS packet. This may be caused by a collision between T_x 's RTS and another control or DATA packet, or because R_x has adjusted its Navigation Vector (NAV) [2] before it received the RTS. In this situation, after the expiration of CTS_Timeout , T_x goes into backoff.

— **Data Packet Collision:** As we mentioned in I, there are certain cases, even under perfect channel conditions, where the RTS/CTS scheme fails and the DATA packet that follows collides with another transmitted packet. In such a case T_x senses that its DATA packet was not successfully sent only after $\text{DATA} + \text{ACK_Timeout}$ from the moment it started the DATA packet transmission. Thus this collision incurs a high penalty.

— **Defer:** In this last case, even though a packet from upper network layers of the T_x requests access to the MAC layer and, ultimately, an RTS should be sent at $t = 0$, T_x refrains from sending that RTS because it either senses the channel busy or it has already adjusted its NAV because of a transmission it has already 'heard'. Thus, even though there is no RTS transmission, this case influences the node throughput as the DATA packet remains in the buffer and its transmission is delayed.

Note that although we present all the above states for the analysis to be compound and detailed, the states Control Packet Collision and Data Packet Collision will be explicitly used for the calculation of the collision probability.

A. Space-Domain Analysis

Fig. 2 shows areas of consideration in the analysis. The set of nodes C_R (C_T) consists of the one-hop neighbours of R_x (T_x) that are hidden to T_x (R_x). The set of nodes D includes all two-hop neighbours of R_x , which cannot 'hear' T_x in addition to the two-hop neighbours of T_x , which cannot be 'heard' by R_x . Finally, there is the set of nodes that are 'heard' by both T_x and R_x (the only interferers one would

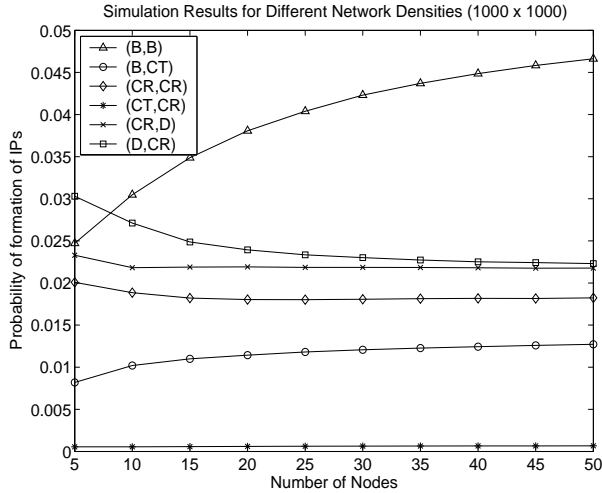


Fig. 3. Probability of formation of interfering pairs for different network densities.

have in a fully-connected network), to which we will refer as set B. If the distribution of source and destination nodes can be expressed analytically², then one can derive analytical expressions for the sets C_R , C_T , D and B. Otherwise, they have to be found through Monte-Carlo simulations, which is the method we used in this paper. The results of the Monte-Carlo simulations (see Fig. 3) show that the probability of formation of pairs like (C_R, D) or (B, C_T) (actually all of the possible pairs apart from (C_R, C_T)) is of the same order of magnitude as the probability of formation of pairs (B, B) which are the interferers in a fully-connected network. Note that the symbol (X, Y) represents an IP whose transmitter belongs to the set X and whose receiver belongs to the set Y.

B. Time Domain Analysis

The analysis that follows supposes that a transmission between T_x and R_x starts with an RTS packet at time $t = 0$. Also, a units of time before or after the first byte of this RTS packet is sent, the first byte of the RTS packet of the ‘interferer’ is sent. The reason behind the use of both positive and negative values of a has to do with symmetry. The fact that we ‘discriminate’ between ‘proper T_x - R_x pairs’ and ‘IPs’ does not imply that there are communicating pairs which we neglect in our analysis because we treat them as interferers. We should take into account both T_x - R_x pairs and interferers, even if we do make such a categorisation in order to facilitate our analysis. The approach we followed was to consider each time only what is the influence on the T_x - R_x pair, but take into account negative and positive a values.

1) *General Case:* Because of space limitation we will not present the analysis for all possible IPs, but we will describe our methodology with the case study that the transmitter of

the IP belongs to the set C_R and the receiver to any of the sets C_T or B (the conclusions are the same for both types of receivers).

Case I: $a < -(RTS + SIFS + \sigma)$, **Defer**

In this case T_x would attempt to transmit its RTS after the first bytes from C_T ’s CTS have been received by its antenna. So, since it senses the channel busy it defers its transmission, see Fig. 4(a).

Case II: $-(RTS + SIFS + \sigma) < a < 0$, **Control Packet Collision**

There are two possible collision cases with the same outcome. If $-(RTS + SIFS + \sigma) < a < -RTS$ then T_x starts transmitting RTS because it did not hear C_R ’s CTS, but R_x received C_R ’s RTS and adjusted its NAV, see Fig. 4(b). In other words, T_x will go into backoff after the expiration of CTS_Timeout. Also, if $a > -RTS$ the two RTS packets collide at both receivers R_x and C_T , so both transmitters will go into backoff.

Case III: $0 < a < RTS$, **Control Packet Collision**

The RTS packets collide at both receivers R_x and B, so the corresponding transmitters go into backoff after the expiration of the CTS_Timeout. The ‘winner’ of the contention will be randomly decided by the time they spend in backoff (Fig. 4(c)).

Case IV: $RTS < a < RTS + SIFS + \sigma$, **Data Packet Collision**

According to [2] physical carrier sense requires $aCCATime$ (about $15 \mu s$) in order to determine the channel state, which is longer than $aSIFSTime$ ($10 \mu s$). Thus, R_x does not have sufficient time to establish that C_R started sending an RTS, so it will send the CTS. Moreover, because of the relative size of the RTS and CTS control packets and since the RTS/CTS mechanism failed to inform node C_R of the other transmission, the latter’s RTS will corrupt the bytes of DATA at R_x , see Fig. 4(d). This event will not be noticed by the transmitter of DATA until it does not receive ACK. It is evident that this situation is very bandwidth-consuming. The above is true under the assumption of no capture.

Case V: $a > RTS + SIFS + \sigma$, **Success**

In this scenario, the first bytes of R_x ’s CTS have already reached C_R , so when a DATA packet from the upper layers arrives at the MAC layer, C_R is forced to defer this transmission as it senses the channel busy. After a while, it will receive the whole CTS, so it will adjust its NAV accordingly and it will not get to send RTS until after T_x - R_x ’s handshake has been terminated, see Fig.4(e).

All the other possible interactions were analyzed in a similar manner and the results of the analysis are summarised in Table I (note that $|a|$ is bounded by the transmission duration T_d). However, it is important to point out that when IP is (D, C_R) and $SIFS < a < RTS + CTS + SIFS$ special consideration is required as we will show in the analysis that follows.

2) *Special Case:* In this scenario, there is a collision of D’s RTS and R_x ’s CTS at C_R . Thus, D does not get a response from C_R and it goes into backoff. Meanwhile, T_x receives the CTS from R_x correctly and it starts the transmission of DATA packet. Depending on the size of DATA, the value of

² [10] provides an interesting analytical solution to a similar problem.

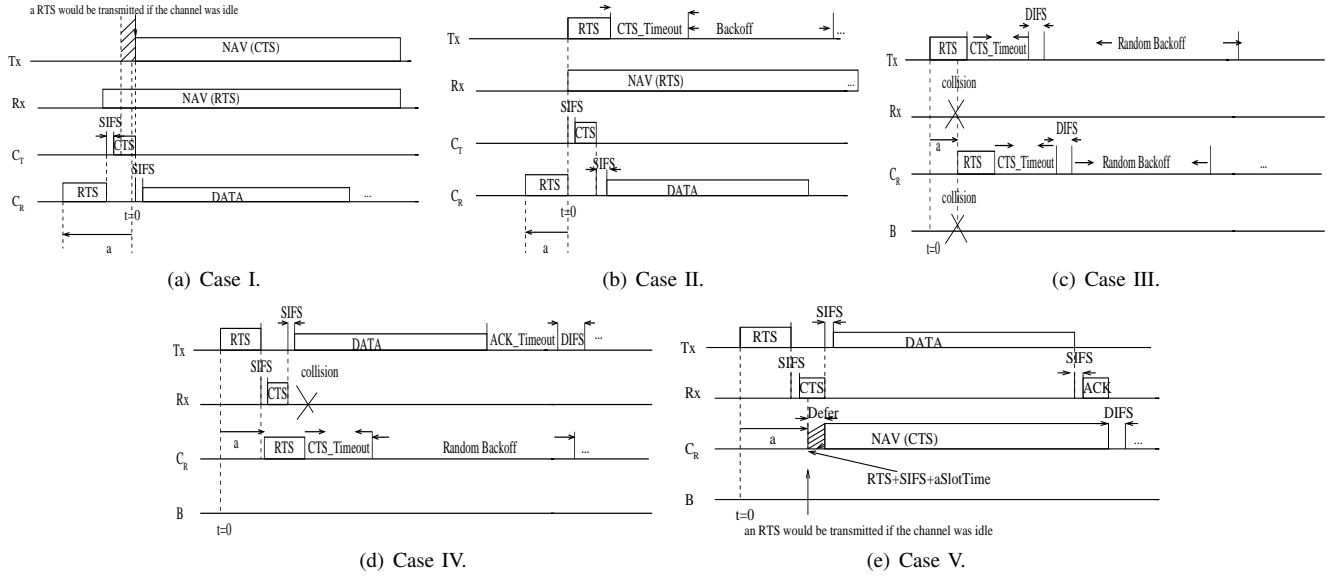


Fig. 4. Description of the analysis for the IP $(C_R, \{B, C_T\})$.

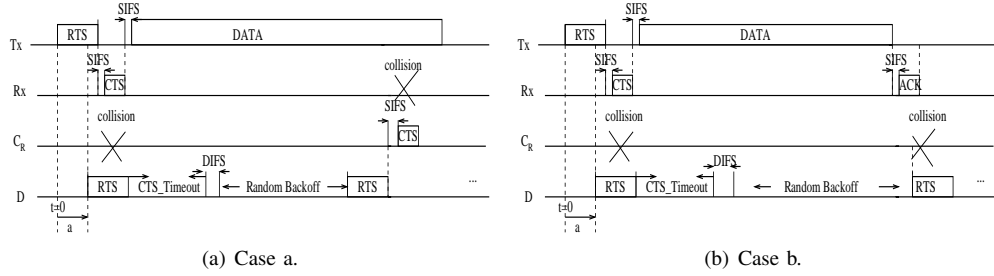


Fig. 5. Special Case: IP is (D, C_R) and $SIFS < a < RTS + CTS + SIFS$.

CTS_Timeout and the time which D will spend in backoff, we have two possible outcomes of the above situation. In the first (event E), D retransmits an RTS, which is correctly received by C_R , who responds by sending CTS. Because of the broadcast nature of the wireless medium, this CTS is also received at R_x , thus corrupting T_x 's DATA, see Fig. 5(a) (**Data Packet Collision**). In the other possible case (event \bar{E} , occurring with probability $P\{\bar{E}\} = 1 - P\{E\}$), illustrated in Fig. 5(b), the reception of DATA at R_x has finished before C_R transmits a CTS, so the handshake of T_x - R_x is successful (**Success**).

The probability of event E occurring can be calculated as follows: From Fig. 5(a) we have a DATA packet collision when $a + CTS_Timeout + RTS + Backoff < DATA + CTS + SIFS$. For abbreviation we define the constant $K \triangleq DATA + CTS + SIFS - CTS_Timeout - RTS$. We also define $u_{min} \triangleq SIFS$ and $u_{max} \triangleq RTS + CTS + SIFS$. The analysis that follows is based on the modeling of backoff mechanism with a two-dimensional Markov chain (for more details the reader should refer to [1], [13]). The probability that E occurs (conditioned on the fact that we are in this special case) is

$$P\{E\} = \sum_{i=0}^m \sum_{k=0}^{W_i-1} P\{E | \text{counter} = k, \text{stage} = i\} \cdot P\{\text{counter} = k, \text{stage} = i\}, \quad (2)$$

where m is the maximum backoff stage, W_i is the contention window at stage i and $P\{\text{counter} = k, \text{stage} = i\} = b_{i,k}$ as in [13]. The conditional probabilities of (2) are equal to:

$$\begin{cases} 1 & , \text{for } j < \frac{K - u_{max}}{\sigma}, j \in N \\ \frac{K - j \cdot \sigma - u_{min}}{u_{max} - u_{min}} & , \text{for } \frac{K - u_{max}}{\sigma} < j < \frac{K - u_{min}}{\sigma}, j \in N \\ 0 & , \text{for } j > \frac{K - u_{min}}{\sigma}, j \in N \end{cases} \quad (3)$$

In order to make the derivation of the above probabilities tractable we assumed that the counter is decremented at each time-slot without freezing.

C. Derivation of the transmission probability

The main difficulty in the performance analysis of a network with hidden terminals comes from the fact that (1) is not

IP	Success	Control Packet Collision	Data Packet Collision	Defer
$(C_R, \{C_T, B\})$	$a > \text{RTS} + \text{SIFS} + \sigma$	$-(\text{RTS} + \text{SIFS} + \sigma) < a < \text{RTS}$	$\text{RTS} < a < \text{RTS} + \text{SIFS} + \sigma$	$a < -(\text{RTS} + \text{SIFS} + \sigma)$
$(C_R, \{C_R, D\})$	$a > \text{RTS} + \text{SIFS} + \sigma$	$a < \text{RTS}$	$\text{RTS} < a < \text{RTS} + \text{SIFS} + \sigma$	-
(C_T, all)	$a > -\sigma$	-	-	$a < -\sigma$
(B, all)	$a > \sigma$	$-\sigma < a < \sigma$	-	$a < -\sigma$
(D, B)	$a > -\text{RTS}$	$-(\text{RTS} + \text{SIFS} + \sigma) < a < -\text{RTS}$	-	$a < -(\text{RTS} + \text{SIFS} + \sigma)$
(D, C_T)	$a > -(\text{RTS} + \text{SIFS} + \sigma)$	-	-	$a < -(\text{RTS} + \text{SIFS} + \sigma)$
(D, C_R)	$a > \text{RTS} + \text{CTS} + \text{SIFS}$	$a < -\text{SIFS}$	$\text{SIFS} < a < \text{RTS} + \text{CTS} + \text{SIFS}^*$	-

TABLE I
SUMMARY OF ALL POSSIBLE INTERACTIONS.

$$\tau = \frac{2(1-2p)(1-p^{R+1})}{(1-2p)(1-p^{R+1}) + W_0(1-(2p)^{m+1})(1-p) + W_0 2^m p^{m+1}(1-2p)(1-p^{R-m})} \quad (4)$$

valid. To the authors' knowledge, this observation is not taken into account by the researchers with the only exception of the recent paper [12]. A first, simplistic correction of (1) would be to claim that in order for the packet sent by T_x to be successfully delivered to R_x all one- and two-hop neighbours of T_x and R_x , say M , must defer any kind of transmission during a vulnerable period T_{vuln} (normalised to the time-slot). So, then (1) would take the form $p = 1 - (1 - \tau)^{M \cdot T_{vuln}}$.

However, as we showed previously, this would give a false estimation of the conditional collision probability, because the effect of an IP to the transmission between T_x and R_x varies according to the type of the IP and the factor a . In other words the vulnerable period is different for different interferers. We claim that the probability p that a transmitted packet encounters a collision is equal to

$$p = 1 - \prod_{j=1}^{15} (1 - \tau)^{t_j \cdot s_j}. \quad (5)$$

In (5) j is an index that shows the type of the IP, e.g. for (C_R, C_T) $j=1$, for (C_R, B) $j=2$, etc (j can take integer values up to 15, which are the different types of IPs). In addition, t_j is the normalised to the time-slot collision period for each IP (with reference to the columns Control Packet Collision and Data Packet Collision in Table I) and s_j is the number of the corresponding type of IPs. In other words, a transmitted packet encounters a collision when at least one of the IPs transmits at any of the corresponding time-slots shown by the cases Control Packet Collision and Data Packet Collision of Table I. We emphasize the fact that (2) and (5) are interdependent.

In order to find the transmission probability we refer to [1], [13]. To obtain an additional equation that relates p to τ we use, from [13], the equation (4), where W_0 is the initial contention window of the backoff mechanism, m is the maximum backoff stage and R is the Short Retry Limit defined in [2]. Consequently, we have a system of three non-linear equations (2), (4) and (5) which we solve using numerical methods and, thus, calculate the value of τ .

D. Derivation of the saturation throughput

Let L be the DATA packet length, which we assume to be constant. The saturation throughput S for a random

communication pair is according to the previous analysis

$$S = \frac{\tau \cdot (1-p) \cdot L}{\text{average time-slot}}. \quad (6)$$

The average duration of a time-slot is obtained as follows: If the transmitter sees an idle slot (with probability p_{id}) the duration of the time-slot is σ . In the opposite case (busy slot, with probability $1-p_{id}$), the duration is equal to $\text{RTS} + \text{EIFS}$ if T_x sees a collision, or to the whole transmission duration T_d , if it sees a successful transmission. In particular, for p_{id} we have:

$$p_{id} = (1 - \tau) \cdot \prod_{j_a} (1 - \tau)^{s_{j_a}} \cdot \prod_{j_b} (1 - \tau \cdot (1 - p_{co}))^{s_{j_b}}, \quad (7)$$

where the first term means that the node under consideration is not currently transmitting, the second term that the corresponding interferers do not send an RTS and the third that the corresponding interferers do not send a CTS. In particular, p_{co} is the probability of Control Packet Collision, j_a refers to the indexes of pairs whose transmitter is heard by the current T_x and j_b to those whose receiver is heard by T_x . The probability p_{co} is given by the formula:

$$p_{co} = 1 - \prod_{l=1}^{15} (1 - \tau)^{t_l \cdot s_l}, \quad (8)$$

where now l refers only to the column Control Packet Collision. Furthermore, the probability $p_{s,b}$ that the transmitter sees a successful slot, given that it sees a busy slot is

$$p_{s,b} = \frac{(\sum_{j_a} s_{j_a} + 1) \cdot \tau \cdot (1-p)}{1 - p_{id}}, \quad (9)$$

where a successful slot could occur because of its own transmission or because of a successful transmission of its one-hop neighbours. For the calculation of $p_{s,b}$ we assumed that, when the node under consideration is not transmitting, it observes a successful transmission if and only if its immediate neighbours are involved in a successful transmission. This is not entirely correct because T_x could successfully receive an

RTS or CTS from an immediate neighbour and accordingly adjust its NAV, even if that transmission is not successful in the end. Our future work will address this subtle issue. Consequently, the equation for the saturation throughput (6) takes the form:

$$S = \frac{\tau \cdot (1 - p) \cdot L}{p_{id}\sigma + (1 - p_{id}) \cdot \{p_{s,b}T_d + (1 - p_{s,b})(RTS + EIFS)\}} \quad (10)$$

IV. VALIDATION OF THE MODEL

In order to validate our model we compare it to simulation results we obtained using NS2. To eliminate the effect of routing we assume that the nodes have knowledge of the network topology, so they are able to send packets to their immediate neighbours without any kind of routing. For each number of nodes (5 to 50) we keep the network size constant (1000 m x 1000 m), the bandwidth 1Mbps (DSSS), the DATA length 512 bytes and we keep increasing the data packet rate until the point of saturation. At this rate, we measure the throughput. This procedure is repeated for 20 different network topologies for each number of nodes. Note that the maximum contention window is 1024, the Short Retry Limit is 7 as in [2], the values for CTS.Timeout and ACK.Timeout are 314 μs and for EIFS 364 μs as in NS2 [14].

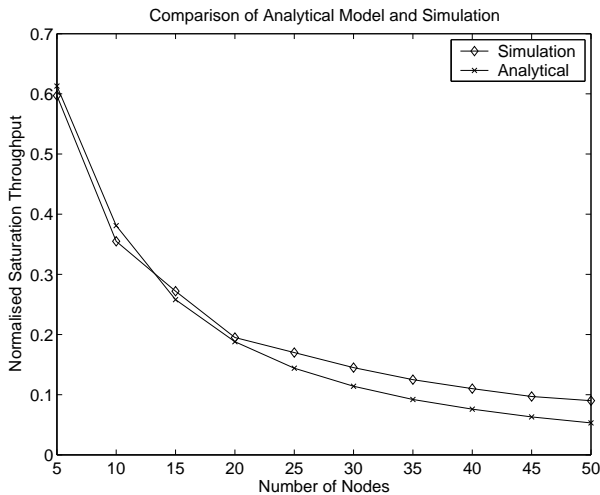


Fig. 6. Normalised saturation throughput for different network densities.

In Fig. 6 the normalised to the bandwidth saturation throughput is plotted for different network densities. As the network density increases, the throughput that each communication pair can achieve decreases due to the fact that each pair has to contend with more IPs for access to the channel. From the comparison of the analytical results to the simulation results we observe that our model is very consistent with the simulation results for low network densities. For more dense networks the analytical approach seems to underestimate the throughput by less than 5%. We believe that this is due to the

several assumptions we have made and, most importantly, due to the fact that for the analysis in Section III.B. we assumed that only one IP can exist.

V. CONCLUSIONS

In this paper we presented an analytical framework for the calculation of saturation throughput in networks exhibiting hidden terminals. Our case study was the RTS/CTS scheme of the IEEE 802.11 DCF but the model can also be used for other MAC schemes using CSMA/CA. The model is based on certain assumptions which we intend to relax in our future work. In spite of that, however, it is shown that it is fairly accurate by comparing it to simulation results.

REFERENCES

- [1] *Performance Analysis of the IEEE 802.11 Distributed Coordination Function*, **Giuseppe Bianchi**, in IEEE Journal on Selected Areas in Communications, vol 18, no.3, March 2000.
- [2] *ANSI/IEEE Std. 802.11-1999 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 1999.
- [3] *How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks?*, **Kaixin Xu, Mario Gerla and Sang Bae**, in IEEE GlobeCom, 2002.
- [4] *Floor Acquisition Multiple Access (FAMA) for packet-radio networks*, **Chane L. Fullmer and J.J Garcia-Luna Aceves**, in Proceedings of SIGCOMM '95, 1995.
- [5] *On the performance of a medium access control scheme for the re-configurable wireless networks*, **Zygmunt J. Haas**, in Proceedings of MILCOM '97, 1997.
- [6] *Analysis of the hidden terminal effect in multi-rate IEEE 802.11b networks*, **Mauro Borgo, Andrea Zanella, Paola Bisaglia and Simone Merlin**, in International Symposium of Wireless Personal Multimedia Communication WPMC 2004, September 2004.
- [7] *Evaluation of the Masked Node Problem in Ad-Hoc Wireless LANs*, **Saikat Ray, Jeffery B. Carruthers and David Starobinski**, accepted for publication in the IEEE Transactions on Mobile Computing, 2005.
- [8] *Modelling of Collision Avoidance Protocols in Single-Channel MultiHop Wireless Networks*, **Yu Wang and J.J. Garcia-Luna-Aceves**, in ACM WINET Journal, Special Issue on Modelling and Analysis of Mobile Networks, 2003.
- [9] *A Scalable Model for Channel Access Protocols in Multihop Ad Hoc Networks*, **Marcelo M. Carvalho and J.J. Garcia-Luna Aceves**, in Proc. ACM Mobicom 2004, September 2004.
- [10] *Theoretical channel capacity in multi-hop ad hoc networks*, **Yue Fang and Bruce McDonald**, in the 13th IEEE Workshop on Local and Metropolitan Area Networks, April 2004.
- [11] *Towards the Performance Analysis of IEEE 802.11 in Multi-hop Ad-Hoc Networks*, **Yawen D. Barowski and Saad Biaz**, in IEEE Wireless Communications and Networking Conference WCNC 2005, March 2005.
- [12] *MAC layer Performance Analysis of Multi-Hop Ad Hoc Networks*, **Farshid Alizadeh-Shabdiz and Suresh Subramaniam**, in IEEE GlobeCom, 2004.
- [13] *Performance of Reliable Transport Protocol over IEEE 802.11 Wireless LAN: Analysis and Enhancement*, **Haitao Wu, Yong Peng, Keping Long, Shiduan Cheng and Jian Ma**, in IEEE INFOCOM 2002, 2002.
- [14] *The Network Simulator -ns-2, release ns-2.1b9a*, in <http://www.isi.edu/nsnam/ns/>.