Contents lists available at SciVerse ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A joint solution for the hidden and exposed terminal problems in CSMA/CA wireless networks

Caishi Huang [a,*], Chin-Tau Lea [b], Albert Kai-Sun Wong [b]

[a] *University of Macau, Macao*

[b] *Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology, Hong Kong*

ARTICLE INFO

Article history:
Received 30 October 2011
Received in revised form 10 June 2012
Accepted 17 June 2012
Available online xxxx

Keywords:
Hidden terminal problem
Exposed terminal problem
CSMA/CA
Multihop
Medium access control (MAC)
Ad hoc networks

ABSTRACT

It is well-known that the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)-based wireless networks suffer seriously from the hidden terminal problem and the exposed terminal problem. So far, no satisfactory solutions that can resolve both problems simultaneously have been found. In this paper, we present a joint solution to the two problems. Our approach avoids the drawback of lessening one problem but aggregating the other. It is compatible with the IEEE 802.11 MAC and requires no protocol change. Analysis and simulations show that the proposed scheme can significantly reduce the hidden and exposed terminal problems. Not only it can significantly improve the throughput of the network and the fairness among different flows, it can also provide a much more stable link layer. In simulated scenarios under heavy traffic conditions, compared to the conventional IEEE 802.11 MAC, the new method can achieve up to 1.8 times gain in network throughput for single-hop flows and up to 2.6 times gain for multihop flows.

1. Introduction

The medium access control (MAC) protocol plays a key role in determining the delay, throughput, and fairness performance of a wireless LAN or an ad hoc network. It is well-known that the CSMA/CA protocol used by IEEE 802.11 suffers seriously from both hidden and exposed terminal problems inherent in a wireless environment [1,2]. The performance degradation becomes more severe in a multihop environment, and will be amplified by higher layer protocols [1]. A lot of research has been done addressing the two problems [2–12]. Often, these studies try to solve the problems separately. But there are two reasons why finding a joint solution is a better strategy. One is that a separate solution to one problem may aggravate the other. For example, setting a larger carrier sensing range (R_{cs}) can alleviate the hidden terminal problem. But this is done at the expense of heightening the exposed terminal problem [1,5]. The second reason for finding a joint solution is that sometimes a technique for solving a problem cannot be used unless the solution to the other problem is found. Take transmission power control as an example. Reducing transmission power can lessen the exposed terminal problem, but will aggravate the hidden terminal problem. But power control can still be a useful tool when it is jointly considered with other techniques for finding an overall solution to the two problems.

To the best of our knowledge, within the single-channel framework, there is currently no effective solution that can fully address both the hidden and exposed terminal problems simultaneously. In the paper, we propose a joint solution to the two problems. To solve the hidden terminal problem, the proposed technique exploits an important fact in digital communications: different transmission rates have different Signal to Interference and Noise Ratio (SINR) requirements and the received power thresholds (called receiver sensitivity), as shown in Table 1, and hence different transmission ranges (R_{tx}) and interference ranges

[*] Corresponding author.
E-mail addresses: cshuang@umac.mo (C. Huang), eelea@ece.ust.hk (C.-T. Lea), eealbert@ust.hk (A.K.-S. Wong).

1389-1286/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.comnet.2012.06.008

Table 1
802.11a/b/g specifications with Bit Error Rate $\leqslant 10^{-5}$ [14,15].

Transmission rate (Mbps)	Receiver sensitivity (P_{th}) (dBm)	SINR$_{th}$
54	−65	24.56
48	−66	24.05
36	−70	18.80
24	−74	17.04
18	−77	10.79
12	−79	9.03
11	−82	6.99
9	−81	7.78
6	−82	6.02
5.5	−87	5.98
2	−91	1.59
1	−94	−2.92

(R_I). This fact has often been ignored by previous studies related to the hidden/exposed terminal problems [1,2,5,6,13,14]. It is shown in the paper that for a given DATA packet transmission rate, the associated hidden terminals can be mostly removed by selecting an appropriate rate for sending RTS/CTS packets. Following this, we then propose a power control scheme to solve the exposed terminal problem. Although the two solutions seem independent, they are not. As explained later, the power control technique cannot work unless the hidden terminal problem is satisfactorily addressed. Through analysis and simulations, we show that the proposed joint solution can significantly reduce the hidden and exposed terminal problems and enhance the network throughput. Under heavy traffic conditions, the new approach can achieve up to 1.8 times throughput gain for single-hop flows and up to 2.6 times for multihop flows. The new approach can also significantly improve the degree of fairness in resource sharing among different network flows.

The rest of this paper is organized as follows: Section 2 reviews the related work. Section 3 presents the channel model. The solution to the hidden/exposed terminal problem is elaborated in Section 4. Section 5 discusses various simulation comparisons of the performance between the proposed scheme and 802.11 in terms of fairness and throughput via NS2-based simulations. Section 6 concludes the paper.

2. Related work

Much work has been done to address the hidden and exposed terminal problems. The focus of this paper is on single-channel solutions. Multiple-channel schemes have been proposed [13,14,17–21]. Regardless of their claimed effectiveness, cost is obviously an issue here because multiple communication channels and multiple transceivers on each node are required. The management of control channels, the collision resulting from contention in control channels, and the efficiency of using multiple channels are additional issues with these proposals. Because they are not relevant to our proposed single-channel scheme, our discussion below will not include multiple-channel approaches.

The IEEE 802.11 MAC and other existing single-channel schemes [2–8] rely on two kinds of techniques to address the hidden terminal problem: carrier sensing and RTS/CTS exchanges. Carrier sensing can prevent interferences at a receiver as long as the potential interfering stations can sense the radio signal from the transmitter (e.g. node C in Fig. 1a). But due to signal attenuation and transmission barriers (e.g. node D and node E respectively in Fig. 1a), a potential interferer may not detect the carrier. As a remedy, the RTS (Request To Send)/CTS (Clear To Send) handshake has been proposed [6]. The idea is based on the assumed symmetry between the transmission range and the interference range so that any terminal that can corrupt the reception would receive the CTS packet and any terminal that can corrupt the ACK would receive the RTS packet, as a result such terminals will refrain from transmitting. This technique avoids the dilemma that carrier sensing is to the sender while protection is to the receiver. But this technique still does not solve the hidden terminal problem [2] because even if a terminal is out of the transmission range, it can still be within the interference range (see Fig. 1b) and corrupt either DATA or ACK packet.

Many schemes have been proposed to improve the performance of carrier sensing and the RTS/CTS method for the hidden terminal problem. Refs. [4,5] suggest using an even larger carrier sensing range (see the two carrier sensing ranges R_{cs1} and R_{cs2} in Fig. 1a). This can only help to some extent and it does not work when transmission barriers are present. Besides, the cost of a much more severe exposed terminal problem outweighs the benefit. As the interference range varies with the transmitter–receiver distance, Ref. [2] proposes to shorten the communication distance to 0.56 times the transmission distance so that the CTS packet can cover the interference range at the receiver. But this proposal is based on a fixed SINR requirement, and it artificially reduces the effective transmission range, which is contrary to the practice of most routing protocols, like DSR and AODV, that aim to reach the farthest node and use it to relay traffic [22,23]. In FAMA [7], a node sensing any noise is required to defer its transmission long enough for a maximum-length data packet to be received. But this obviously creates unnecessarily deferred transmissions and exacerbates the exposed terminal problem. The methods mentioned above have a negative impact on network throughput and overlook the exposed terminal problem.

Recent studies in [24] have shown that exposed terminals are in fact much more prevalent than hidden terminals in WiFi jungles. Although the existing 802.11 MAC contains no effective methods to handle this problem, several approaches can be found in previous studies. MACA-P [9] introduces a control gap between the RTS/CTS exchange and the subsequent DATA/ACK exchange to enhance the probability that other communication pairs may conduct concurrent transmissions. Refs. [10,11] attempt to create more concurrent transmission opportunities via overhearing. However, the proposals from Refs. [9–11] apply to limited scenarios only and rely on the assumption that the interference range equals the transmission range, which does not hold true in reality. Refs. [25,26] suggest making the sensing threshold tunable to control the effective sens-

Please cite this article in press as: C. Huang et al., A joint solution for the hidden and exposed terminal problems in CSMA/CA wireless networks, Comput. Netw. (2012), http://dx.doi.org/10.1016/j.comnet.2012.06.008

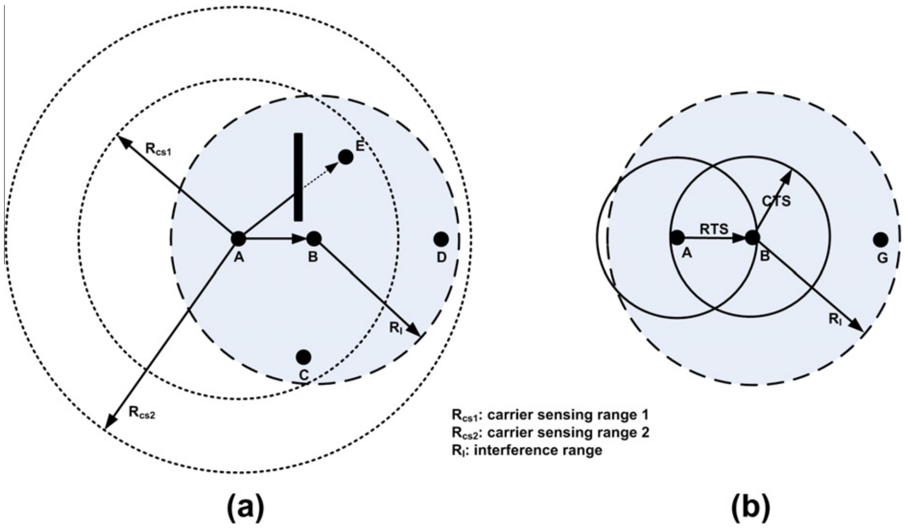

R_cs1
E
A
B
D
R_I
C
R_cs2
R_cs1: carrier sensing range 1
R_cs2: carrier sensing range 2
R_I: interference range
(a)
RTS
CTS
A
B
G
R_I
(b)

Fig. 1. (a) Carrier sensing mechanism with different carrier sensing ranges. (b) The RTS/CTS handshake.

ing range so that more concurrent transmissions can be achieved. But several issues are neglected in the discussion, such as the asymmetric link problem and the lack of an efficient algorithm to adjust the carrier sensing threshold, which will call into question the effectiveness of the scheme. Several other approaches suggest reducing the transmit power to shrink the reserved area for an ongoing transmission so that more concurrent transmissions are possible [27–29]. But the potential gain cannot be easily realized because it often aggravates the hidden terminal problem because of the asymmetric link problem [5,30]. There is also literature trying to avoid the aforementioned drawback when power control is employed [31,32], but they may see other problems. The above mentioned approaches only focus on the exposed terminal problem and ignore the impact on the hidden terminal problem. It is important to note that our approach also incorporates power control to tackle the exposed terminal problem. But we avoid the aforementioned drawback of power control by tackling the hidden and exposed terminal problems together.

There are also some studies trying to strike a good balance between the hidden and exposed terminal problem in term of network performance [33,34]. Ref. [33] argues that neither the hidden nor the exposed terminal problem can be eliminated and suggests maintaining a good balance between the two by adjusting the carrier sensing threshold and receiver sensitivity collectively. While [34] suggests the combination of adjusting the carrier sensing threshold and adaptively changing the transmission rate. However, neither of them is trying to fully solve the two problems and they only focus on WLAN.

3. Channel model

We assume a single channel environment, that is, all nodes are equipped with the same radio and the entire bandwidth forms one channel for resource sharing.

In real networks, the received power of a signal, affected by shadowing and small-scale fading, is a random variable. But in MAC layer analyses, the shadowing and fading effects are often ignored and a path loss model is used instead [2,4,5,35,36]. Let P_{r_jk} be the power received at user k for a signal sent by j, and P_{t_j} the transmit power of sender j. We have

$$P_{r\_jk} = G_{jk}P_{t\_j} \tag{1}$$

where G_{jk} is the channel gain between the sender j and the receiver k, and $G_{jk} = \beta/d_{jk}^{\alpha}$, β is the antenna gain coefficient, d_{jk} the distance between node j and node k, and α is the path loss coefficient. $G_{jk} = P_{r\_jk}/P_{t\_j}$, can be easily measured by the receiver if P_{t_j} is known. In practice, it is often assumed that the channel is reciprocal (i.e., $G_{jk} = G_{kj}$) and that G_{jk} is stationary for the duration of the control and data packet transmissions [5,19,20,28–30].

When interference is present, the total power detected by receiver k consists of the signal from the intended transmitter j, the interference from unexpected transmitters, and noise. The intended signal can be correctly decoded only if the received power is greater than the corresponding received power threshold (receiver sensitivity requirement), denoted by P_{th},

$$P_{r\_jk} \geqslant P_{th} \tag{2}$$

and the SINR is above a certain threshold (denoted by SINR$_{th}$),

$$\text{SINR} = \frac{P_{r\_jk}}{P_I + P_N} \geqslant \text{SINR}_{th} \tag{3}$$

where P_I is the cumulative interference power from multiple simultaneous transmitters $P_I = \sum_{i \neq j,k} P_{r\_ik}$, P_{r_ik} denotes the received power at node i, and P_N is the power of noise. Because carrier sensing is used in the network, the chance of multiple interferers transmitting simultaneously in the same vicinity is usually small. Thus a single interferer which is closest to the intended receiver is normally assumed in the analyses of [2,8,14,17,13,6]. The same is also assumed in our discussion. But our analysis can be easily extended to the case with multiple interferers as the effect of multiple interferers can be represented by a higher P_I at the receiver, a situation that is equivalent to the single interferer case with a higher SINR_{th} requirement for correct decoding. Currently, multirate transmission is a standard feature in wireless devices. Because different data rates generally imply different receiver sensitivity and SINR requirements (see Table 1), we use $P_{th}(\text{Rate}_m)$ and $\text{SINR}_{th}(\text{Rate}_m)$ to denote this dependency, where Rate denotes the data rate and m is the index of the data rates. Combining (1)–(3), we have the following equation:

$$\begin{cases} G_{jk}P_{t\_j} \geqslant P_{th}(\text{Rate}_m) \\ \frac{G_{jk}P_{t\_j}}{G_{ik}P_{t\_i}} \geqslant \text{SINR}_{th}(\text{Rate}_m) \end{cases} \tag{4}$$

4. Proposed solution to hidden/exposed terminal problems

Our joint solution to the hidden/exposed terminal problems is presented below. We first address the hidden terminal problem because the proposed solution to the exposed terminal problem hinges on the condition that a successful solution can be found for the hidden terminal problem.

4.1. Solution to the hidden terminal problem

Our proposed solution to the hidden terminal problem exploits the fact that the receiver sensitivity and SINR requirement are generally different at different transmission rates. In the proposed scheme, RTS/CTS control packets are used to eliminate the hidden terminal problem in the DATA/ACK packet transmissions, but are sent at a rate different from that for the DATA/ACK packets. It is shown below that by selecting the appropriate rate of RTS/CTS, the hidden terminal problem can be fully eliminated.

Let Rate_1 be used for RTS and CTS transmissions and Rate_2 for DATA and ACK transmissions. The notations for the receiver sensitivity and the SINR requirement of both transmission rates are given in Table 2. In the following, we will derive Rate_1 for a given Rate_2 in order to silence all the potential interferers. The following notations are used in our analysis.

- j: the sender,
- k: the receiver,
- i: a potential interferer,
- P_{r_jk}: the received power at receiver k sent from sender j,
- P_{r_ik}: the received power at receiver k sent from interferer i,
- P_{r_ki}: the received power at interferer i sent from receiver k,
- P_{t_i}: the transmit power from interferer $i, 0 < P_{t\_i} \leqslant P_{\max}$, where $P_{\max}$ denotes the maximum transmission power level allowed,
- P_{t_k}: the transmit power from receiver $k, 0 < P_{t\_k} \leqslant P_{\max}$.

Table 2
Specifications for Rate_1 and Rate_2.

Transmission rate	Receiver sensitivity (P_{th})	SINR_{th}
Rate_1	$P_{th}(\text{Rate}_1)$	$\text{SINR}_{th}(\text{Rate}_1)$
Rate_2	$P_{th}(\text{Rate}_2)$	$\text{SINR}_{th}(\text{Rate}_2)$

For receiver k to correctly decode a DATA packet sent by sender j, the SINR at the receiver side must satisfy

$$\text{SINR} = \frac{P_{r\_jk}}{P_{r\_ik} + P_N} \geqslant \text{SINR}_{th}(\text{Rate}_2) \tag{5}$$

Since P_N is negligible compared to either the signal or the interference [2,4,5], we can rewrite (5) as

$$P_{r\_ik} \leqslant \frac{P_{r\_jk}}{\text{SINR}_{th}(\text{Rate}_2)} \tag{6}$$

Besides, for correct decoding, P_{r_jk} should be not less than the received power threshold of Rate_2:

$$P_{r\_jk} \geqslant P_{th}(\text{Rate}_2) \tag{7}$$

As the channel is reciprocal, i.e., $G_{ik} = G_{ki}$, we have

$$P_{r\_ik} = \frac{P_{r\_ki}}{P_{t\_k}} P_{t\_i} \tag{8}$$

Combining (6) and (8), we have

$$\frac{P_{r\_jk}}{P_{r\_ki}} \frac{P_{t\_k}}{P_{t\_i}} \geqslant \text{SINR}_{th}(\text{Rate}_2) \tag{9}$$

The worst-case scenario for the hidden terminal problem happens when the interferer transmits with the maximum power, i.e. $P_{t\_i} = P_{\max}$, and the received power at the receiver side, shown in (7), is as low as $P_{r\_jk} = P_{th}(\text{Rate}_2)$, i.e., the receiver is located on the fringe of the transmission range of the sender. Substituting the worst case values of P_{t_i} and P_{r_jk} into (9), we observe that, P_{r_ki}, the received power at interferer i of the packet sent from receiver k, is not larger than the following:

$$P_{r\_ki} \leqslant \frac{P_{th}(\text{Rate}_2)}{\text{SINR}_{th}(\text{Rate}_2)} \frac{P_{t\_k}}{P_{\max}} \tag{10}$$

Meanwhile, if the following equation holds true, interferer i will be able to receive and decode the CTS packet sent from receiver k using rate Rate_1 and thus prevent i from becoming a hidden terminal to receiver k:

$$P_{r\_ki} \geqslant P_{th}(\text{Rate}_1) \tag{11}$$

Combining (10) and (11), we have

$$P_{th}(\text{Rate}_1) \leqslant \frac{P_{th}(\text{Rate}_2)}{\text{SINR}_{th}(\text{Rate}_2)} \frac{P_{t\_k}}{P_{\max}} \tag{12}$$

In our design, fixed power is used for sending RTS and CTS packets, thus $P_{t\_k} = P_{\max}$ and (12) becomes

$$P_{th}(\text{Rate}_1) \leqslant \frac{P_{th}(\text{Rate}_2)}{\text{SINR}_{th}(\text{Rate}_2)} \tag{13}$$

Eq. (13) means that when a transmission rate, say Rate_2, is used for sending DATA packets, we can derive Rate_1 from (13) for sending RTS/CTS packets, and then all hidden terminals can receive and decode the RTS/CTS packets (see Fig. 2). Moreover (13) indicates when designing a multirate network, we can always derive a rate, say Rate_1, such that $P_{th}(\text{Rate}_1)$ satisfies (13) for all other rates provided in the network in order to solve the hidden terminal problem.

With the above analysis, we design our solution to the hidden terminal problem as follows: in a multirate network, we derive a rate, say Rate_1, such that $P_{th}(\text{Rate}_1)$ satisfies (13) for all other rates provided in the network, then we use Rate_1 to send RTS/CTS packets. The above analysis shows that all hidden terminals will be removed with this scheme.

As $\text{SINR}_{th}(\text{Rate}_2)$ is normally >1 (or 0 dB equivalently, see Table 1), then based on (13), $P_{th}(\text{Rate}_1)$ should be $< P_{th}(\text{Rate}_2)$, which means that the transmission range of Rate_1 should be larger than that of Rate_2. While in general, as indicated in Table 1, the higher transmission rate, the higher the requirement is on the received power threshold and SINR, and vice versa. So for a given Rate_2 for the DATA packet, the rate Rate_1, found by (13), is generally a lower rate as compared with Rate_2.

We would like to point out that the RTS/CTS sent by Rate_1 may face a hidden terminal problem as well, although few studies have paid attention to this case. But due to their short transmission times and low SINR requirements compared with the DATA packet's transmission, the hidden terminal problem in sending RTS/CTS packets is generally negligible. This is why existing studies on the hidden terminal problem have mainly focused on DATA packet's transmissions [2,6,7,14,17].

Besides, it is important to note that 802.11 standards use a lower transmission rate (e.g. 1 or 2 Mbps in 802.11b standard; 6/12/24 Mbps in 802.11a) for sending RTS/CTS packets than for DATA packets, this is mainly for maintaining backward compatibility, not for eliminating hidden terminals, and no literature has discussed its impact on the hidden terminal problem as has been done in this paper.

Finally, it needs to be pointed out that our proposed scheme differs from rate adaption. The objective of rate adaption is to make the transmission rate be adaptive to the channel condition and interference. It does not seek to eliminate the interference. Our proposed scheme tries to eliminate the interference from the potential hidden terminals.

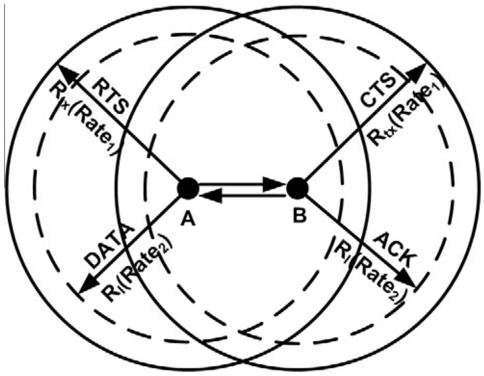


Fig. 2. An illustration of how Rate_1 used for RTS/CTS packets can solve the hidden terminal problem for Rate_2 used for DATA packets; the dashed circles denote the interference areas of DATA/ACK sent by Rate_2; the solid circles denote the transmission areas of RTS/CTS packets. $R_I(\text{Rate}_2)$ denotes the interference range of Rate_2; $R_{tx}(\text{Rate}_1)$ denotes the transmission range of Rate_1.

4.2. Solution to the exposed terminal problem

4.2.1. Proposed solution

With the proposed solution to the hidden terminal problem in Section 4.1, all the nodes that can corrupt an on-going transmission will be covered by the RTS/CTS packets transmitted by an appropriate transmission rate. Consider the area that is outside the transmission range of the RTS/CTS packets but within the carrier sensing range. Terminals located in this area can sense the on-going transmission, and thus will not transmit in spite of the fact that their transmissions cannot corrupt the on-going transmission. This area is called the "exposed terminal area" as shown in Fig. 3.

To understand how large the exposed terminal area is, we can just compare the transmission range of RTS/CTS packets and the carrier sensing range of 802.11. The former is rate dependent, but the latter is not. Suppose we use the lowest transmission rate (1 Mbps) for sending RTS/CTS packets, and which leads to the longest transmission range in 802.11 standards. The carrier sensing range is around 2.2 times that of the transmission range of the 1 Mbps RTS/CTS packets [37,35]. The discussion shows that the exposed terminal area is about 4 times as large as the area reserved by the 1 Mbps RTS/CTS packets. This result reconfirms the recent study by Judd and Steenkiste [24], which shows that exposed terminals are in fact much more prevalent than hidden terminals in WiFi jungles. In its CMU campus-wide WiFi network measurement, there are as many as 11,438 exposed pairs, while there are only 406 hidden pairs.

To tackle the exposed terminal problem, it is necessary to find a method that can reduce this area as much as possible. Our idea is based on the fact that the received power usually exceeds what is needed for the reliable reception of signals because the distance between the sender and the receiver is usually shorter than that of the transmission range, which represents the longest distance allowed between the sender and the receiver. If we can trim the excessive power, we can reduce the sensing range and thus the exposed terminal area. Power control is the way to trim the excessive power. But here we use power control only for DATA/ACK packet transmissions. We still need to use full power (no power control) for sending RTS/CTS packets. This is required by the scheme we designed for solving the hidden terminal problem. Note that if we have not solved the hidden terminal problem, power control could not be used because it would aggravate the hidden terminal problem. This is why we argue in the beginning that finding a joint solution is a good strategy. Note also that by removing the excessive transmission requirement, the proposed protocol is more energy efficient than the IEEE 802.11 MAC.

The power control scheme works as follows. After the RTS/CTS packets are exchanged, the sender will use the re-

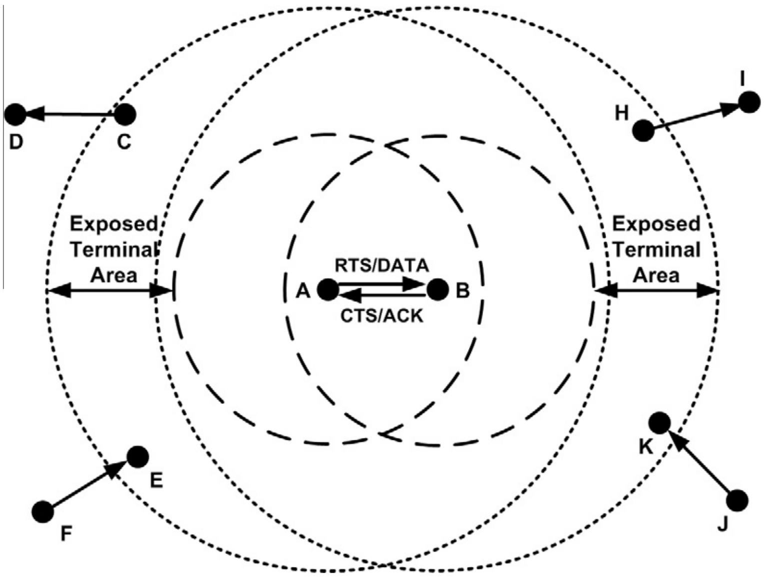


Fig. 3. Exposed terminal area (the gap between carrier sensing area and interference area); dotted circles represent carrier sensing areas; dashed circles denote the interference areas.

ceived power of the CTS packet to estimate the transmit power required for the reliable reception of the subsequent DATA packet and use that power for DATA packet transmission accordingly. How to estimate the transmit power will be discussed later. Note that the power control scheme is done on a per packet basis. Once the transmit power is decided on, it will not change until the current transmission finishes. Assume the computation of the transmit power is done correctly. An illustration of the resulting total reserved area as a function of time during the entire transmission cycle is shown in Fig. 4. Let Area$_{cs}$ represent the total sensed area when using fixed transmit power $P_{\max}$. In the conventional scheme, the reserved area remains the same as Area$_{cs}$ during the entire cycle. In the proposed scheme, the reserved area will be Area$_{cs}$ only during the transmissions of RTS/CTS packets. After that, the power control activates and the reserved area is much smaller during the remaining period of the cycle. The nodes within the reduction area are now free to transmit. Because the transmission time of the RTS/CTS packet is usually much shorter than that for a DATA packet, the average reserved area during the entire cycle is much smaller than that in a conventional scheme.

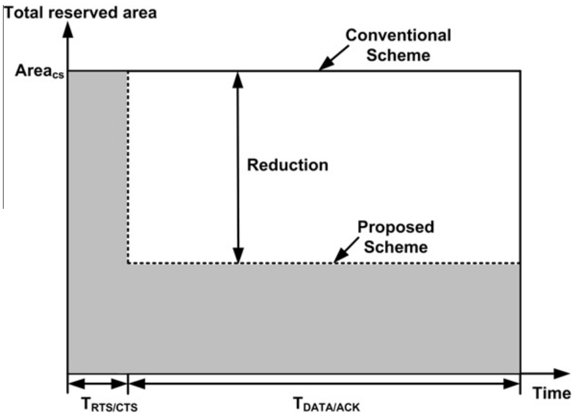


Fig. 4. An illustration of total reserved area as a function of time during a RTS/CTS/DATA/ACK transmission cycle; the shadow area is the total reserved area by the proposed power control scheme.

4.2.2. Compute the transmit power

Below is the detail description of how to compute the transmit power for DATA/ACK packets. Suppose the transmission is from sender j to receiver k.

(i) RTS and CTS packets are transmitted with the maximum power $P_{\max}$, as discussed in Section 4.1.
(ii) DATA and ACK packets are transmitted with different power levels. Based on the received power level of the CTS and RTS packets, the sender and the receiver can estimate the channel gain and will compute the needed transmit powers for the subsequent DATA and ACK packets separately. The procedure for sender j to compute the needed transmit power for the subsequent DATA packet (denoted by $P_{t\_j}(DATA)$) is described below and a similar procedure would be done at receiver k upon receiving the RTS packet to compute the transmit power for the ACK packet.
(iii) Sender j measures the received power level of the CTS packet P_{r_kj} and computes the channel gain $G_{jk} = P_{r\_kj}/P_{\max}$. To ensure a correct decoding, $P_{t\_j}(DATA)$ should be

$$P_{t\_j}(DATA) \geqslant \eta \frac{P_{th}(\text{Rate}_2)}{G_{jk}} = \eta \frac{P_{th}(\text{Rate}_2)P_{\max}}{P_{r\_kj}} \qquad (14)$$

where $\eta \geqslant 1$ is the safety margin. But in the meantime, $P_{t\_j}(DATA)$ should be $\leqslant P_{\max}$. Combined with (14), we have

$$P_{t\_j}(DATA) = \min\left(\eta \frac{P_{th}(\text{Rate}_2)P_{\max}}{P_{r\_kj}}, P_{\max}\right) \tag{15}$$

5. Performance evaluation

NS-2 (version 2.30) simulator [35] is used to evaluate and compare the performance of the proposed protocol and of the IEEE 802.11 MAC. IEEE 802.11 MAC protocol is the dominated MAC protocol used in study of ad hoc and WLAN networks. Comparing a proposed protocol with the IEEE 802.11 MAC is also a common practice used by existing literatures [4,5,7–11,14,20,25,26,30,33,34]. To differentiate from 802.11 MAC, our proposed scheme is named ***PMAC*** in the simulations (The letter "P" represents power control). Two performance measures are used in our comparison: network throughput at the transport layer and fairness among different sender/receiver pairs. Network throughput measures the protocol's efficiency in channel utilization, and fairness indicates how channel bandwidth is shared among different communication links. The degree of fairness is indicated by the instantaneous throughput of a sender/receiver pair versus the total channel capacity.

Both UDP and TCP flows are used in our performance evaluation. Their default setting in NS-2 is adopted in the simulations. In the UDP evaluation, continuously-backlogged data packets, with a fixed size of 1 KB, from CBR (Constant Bit Rate) flow, are generated by the source. In the TCP evaluation, continuously-backlogged data packets, with a fixed packet size 1 KB, are generated by the source.

In the CSMA/CA function in NS-2, the channel state update algorithm (i.e., the Clear Channel Assessment function) does not reflect the real situation when multiple packet transmissions occur concurrently. Therefore, we modified the NS-2 implementation to make it reflect the real channel conditions at each node.

We realized our PMAC based on 802.11 MAC prototype in NS-2. It should be noted that, in the 802.11 MAC protocol in NS-2, the same R_{tx} and SINR$_{th}$ values are applied to all data and control packet transmissions even if their rates are different. We change the simulator so that different R_{tx} and SINR$_{th}$ values for different transmission rates can be used in PMAC simulations.

Five typical scenarios are simulated: (a) exposed terminal problem: exposed sender, (b) exposed terminal problem: exposed receiver, (c) hidden terminal problem, (d) intra-flow contention in multihop communications, and (e) inter-flow contention in multihop communications. These scenarios have been widely used in other studies on hidden and exposed terminals [1–3,8,7,9–11,38].

In the simulations, transmission rates from IEEE 802.11a/b/g are used and the rate dependent values (SINR requirements and transmission ranges) are derived from Table 1. Unless indicated otherwise, the following default parameter settings are used:

(1) The carrier sensing range is $R_{cs} = 550$ m; (2) the transmission range for 1 Mbps, $R_{tx}(1\text{ M})$, is set to be 250 m, and then the transmission ranges of other rates are set proportionally based on Table 1, for example, $R_{tx}(11\text{ M}) = 125$ m, R$_{tx}$(24 M) = 80 m; (3) the transmission rate for RTS/CTS and DATA/ACK are set to be 1 Mbps and 11 Mbps respectively; (4) IEEE 802.11b parameters are adopted in the simulations; (5) each simulation runs for 50 s; and (6) two-ray ground reflection propagation model is used.

5.1. Single-hop scenarios

5.1.1. Exposed terminal problem: exposed sender

This refers to the scenario involving D–C–A–B in Fig. 3. There are two UDP communication flows: $C \rightarrow D$ and $A \rightarrow B$ (i.e. A and C are the senders). Flow $C \rightarrow D$ begins its transmissions at $t = 0$, and flow $A \rightarrow B$ begins its transmissions at $t = 4$ s. The distances between D and C, C and A, A and B are 100 m, 500 m, and 100 m respectively. The two communication links affect each other via the interaction between the two senders C and A. Both nodes are the exposed senders to each other. In the exposed sender scenario, fairness is not an issue because both senders can contend for the channel effectively. The main issue is to allow more concurrent transmissions.

Fig. 5a and b shows the instantaneous throughputs of the two UDP flows under PMAC as well as under 802.11. We can see that both flows under PMAC achieve a throughput of about 90% of the channel capacity, while the two flows under 802.11 can only achieve 50% of the total channel capacity. In PMAC, the transmit power is reduced once the phase for DATA transmission begins. This greatly enhances the chances for concurrent transmissions. The throughput ratio of PMAC over 802.11 is about 1.8 times (Fig. 5c).

5.1.2. Exposed terminal problem: exposed receiver

This refers to the scenario involving F–E–A–B in Fig. 3. There are two UDP flows: $F \rightarrow E$ and $A \rightarrow B$. Flow $F \rightarrow E$ starts first and begins its transmission at $t = 0$. At $t = 4$ s, flow A → B starts. The distances between F and E, E and A, A and B are 100 m, 500 m, and 100 m respectively. The two communication links affect each other via the interaction between E and A. Node E is the exposed receiver. Besides throughput degradation, unfair sharing of the channel capacity is another negative effect caused by the exposed receiver. We study both effects in the simulation.

Fig. 6a and b describes the instantaneous throughputs of the two links under PMAC and under 802.11. We can see that the instantaneous throughput of F → E under 802.11 is seriously affected by E's carrier sensing. But in PMAC, F → E can still maintain a throughput comparable to that of link A → B. The power reduction in DATA/ACK packet transmissions by flow A → B greatly reduces the chances of detecting a carrier by node E's carrier sensing. This allows F → E to share more of the channel capacity. In terms of fairness, Fig. 6a and b shows that PMAC can effectively improve the performance of the disadvantaged link suffering from the exposed terminal problem. Fig. 6c compares the network throughput between 802.11 and

Please cite this article in press as: C. Huang et al., A joint solution for the hidden and exposed terminal problems in CSMA/CA wireless networks, Comput. Netw. (2012), http://dx.doi.org/10.1016/j.comnet.2012.06.008

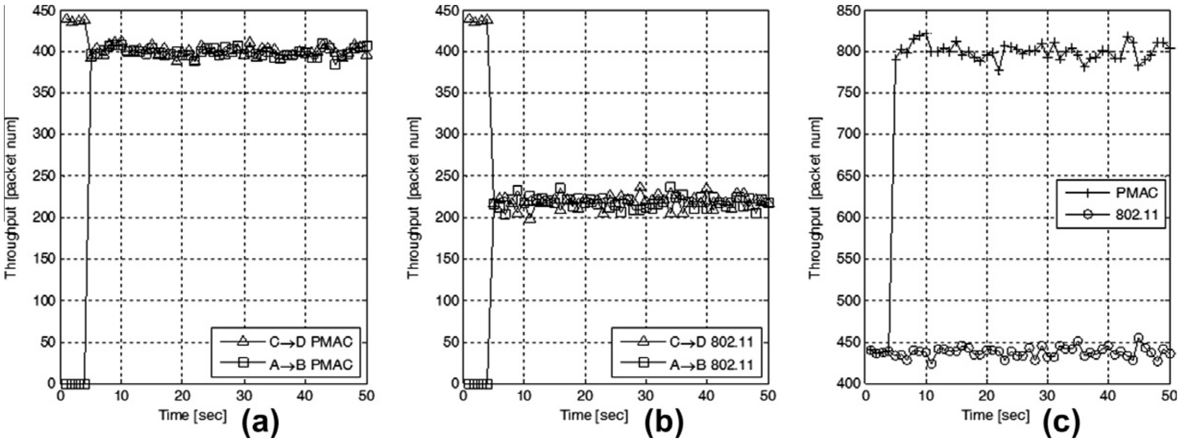


Fig. 5. Exposed terminal problem: exposed sender: throughput comparison between PMAC and 802.11. (a) Throughput performance of two links in PMAC. (b) Throughput performance of two links in 802.11. (c) UDP network throughput comparison between PMAC and 802.11.

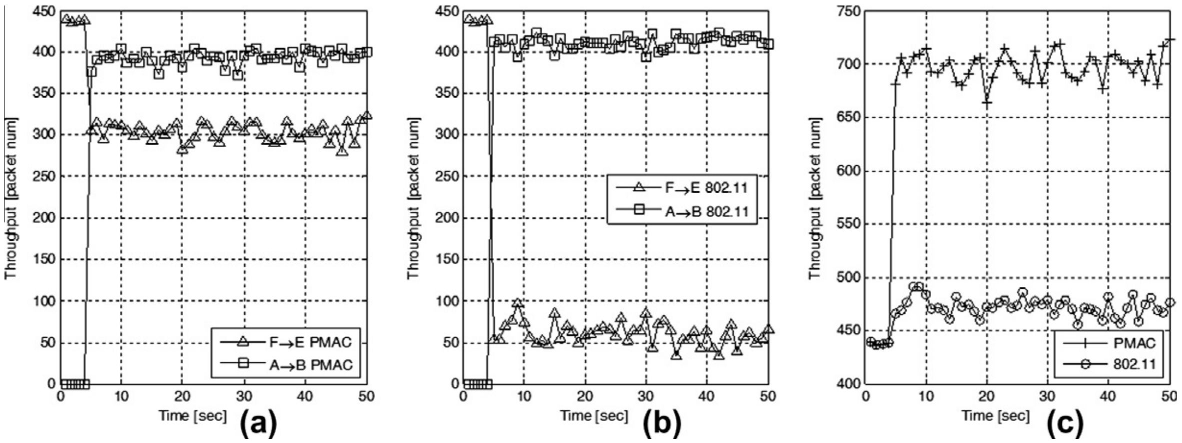


Fig. 6. Exposed terminal problem: exposed receiver: throughput comparison between PMAC and 802.11. (a) Throughput performance of two links in PMAC. (b) Throughput performance of two links in 802.11. (c) UDP network throughput comparison between PMAC and 802.11.

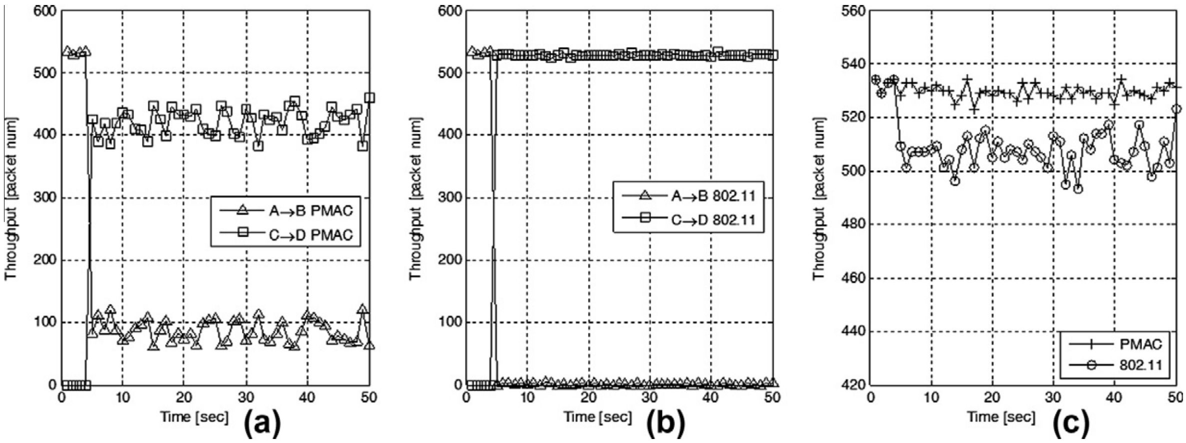


Fig. 7. Hidden terminal problem: throughput comparison between PMAC and 802.11. (a) Throughput performance of two links in PMAC. (b) Throughput performance of two links in 802.11. (c) UDP network throughput comparison between PMAC and 802.11.

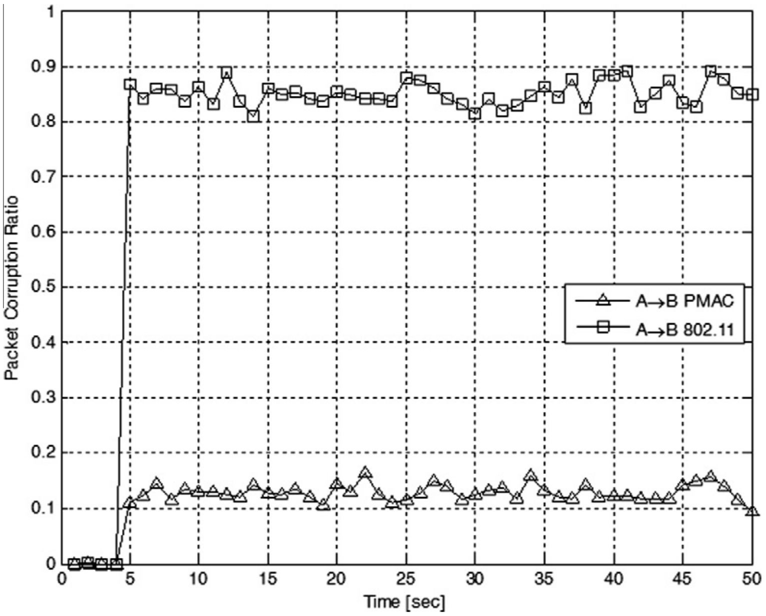


Fig. 8. The packet corruption ratio comparison between PMAC and 802.11 at receiver side (node B at link A → B), which is suffering from hidden terminal problem.

PMAC. Again, the network throughput of PMAC is significantly higher than that of 802.11. The throughput ratio of PMAC over 802.11 is about 1.5 times.

5.1.3. Hidden terminal problem

This refers to the scenario involving A–B–C–D. There are two UDP flows: A → B and C → D. The two flows only affect each other via the interaction between node B and C. Node C is within the interference range of B but out of the carrier sensing range of A. The transmission rate for DATA/ACK and RTS/CTS is set to be 24 Mbps and 1 Mbps respectively. Their SINR requirements of the transmission rates are set with data provided in Table 1. The distances between A and B, B and C, C and D are 80 m, 200 m, and 80 m respectively. The two communication links affect each other via the interaction between node B and node C. Node C is the hidden terminal to node B. Flow A → B starts first and begins its transmissions at $t = 0$. At $t = 4$ s, flow C → D starts. As the simulation environment in NS-2 provides no walls and obstacles, we choose a small carrier sensing range ($R_{cs} = 250$ m) to facilitate the simulation of the hidden terminal problem. Also, packet collisions due to the capture effect are filtered out by modifying NS-2 configuration so that packets arriving later can still be recaptured so long as the strength of the signal is high enough to exceed the corresponding threshold. This allows us to focus on the effect of packet collisions caused by the hidden terminal problem.

Fig. 7a and b shows the instantaneous throughputs of the two links under 802.11 and under PMAC. In 802.11, the throughput of link A → B drops to zero right after the start of the transmission from C to D. As long as C keeps transmitting, rarely can flow A → B have any successful transmission. But in PMAC, flow A → B can still capture around 20% of the total channel capacity while there is continuously-backlogged traffic from C to D. The reason that A → B cannot seize an equal share of the channel capacity is that A → B has to contend for the channel via receiver B while node C has continuously-backlogged traffic to send.

Fig. 7c compares the network throughput between 802.11 and PMAC. It shows that besides fairness, the network throughput is also significantly enhanced by PMAC.

Fig. 8 plots the packet corruption ratios at node B under PMAC and 802.11. The packet corruption ratio is defined as the ratio of the number of unsuccessfully received packets (DATA and RTS packets) at the receiver over the total number of transmitted packets from the sender at the same time slot. In 802.11, 85% of the packets sent from A to B are corrupted. In PMAC, only 12% are corrupted. The reason is that, in PMAC, CTS packets are sent at a lower rate, and therefore can reach all potential hidden terminals. This is not the case in 802.11. The results shown in Figs. 7 and 8

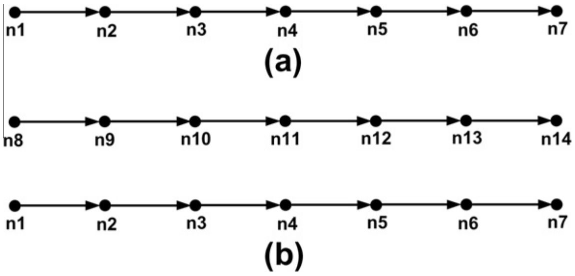


Fig. 9. Multihop (chain topology) scenarios. (a) Single chain topology. (b) Two parallel chain topology.

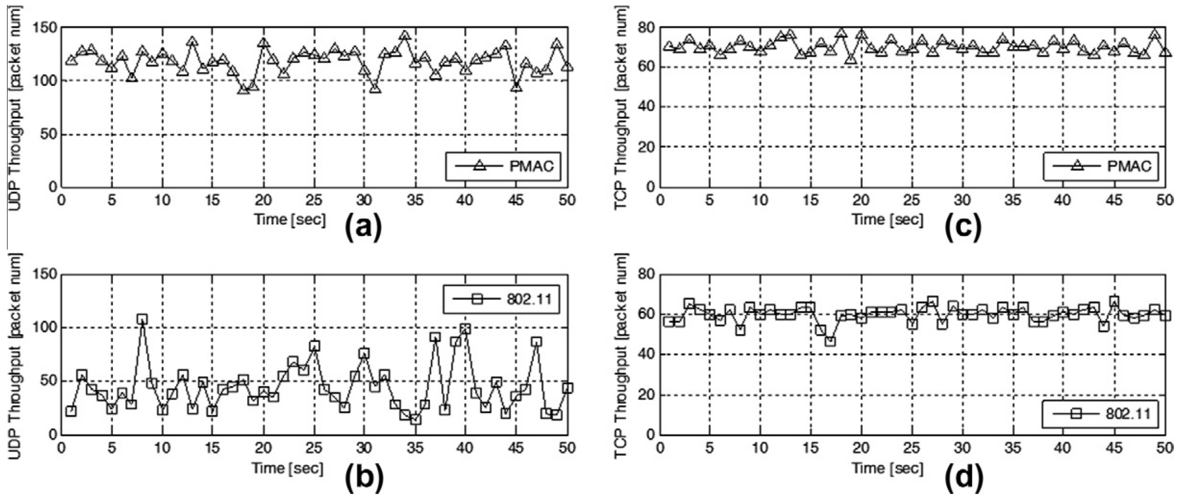


Fig. 10. UDP and TCP throughput of the single-chain topology given in Fig. 9a. (a) UDP throughput under PMAC. (b) UDP throughput under 802.11. (c) TCP throughput under PMAC. (d) TCP throughput under 802.11.

together demonstrate the effectiveness of our proposed scheme in solving the hidden terminal problem.

5.2. Multihop scenarios

In the multihop scenario, we study two major issues: intra-flow contention and inter-flow contention. They are the two main issues affecting the multihop network performance. In the intra-flow contention problem, a node's transmission/reception is interfered by other nodes in the same chain. In the inter-flow contention, a node's transmission/reception is interfered not only by other nodes in the same chain, but also by the nodes in other chains.

To study intra-flow contention in a multihop environment, we assume a flow involving seven nodes as shown in Fig. 9a. The same scenario is used in widely cited literature [38] for studying wireless ad hoc networks. Node $n1$ is the source node and the last node $n7$ is the sink node, and each node is 200 m away from its immediate neighbors. Data rates for DATA/ACK and RTS/CTS are 24 Mbps and 5.5 Mbps respectively. The values of $R_{tx}(24\,\text{M})$ and $R_{tx}(5.5\,\text{M})$ are set to 225 m and 455 m based on Table 1. The SINR$_{th}$ values are also set according to the same Table. Other settings are as described at the beginning of this section.

To study inter-flow contentions in a multihop environment, we add one more flow in parallel as shown in Fig. 9b. For this flow, node $n8$ is the source and node $n14$ is the sink. The vertical distance between the two parallel flows is set to be 500 m. Two flows start their transmission at $t = 0$. Other settings remain unchanged as in the intra-flow study.

5.2.1. Intra-flow contention

We first study the intra-flow contention problem where a node's transmission/reception is interfered by other nodes in the same chain. Fig. 10a and b plots the UDP throughputs under PMAC and under 802.11 MAC. The throughput of PMAC is 2.6 times that of 802.11 MAC. For 802.11, many collisions occur at the intermediate nodes and only a small portion of the packets reach the destination node ($n7$). As can be seen, the throughput gain of the proposed protocol is much higher than in a single-hop environment. In the multihop scenario, packets have to travel along a chain of nodes toward the destination. The nodes along the chain have to contend with each other in order to access the channel. Any node suffering from the hidden or exposed terminal problem will affect the end-to-end performance of the flow. The impact of the hidden and exposed terminal problems will become more severe than in a single hop environment.

Fig. 10c and d plots the TCP throughput under PMAC and under 802.11 MAC. We can see that PMAC still outperforms 802.11, but the throughput gap between them is narrower. The reason is that when packets are lost, TCP congestion control will kick in and the source node ($n1$) will sharply reduce its traffic into the network.

5.2.2. Inter-flow contention

In inter-flow contention, a node's transmission/reception is interfered not only by other nodes in the same chain, but also by the nodes in other chains. Fig. 11a–d plots the UDP throughputs of the two flows under PMAC as well as under 802.11 MAC. The two flows in PMAC have similar throughputs. But, in 802.11 MAC, only one flow enjoys a similar throughput as that in PMAC. The other flow starves and its throughput even drops to zero at the end of the simulation. Fig. 11e and f plots the sum of the throughputs of the two flows. They show that PMAC's throughput is 40% higher than that of 802.11.

Fig. 12a–d plots the TCP throughput of the two flows under PMAC and 802.11 MAC. Similar conclusions to the UDP performance still hold. Fig. 12e and f plot the sum of the throughputs of the two TCP flows. They show that PMAC's performance is 22% better than that of 802.11 MAC.

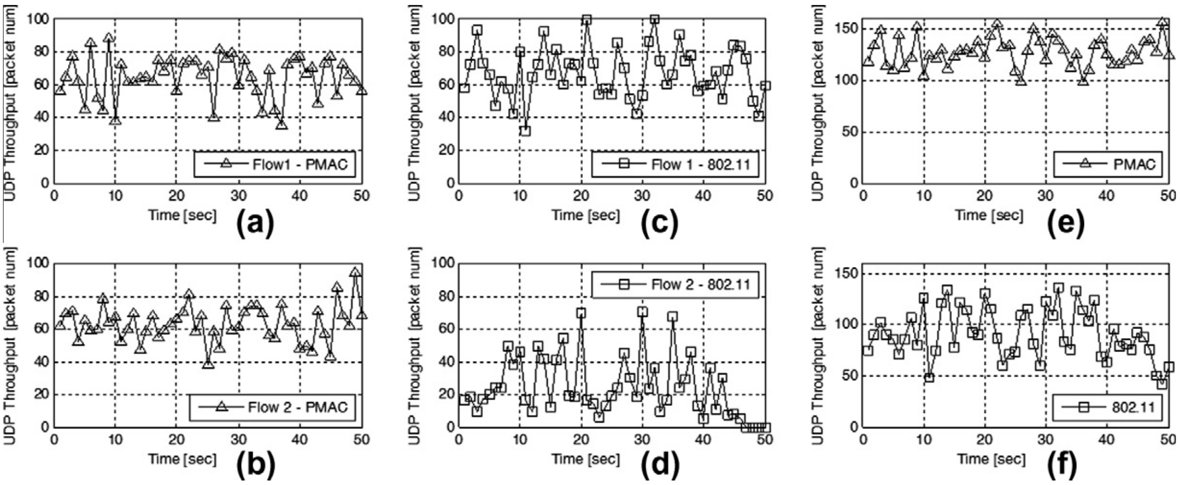


Fig. 11. UDP throughput of the two parallel chain topology given in Fig. 12b. (a) UDP throughput of flow 1 under PMAC. (b) UDP throughput of flow 2 under PMAC. (c) UDP throughput of flow 1 under 802.11. (d) UDP throughput of flow 2 under 802.11. (e) Total UDP throughput of two flows under PMAC. (f) Total UDP throughput of two flows under 802.11.

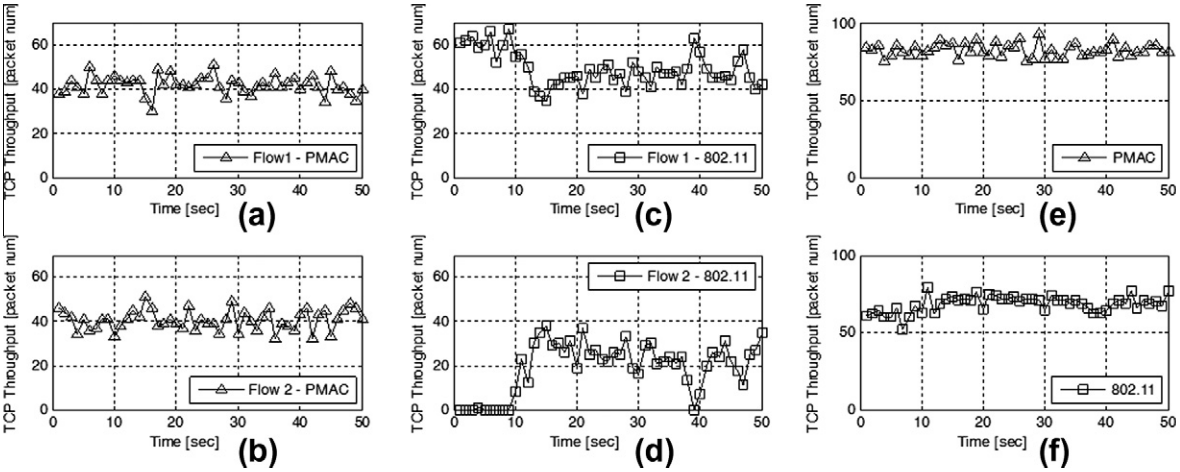


Fig. 12. TCP throughput of the two parallel chain topology given in Fig. 12b. (a) TCP throughput of flow 1 under PMAC. (b) TCP throughput of flow 2 under PMAC. (c) TCP throughput of flow 1 under 802.11. (d) TCP throughput of flow 2 under 802.11. (e) Total TCP throughput of two flows under PMAC. (f) Total TCP throughput of two flows under 802.11.

6. Conclusion

In this paper, we present a joint approach to resolve the hidden and exposed terminal problems in wireless networks. For the hidden terminal problem, the proposed technique exploits an important fact in digital communication: different transmission rates have different SINR requirements and received power thresholds, and hence different transmission ranges and interference ranges. This fact has often been ignored in the literatures related to the hidden/exposed terminal problems. It has been shown in the paper that for a given DATA packet transmission rate the associated hidden terminals can be mostly removed by selecting an appropriate rate for sending RTS/CTS packets. We then propose to integrate the transmission power control into our solution to tackle the exposed terminal problem. By reducing the power for the DATA/ACK packet transmissions to a level suitable for successful decoding, the area reserved during the transmission cycle of a packet can be significantly reduced. Note that only have we solved the hidden terminal problem, power control could be used because it is well understood that power control would aggravate the hidden terminal problem.

The proposed solution has several major advantages. First, unlike the techniques presented previously, the proposed solution resolves both problems simultaneously and avoids the drawback of lessening one problem but aggregating the other. Second, the solution has a significant throughput gain over the conventional IEEE 802.11 MAC: up to 1.8 times for single-hop flows and up to 2.6 times for multihop flows. Third, the solution is fully compatible with the IEEE 802.11 MAC and requires no protocol change.

References

[1] S. Xu, T. Saadawi, Does the IEEE 802.11 MAC protocol work well in multihop wireless adhoc networks?, Communications Magazine IEEE 39 (6) (2001) 130–137

[2] K. Xu, M. Gerla, S. Bae, How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks? in: Proc. GlobeCom, vol. 1, 2002, pp. 72–76.

[3] V. Bharghavan, A. Demers, S. Shenker, L. Zhang, MACAW: A media access protocol for wireless LANs, in: Proc. SIGCOMM, 1994.

[4] X. Yang, N. Vaidya, On physical carrier sensing in wireless ad hoc networks, in: Proc. IEEE INFOCOM, vol. 4, 2005, pp. 2525–2535.

[5] H. Zhai, Y. Fang, Physical carrier sensing and spatial reuse in multirate and multihop wireless ad hoc networks, in Proc. IEEE INFOCOM, vol. 6, 2006.

[6] P. Karn, MACA-a new channel access method for packet radio, ARRL/CRRL Amateur Radio 9th Computer Networking Article 140 (1990).

[7] C. Fullmer, J. Garcia-Luna-Aceves, Solutions to hidden terminal problems in wireless networks, in: Proc. ACM SIGCOMM, 1997, pp. 39–49.

[8] C. Huang, C.-T. Lea, A.K.-S. Wong, Rate matching: a new approach to hidden terminal problem in ad hoc networks, ACM Wireless Networks 16 (8) (2010) 2139–2150.

[9] A. Acharya, A. Misra, S. Bansal, MACA-P: a MAC for concurrent transmissions in multi-hop wireless networks, in: Proc. IEEE PerCom, 2003.

[10] D. Shukla, L. Chandran-Wadia, S. Iyer, Mitigating the exposed node problem in IEEE 802.11 ad hoc networks, in Proc. of IEEE ICCCN, 2003.

[11] M. Vutukuru, K. Jamieson, H. Balakrishnan, Harnessing exposed terminals in wireless networks, in: USENIX NSDI, 2008, pp. 59–72.

[12] C. Huang, C.T. Lea, A.K.-S. Wong, On Fairness Enhancement for CSMA/CA Wireless Networks, IEEE Systems Journal 4 (4) (2010) 511–523.

[13] Z. Haas, J. Deng, Dual busy tone multiple access (DBTMA) – a multiple access control scheme for ad hoc networks, IEEE Transactions on Communications 50 (6) (2002) 975–985.

[14] H. Zhai, J. Wang, Y. Fang, DUCHA: a new dual-channel MAC protocol for multihop ad hoc networks, IEEE Transactions on Wireless Communications 5 (11) (2006) 3224–3233.

[15] J. Yee, H. Pezeshki-Esfahani, Understanding Wireless LAN Performance Trade-offs, November 2002. <http://www.commsdesign.com>.

[16] B. Awerbuch, D. Holmer, H. Rubens, The medium time metric: high throughput route selection in multi-rate ad hoc wireless networks, Mobile Networks and Applications 11 (2) (2006) 253–266.

[17] F. Tobagi, L. Kleinrock, Packet switching in radio channels: part II – the hidden terminal problem in carrier sense multiple-access and the busy-tone solution, IEEE Transactions on Communications 23 (12) (1975) 1417–1433.

[18] C. Wu, V. Li, Receiver-initiated busy-tone multiple access in packet radio networks, ACM SIGCOMM Computer Communication Review 17 (5) (1987) 336–342.

[19] J. Monks, V. Bharghavan, W. Hwu, A power controlled multiple access protocol for wireless packet networks, in: Proc. IEEE INFOCOM, vol. 1, 2001, pp. 219–228.

[20] A. Muqattash, M. Krunz, Power controlled dual channel (PCDC) medium access protocol for wireless ad hoc networks, in: Proc. IEEE INFOCOM, vol. 1, 2003, pp. 470–480.

[21] P. Wang, H. Jiang, W. Zhuang, A new mac scheme supporting voice/data traffic in wireless ad hoc networks, IEEE Transactions on Mobile Computing (2008) 1491–1503.

[22] D. Johnson, D. Maltz, Dynamic source routing in ad hoc wireless networks, Mobile computing (1996) 153–181.

[23] C. Perkins, E. Royer, Ad-hoc on-demand distance vector routing, in: Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications, 1999, pp. 90–100.

[24] G. Judd, P. Steenkiste, Understanding link-level 802.11 behavior: replacing convention with measurement, in: Proceedings of the 3rd International Conference on Wireless Internet, 2007, pp. 1–10.

[25] J. Zhu, X. Guo, L. Yang, W. Conner, Leveraging spatial reuse in 802.11 mesh networks with enhanced physical carrier sensing, in: Proc. IEEE ICC, 2004.

[26] J. Deng, B. Liang, P. Varshney, Tuning the carrier sensing range of IEEE 802.11 MAC, in: Proc. IEEE GLOBECOM, vol. 5, 2004, pp. 2987–2991.

[27] P. Gupta, P. Kumar, The capacity of wireless networks, IEEE Transactions on Information Theory 46 (2) (2000) 388–404.

[28] M. Pursley, H. Russell, J. Wysocarski, Energy-efficient transmission and routing protocols for wireless multiple-hop networks and spread-spectrum radios, in: Proc. EUROCOMM, 2000, pp. 1–5.

[29] J. Gomez, A. Campbell, M. Naghshineh, C. Bisdikian, Conserving transmission power in wireless ad hoc networks, in: Proc. IEEE ICNP, 2001, pp. 24–34.

[30] E. Jung, N. Vaidya, A power control MAC protocol for ad hoc networks, Wireless Networks, Springer 11 (1) (2005) 55–66.

[31] V. Mhatre, K. Papagiannaki, F. Baccelli, Interference mitigation through power control in high density 802.11 WLANs, in: IEEE INFOCOM, 2007, pp. 535–543.

[32] K. Ramachandran, R. Kokku, H. Zhang, M. Gruteser, Symphony: synchronous two-phase rate and power control in 802.11 WLANs, in: ACM MobiSys, 2008, pp. 132–145.

[33] J. Zhu, B. Metzler, X. Guo, Y. Liu, Adaptive CSMA for scalable network capacity in high-density WLAN: a hardware prototyping approach, in: IEEE INFOCOM, 2006.

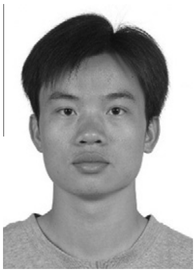
[34] M. Brodsky, R. Morris, In defense of wireless carrier sense, in: Proceedings of the ACM SIGCOMM 2009 Conference on Data, Communication, 2009, pp. 147–158.

[35] Network Simulator-2. <http://www.isi.edu/nsnam/ns/>.

[36] T. Rappaport, Wireless Communications: Principles and Practice, Prentice Hall, NJ, USA, 1996.

[37] IEEE-SA Standards Board, ANSI/IEEE Std. 802.11, 1999 Edition (R2003), 1999.

[38] J. Li, C. Blake, D. De Couto, H. Lee, R. Morris, Capacity of ad hoc wireless networks, in: Proc. ACM Mobicom, 2001.



Caishi Huang received the B.Eng. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 2005, and the M.Phil. degree in Electronic and Computer Engineering from Hong Kong University of Science and Technology, Hong Kong, in 2007. He is currently working toward the Ph.D. degree in the same Department. His research interests include architecture, protocol design and performance evaluation of wireless networks.

Chin-Tau Lea received a B.S and a M.S. degree from the National Taiwan University in 1976 and 1978, and a Ph.D. degree from the University of Washington, Seattle, in 1982, all in electrical engineering. He is now a professor at the Hong Kong Univ of Science and Technology which he joined in 1996. Prior to that, he was with AT&T Bell Labs from 1982 to 1985 and with the Georgia Institute of Technology from 1985 to 1995.

Dr. Lea's research interests are in the general area of networking and switching. He is on the editorial board of IEEE JSAC and of Computer Networks. Dr. Lea received the DuPont Young Faculty Award from Georgia Tech in 1987, the IEEE Jack Neubauer Paper Award in 1998, and the School of Engineering Teaching Award from HKUST in 1998. He also holds seven US patents.

Albert Kai-Sun Wong received the S.B., S.M., E.E., and Ph.D. degrees in electrical engineering, all from the Massachusetts Institute of Technology, Cambridge, in 1982, 1984, and 1988 respectively. He is currently a Visiting Associate Professor at HKUST, the Hong Kong University of Science and Technology. From 1988 to 2000, he was with AT&T and Lucent Technologies/ Bell Laboratories in New Jersey, as Member of Technical Staff, Distinguished Member of Technical Staff, Technical Manager, Director of Technical Marketing, and Director, Sales and Technical Marketing. From 2000 to 2008, he held positions in Hong Kong as Chief Operating Officer of Transtech Services Group, Vice President of the Applied Science and Technology Research Institute, and executive director of Nansha development, HKUST. Previously, he has also held visiting and adjunct faculty positions at the Chinese University of Hong Kong, Polytechnic University of New York, and Rutgers University. His current research interests include wireless localization and tracking, mobile and internet applications, and photonic and data switching systems.

Please cite this article in press as: C. Huang et al., A joint solution for the hidden and exposed terminal problems in CSMA/CA wireless networks, Comput. Netw. (2012), http://dx.doi.org/10.1016/j.comnet.2012.06.008