Available at
www.ComputerScienceWeb.com
POWERED BY SCIENCE @ DIRECT®

Ad Hoc Networks 1 (2003) 107–123

Ad Hoc Networks

www.elsevier.com/locate/adhoc

Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks

Kaixin Xu [a,*], Mario Gerla [a], Sang Bae [b]

[a] *UCLA Computer Science Department, Los Angeles, CA 90095, USA*
[b] *The Boeing Company, Phantom Works, Seattle, WA 98124, USA*

Abstract

IEEE 802.11 MAC mainly relies on two techniques to combat interference: physical carrier sensing and RTS/CTS handshake (also known as "virtual carrier sensing"). Ideally, the RTS/CTS handshake can eliminate most interference. However, the effectiveness of RTS/CTS handshake is based on the assumption that hidden nodes are within transmission range of receivers. In this paper, we prove using analytic models that in ad hoc networks, such an assumption cannot hold due to the fact that power needed for interrupting a packet reception is much lower than that of delivering a packet successfully. Thus, the "virtual carrier sensing" implemented by RTS/CTS handshake cannot prevent all interference as we expect in theory. Physical carrier sensing can complement this in some degree. However, since interference happens at receivers, while physical carrier sensing is detecting transmitters (the same problem causing the hidden terminal situation), physical carrier sensing cannot help much, unless a very large carrier sensing range is adopted, which is limited by the antenna sensitivity. In this paper, we investigate how effective is the RTS/CTS handshake in terms of reducing interference. We show that in some situations, the interference range is much larger than transmission range, where RTS/CTS cannot function well. Two independent solutions are proposed in this paper. One is a simple enhancement to the IEEE 802.11 MAC protocol. The other is to utilize directional antennas. Simulation results verify that the proposed schemes indeed can help IEEE 802.11 resolve most interference caused by large interference range.

Keywords: Ad hoc networks; MANET; MAC; IEEE 802.11; Interference range; RTS/CTS

1. Introduction

In wireless networks, interference is location dependent. Thus, the hidden terminal problem may happen frequently [1]. Resolving hidden terminal problem becomes one of the major design considerations of MAC protocols. IEEE 802.11 DCF is the most popular MAC protocol used in both wireless LANs and mobile ad hoc networks (MANETs). Its RTS/CTS handshake is mainly designed for such a purpose. However, it has an underlying assumption that all hidden nodes are within the transmission range of receivers (e.g. to receive the CTS packet successfully). From our study, we realize that such an assumption may not hold when the transmitter–receiver distance exceeds a certain value. Some nodes, which are out

[*] Corresponding author.
E-mail addresses: xkx@cs.ucla.edu (K. Xu), gerla@cs.ucla.edu (M. Gerla), kyle.bae@boeing.com (S. Bae).

1570-8705/$ - see front matter © 2003 Elsevier B.V. All rights reserved.
doi:10.1016/S1570-8705(03)00015-5

of the transmission range of both the transmitter and the receiver, may still interfere with the receiver. This situation happens rarely in a wireless LAN environment since there most nodes are in the transmission range of either transmitters or receivers. However, in an ad hoc network, it becomes a serious problem due to the large distribution of mobile nodes and the multihop operation. In this paper, we show that for the open space environment, the interference range of a receiver is 1.78 times the transmitter–receiver distance (under TWO-RAY GROUND pathloss model). This implies that RTS/CTS handshake cannot function well when the transmitter–receiver distance is larger than 0.56 (equal to 1/1.78) times the transmission range. We then further analyze the effectiveness of RTS/CTS handshake under such situations and its relationship with physical carrier sensing. Our study reveals that large interference range is a serious problem in ad hoc networks and may hurt the network capacity as well as the network performance significantly. This is confirmed via simulation experiments.

To attack this problem, we investigate two techniques in this paper. The first technique is a simple MAC layer scheme with some minor modifications of IEEE 802.11 MAC DCF. Its major idea is to prevent the transmissions when the link quality is weak (e.g. transmitter–receiver distance is large) by selectively replying CTS packets. The major drawback of this MAC layer technique is the reduced effective transmission range. The second technique is to enhance the hardware, more precisely to use receiving beam forming (RBF) antennas. RBF antenna is a type of directional antennas, where the transmission is omnidirectional, but the reception is directional. It is capable to prevent interference by lock onto a specific direction for packet reception. In this paper, we prove that once the beam width of the RBF antenna is smaller than a certain value, it can totally bypass interference due to the large interference range. Both of the two techniques have their advantages and disadvantages, which will be discussed and investigated in this paper.

The rest of this paper is organized as following. In Section 2, we briefly review some related work in the literature. Section 3, we compute interference range and analyze the effectiveness of RTS/CTS handshake using an analytical model. The relationship between interference range and physical carrier sensing range is also discussed. In Section 4, we identify the problems caused by large interference range. In Section 5, two independent solutions are proposed and discussed. Performance evaluations via simulation are given in Section 6 and we conclude the paper in Section 7.

2. Related work

Large interference range has been realized by more and more researchers in recent years [2,3]. In [2], the influence of large interference range to the ad hoc network capacity is studied. In [3], large interference range is also recognized as one of the major factors which causing TCP unfairness/capture problem. However, so far from our knowledge, we have not seen any work trying to analyze and resolve this problem in detail. Thus, this paper presents a preliminary and original study on this topic.

Resolving hidden terminal problem is one of the major tasks of MAC protocols such as IEEE 802.11 [4]. However, most of them assume that hidden nodes are within transmission range of the receiver. Thus, schemes such as RTS/CTS handshake will suffer to the large interference range greatly. In the early times of MAC protocol design for packet radio networks, a receiver-initiated busy-tone scheme was proposed to solve the hidden terminal problems [5]. Receiver-initiated busy-tone is actually able to eliminate the collisions caused by large interference range although it was not originally proposed for this use. However, it needs a separate wireless channel for the busy-tone, which is not desirable in the real ad hoc networks.

Interference reduction is also one of the advantages of MAC schemes for power control. By adjusting the transmission power, a node is able to reduce its interference to other transmissions [6]. In this paper, we assume all wireless radios are homogeneous. Since in the reality (at least in current stage), gracefully adjusting the transmission power is still not practical, we prefer a fixed transmission power. Comparing our proposed MAC scheme to those power control schemes, we have different targets. Our MAC scheme focuses on eliminating the collisions due to large interference range, not power consumption.

3. Effectiveness of RTS/CTS handshake

The RTS/CTS handshake of IEEE 802.11 MAC does not work as well as we expected in theory. It cannot prevent hidden terminal problems completely. In this section, we explain this through a simple theoretical analysis. For better understanding, we first define three radio ranges related to a wireless radio, namely transmission range (R_{tx}), carrier sensing range (R_{cs}) and interference range (R_i).

- *Transmission range* (R_{tx}) represents the range within which a packet is successfully received if there is no interference from other radios. The transmission range is mainly determined by transmission power and radio propagation properties (i.e., attenuation).
- *Carrier sensing range* (R_{cs}) is the range within which a transmitter triggers carrier sense detection. This is usually determined by the antenna sensitivity. In IEEE 802.11 MAC, a transmitter only starts a transmission when it senses the media free.
- *Interference range* (R_i) is the range within which stations in receive mode will be ‘‘interfered with’’ by an unrelated transmitter and thus suffer a loss.

3.1. Interference range and the interference area

Within the three ranges listed above, the transmission range and carrier sensing range are generally well known. They are fixed ranges only affected by the properties of the wireless radios installed at the sender and receiver. The interference range, however, draws little attention. Many research work in ad hoc networks usually ignores the interference range or just simply assume it same to the transmission range. From our study, we realize that the interference range is not a fixed range. Rather it is essentially related to the transmitter receiver distance. In some situations, the interference range can goes far beyond the transmission range, resulting various problems that have not been considered carefully in the literature. In this section, we investigate the interference range and its relationship to the other two ranges.

Nodes within the interference range of a receiver are usually called hidden nodes. When the receiver is receiving a packet, if a hidden node also tries to start a transmission concurrently, collisions will happen at the receiver. When a signal is propagated from a transmitter to a receiver, whether the signal is valid at the receiver largely depends on the receiving power at the receiver. Given transmission power (P_t), the receiving power (P_r) is mostly decided by pathloss over the transmitter–receiver distance, which models the signal attenuation over the distance. Other factors include multipath fading, shadowing, environment noise etc. Here we ignore these factors since they are minor factors in the open space environment. According to [7], in the open space environment, the receiving power (P_r) of a signal from a sender d meters away can be modelled as Eq. (1).

$$P_r = P_t G_t G_r \frac{h_t^2 h_r^2}{d^k}. \tag{1}$$

In Eq. (1), G_t and G_r are antenna gains of transmitter and receiver respectively. h_t and h_r are the height of both antennas. Here, we assume that the ad hoc network is homogeneous, that is all the radio parameters are same at each node. k should be larger than 2 and reflects how fast the signal decays. The larger it is, the faster the signal attenuates. In the open space environment, the TWO-RAY GROUND pathloss model is generally adopted. Within this model, when the transmitter is close to the receiver (e.g. within the Freznel zone [7]), receiving signal power is inverse proportional to d^2. When their distance is larger (e.g. outside of Freznel zone), the receiving signal power is then inverse proportional to d^4 [7]. In this paper, since we mostly focus on situations where transmitter–receiver distance is large, we assume k is always equal to 4 for TWO-RAY GROUND model. Another common pathloss model used in wireless networks is the open space pathloss model, which has k as 2.

A signal arriving at a receiver is assumed to be valid if the signal to noise ratio (SNR) is above a certain threshold (T_{SNR}). Now, we assume a transmission is going from a transmitter to a receiver with transmitter–receiver distance as d meters and at the same time, an interfering node r meters away from the receiver starts another transmission. Let P_{r} denote the receiving power of signal from transmitter and P_{i} denote the power of interference signal at the receiver. Then, SNR is given as $\mathrm{SNR} = P_{\mathrm{r}}/P_{\mathrm{i}}$. Here, we ignore the thermal noise since it is ignorable comparing to interference signal. Under the assumption of homogeneous radios, we get

$$\mathrm{SNR} = P_{\mathrm{r}}/P_{\mathrm{i}} = \frac{P_{\mathrm{t}} G_{\mathrm{t}} G_{\mathrm{r}} \frac{h_{\mathrm{t}}^2 h_{\mathrm{r}}^2}{d^k}}{P_{\mathrm{t}} G_{\mathrm{t}} G_{\mathrm{r}} \frac{h_{\mathrm{t}}^2 h_{\mathrm{r}}^2}{r^k}} = \left(\frac{r}{d}\right)^k \geqslant T_{\mathrm{SNR}}, \tag{2}$$

$$r \geqslant \sqrt[k]{T_{\mathrm{SNR}}} * d. \tag{3}$$

This implies that to successfully receive a signal, the interfering nodes must be at least $\sqrt[k]{T_{\mathrm{SNR}}} * d$ meters away from the receiver. We define this as the interference range R_{i} of the receiver regarding to a specific transmission with transmitter–receiver distance as d meters. Thus we have the formal definition of R_{i} as

$$R_{\mathrm{i}} = \sqrt[k]{T_{\mathrm{SNR}}} * d. \tag{4}$$

From Eq. (4), it is easy to see that when the transmitter–receiver distance d is larger than $R_{\mathrm{tx}} * T_{\mathrm{SNR}}^{-1/k}$, interference range then exceeds the transmission range R_{tx}. In practice, T_{SNR} is usually set to 10. Under the TWO-RAY GROUND pathloss model, k is equal to 4. Then we have interference range as $R_{\mathrm{i}} = \sqrt[4]{10} * d = 1.78 * d$. When d is larger than $0.56 * R_{\mathrm{tx}}$, R_{i} is larger than R_{tx}. This is easy to understand that power level needed for interrupting a transmission is much smaller than that of successfully delivering a packet. With the formal definition of the interference range, we can now define the interference area A_{i} around a receiver as Eq. (5). All nodes located in the interference area are called hidden nodes of the receiver.

$$A_{\mathrm{i}} = \pi R_{\mathrm{i}}^2. \tag{5}$$

3.2. Effectiveness of RTS/CTS handshake

Since the major purpose of RTS/CTS handshake is to avoid interference caused by hidden nodes, it is interesting to evaluate how effective it is. To do so, we first define the effectiveness of RTS/CTS ($E_{\mathrm{RTS/CTS}}$) as below:

$$E_{\mathrm{RTS/CTS}} = \frac{A_{\mathrm{i}\cap\mathrm{RTS/CTS}}}{A_{\mathrm{i}}}. \tag{6}$$

Here, A_{i} is the total interference area defined in Eq. (5). $A_{\mathrm{i}\cap\mathrm{RTS/CTS}}$ represents part of the interference area where nodes can receive RTS or CTS successfully. When $d \leqslant R_{\mathrm{tx}} * T_{\mathrm{SNR}}^{-1/k}$, apparently $A_{\mathrm{i}\cap\mathrm{RTS/CTS}}$ is equal to A_{i} since transmission range is now larger than the interference range. Thus, $E_{\mathrm{RTS/CTS}}$ is equal to 1. When d increases beyond $R_{\mathrm{tx}} * T_{\mathrm{SNR}}^{-1/k}$, $A_{\mathrm{i}\cap\mathrm{RTS/CTS}}$ becomes smaller than A_{i}, resulting the $E_{\mathrm{RTS/CTS}}$ smaller than 1. $E_{\mathrm{RTS/CTS}}$ further decreases along with the increase of d. The upper bound of d is R_{tx} since if d is larger than R_{tx}, the two nodes are out of range of each other. The situation that d is larger than $R_{\mathrm{tx}} * T_{\mathrm{SNR}}^{-1/k}$ and smaller than R_{tx} is illustrated in Fig. 1.

From Fig. 1, we can approximately calculate the $E_{\mathrm{RTS/CTS}}$ when d is within $[T_{\mathrm{SNR}}^{-1/k} * R_{\mathrm{tx}}, R_{\mathrm{tx}}]$. The dark shaded area in Fig. 1 represents part of the interference area which is not covered by RTS/CTS handshake (e.g. $A_{\mathrm{i}} - A_{\mathrm{i}\cap\mathrm{RTS/CTS}}$). To calculate

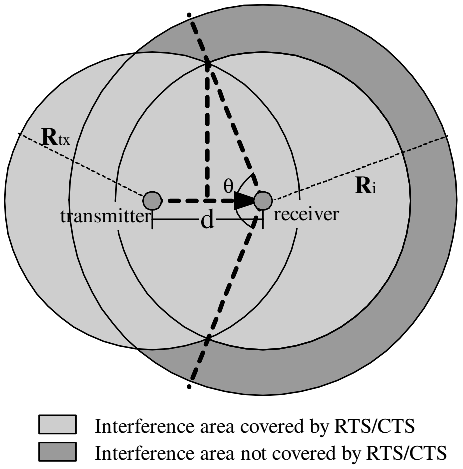

Rtx
Ri
θ
transmitter
d
receiver
Interference area covered by RTS/CTS
Interference area not covered by RTS/CTS

Fig. 1. Effectiveness of RTS/CTS handshake when d is larger than $T_{\mathrm{SNR}}^{-1/k} * R_{\mathrm{tx}}$ and smaller than R_{tx}.

this area, we should first calculate the angle Θ as shown in Fig. 1.

$$\cos\left(\frac{\Theta}{2}\right) = \frac{d/2}{R_{\mathrm{tx}}} \Rightarrow \Theta = 2\arccos\left(\frac{d}{2R_{\mathrm{tx}}}\right). \qquad (7)$$

We approximately calculate the shaded area in Fig. 1 as $\frac{2\pi-\Theta}{2\pi}(\pi R_{\mathrm{i}}^2 - \pi R_{\mathrm{tx}}^2)$. Thus, the interference area covered by RTS/CTS is given as

$$A_{\mathrm{i}\cap\mathrm{RTS/CTS}} = \pi R_{\mathrm{i}}^2 - \frac{2\pi - \Theta}{2\pi}(\pi R_{\mathrm{i}}^2 - \pi R_{\mathrm{tx}}^2). \qquad (8)$$

The total interference area is given as $A_{\mathrm{i}} = \pi R_{\mathrm{i}}^2$. Thus, we get

$$E_{\mathrm{RTS/CTS}} = \begin{cases} 1 \quad \text{if } 0 \leqslant d \leqslant T_{\mathrm{SNR}}^{-1/k} * R_{\mathrm{tx}}, \\ 1 - \frac{\left[\pi - \arccos\left(\frac{d}{2R_{\mathrm{tx}}}\right)\right]\left[d^2 * T_{\mathrm{SNR}}^{2/k} - R_{\mathrm{tx}}^2\right]}{\pi d^2 * T_{\mathrm{SNR}}^{2/k}} \\ \quad \text{if } T_{\mathrm{SNR}}^{-1/k} * R_{\mathrm{tx}} < d \leqslant R_{\mathrm{tx}}. \end{cases} \qquad (9)$$

To see the effectiveness of RTS/CTS handshake clearly, we plot Eq. (9) in Fig. 2 for TWO-RAY GROUND model (e.g. $k = 4$) and SNR-THRESHOLD (T_{SNR}) as 10. The X-axis of Fig. 2 is the transmitter–receiver distance d. Y-axis is the effectiveness of RTS/CTS handshake ($E_{\mathrm{RTS/CTS}}$). Clearly when d exceeds a certain value (for this specific case, the value is $0.56 * R_{\mathrm{tx}}$), the effectiveness of RTS/CTS handshake drops rapidly. In such situations, many collisions may happen due to the large interference range and hidden terminal problem. Certainly this is not as people expected in theory.

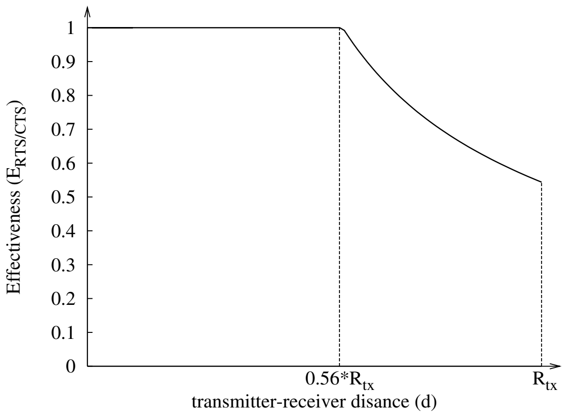


Fig. 2. Effectiveness of RTS/CTS handshake for TWO-RAY GROUND model and SNR threshold as 10.

3.3. Influence of physical carrier sensing

The effectiveness of RTS/CTS can be improved by the physical carrier sensing (CSMA part of IEEE 802.11 MAC which is known as CSMA/CA) performed at each node before it starts a transmission. However, since interference happens at receivers while carrier sensing is detecting transmitters (the same situation as hidden terminal problem which inspires the RTS/CTS handshake), physical carrier sensing cannot help too much. We demonstrate how carrier sensing helps reducing interference in Fig. 3.

Three dotted circles in Fig. 3 represent three different carrier sensing ranges. R_{cs1} represents the ordinary case where carrier sensing range is slightly larger than the transmission range. Such physical carrier sensing cannot reduce the uncovered interference area much. If we can further increase the carrier sensing range to R_{cs3} (equal to $(d + R_{\mathrm{i}})$) as shown in Fig. 3, we can now totally cover the interference area. Interestingly, when the carrier sensing range exceeds R_{cs2} (equal to $(d + R_{\mathrm{tx}})$), all the area covered by RTS/CTS handshake is now totally covered by carrier sensing. That means when the carrier sensing range is larger than $(d + R_{\mathrm{tx}})$, RTS/CTS is no longer

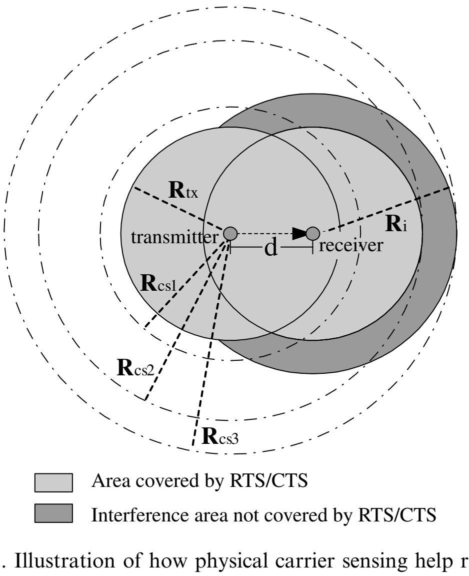


Fig. 3. Illustration of how physical carrier sensing help reducing interference.

needed! Three issues are concerned for such a large carrier sensing range. First, carrier sensing range is usually a fixed range. Adaptively adjusting this range according to different transmitter–receiver distance d would be complex. Thus, the maximum values of R_{cs2} and R_{cs3} when d equals to R_{tx} should be taken, which are $2 * R_{tx}$ and $R_{tx} + 1.78 * R_{tx} = 2.78 * R_{tx}$ respectively (under assumption of TWO-RAY GROUND pathloss model). Second, the carrier sensing range is decided by the sensitivity of antennas. Thus there is a hardware limitation. Third, too large carrier sensing range will reduce the network throughput significantly. All nodes outside of interference range of receiver but still within the carrier sensing range of the transmitter have to defer for current transmission, although most of them would not cause interference at the receiver. Thus, the spatial reuse is reduced significantly.

Through the analysis and discussions above, we draw following conclusions:

- The interference range at a node is not fixed as the transmission range. It is receiver centered and related to transmitter–receiver distance.
- RTS/CTS handshake is not sufficient enough to reserve the total interference area of the receiver when the transmitter–receiver distance is larger than $T_{SNR}^{-1/k} * R_{tx}$.
- A physical carrier sensing range larger than transmission range can help reducing interference. However, big carrier sensing range is not desired due to hardware limitations and significant throughput reduction.

As an end of this section, we list some hardware parameters of Lucent ORiNOCO wireless card in Table 1. Here, we only list the parameters for open space environment with transmission rate as 2 Mbps [8]. Note, the carrier sensing range is not directly from Lucent. We calculated it according to other parameters.

Table 1
Hardware characteristics of the Lucent ORiNOCO wireless card

Parameter name	Values
Transmission rate	2 Mbps
Transmission power (P_t)	15 dBm
Transmission range (R_{tx})	400 m
Receiver sensitivity	−91 dBm
Carrier sensing range (R_{cs})	670 m

4. Problem caused by large interference range

In this section, we investigate how the large interference range affects the network performance. The effect of interference to the capacity of a single chain is discussed in [2], where NS2 simulator is used and the transmission range and interference range are set to 250 and 550 m respectively. The topology of a single chain is illustrated as in Fig. 4 and the distance between neighbor nodes is 200 m. Clearly, if not considering the large interference range, the capacity of this single chain is 1/3 of the channel bandwidth, which is 2 Mbps. (Considering the overhead of RTS, CTS, etc, the authors of [2] give the achievable channel bandwidth as 1.7 Mbps.) The reason is the spatial reuse constrain. When node 1 is transmitting to node 2, node 2 and node 3 cannot transmit at the same time. Thus, capacity is reduced to 1/3 of the channel bandwidth. However, if the large interference range is considered, this capacity is further reduced to 1/4 of the channel bandwidth since now node 4 also cannot transmit concurrently with node 1 since it will interrupt the reception at node 2. (An interference range as large as 550 m is used in [2].) This is certainly a significant reduction to the network capacity.

Several things need to be noticed with above discussion. First, in [2] a fixed interference range as large as 550 m is used, which is more than twice of the transmission range (e.g. 250 m). From our derivation in this paper, we notice that the interference range is not a fixed range. It depends on the distance between the transmitter and the receiver. Second, according to our analysis, the interference range is around 1.78 times the transmitter–receiver distance under TWO-RAY

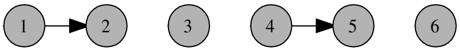


Fig. 4. Influence of interference to the capacity of a chain.

GROUND pathloss model. Thus, for the topology in Fig. 4, the interference range is around 356 m. It means node 4 actually cannot interrupt reception at node 2. However, the capacity reduction due to interference is still clear, although may not be exactly 1/4. Actually, whether node 4 can interfere with node 2 is totally dependent on the distance from node 2 to node 3 and from node 3 to node 4. For example, if the distance of node 2 to node 3 and node 3 to node 4 is slightly reduced to 150 m, then node 4 can interfere with node 2 again. Third, the most important thing we want to stress is that IEEE 802.11 itself can schedule the transmissions of node 1, 2, and 3 very well with the help of RTS/CTS. That is node 2 and node 3 will defer while node 1 is transmitting. However, it cannot schedule the concurrent transmissions of node 1 and node 4 since node 4 is out of transmission range of node 1 and node 2. It cannot hear the CTS packet from node 2. Thus, even an upper bound of capacity considering of interference is given as 1/4 of the channel bandwidth, IEEE 802.11 MAC cannot achieve this bandwidth since a lot of bandwidth will be wasted due to collisions.

To further demonstrate the performance degradation due to large interference range, we did a simple experiment using QualNet simulator [9]. (More detailed description of QualNet is provided at Section 6.1.) The topology of our experiment is demonstrated in Fig. 5. The distance from node 1 to node 2 and node 3 to node 4 is fixed as 300 m. Transmission range of the wireless radio is 367 m with channel bandwidth as 2 Mbps following the standard. We vary the vertical distance between node 3, 4 and node 1, 2 to check the influence of large interference range. Two CBR sessions based on UDP are involved with directions from node 1 to node 2 and node 4 to node 3 correspondingly. Since the CBR is constant rate traffic without retransmissions, it is possible that the two flows may synchronize to each other rendering the results not general enough. To avoid the synchronization of the two flows, we slightly modified the CBR traffic generator. Given the rate as n packets per second (pps), we divided time into slots as $1/n$ seconds. In each time slot, a packet is sent to the network. Sending time of the packet is uniformly distributed in the whole slot.

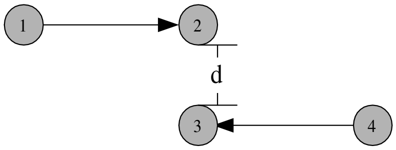


Fig. 5. Scenario for investigation of collisions due to large interference range.

Metrics we selected for our investigation are the aggregated throughput of the two flows and the MAC data packet corruption ratio. MAC data packet corruption ratio is defined as the portion of data packets transmitted at the MAC layer that are interrupted at the receiver due to interference. Two things have to be clarified here. First, IEEE 802.11 may retransmit same data packet several times (e.g. 4 times in most implementations) if no ACK is received. We count each retransmission as an independent data packet transmission. Second, several reasons may cause the drop of a data packet. For example a transmitter will drop a data packet when it retransmits the RTS several times (e.g. 7 times in most implementations) without getting a CTS back. In our experiments, we only count those data packet drops corrupted by interference at the receiver. Experiment results are reported in Figs. 6–9.

In Figs. 6 and 7, the packet rates of two CBR flows are set to 800 Kbps with packet size 1024 bytes (thus 100 pps). The packet rate of CBR is selected as

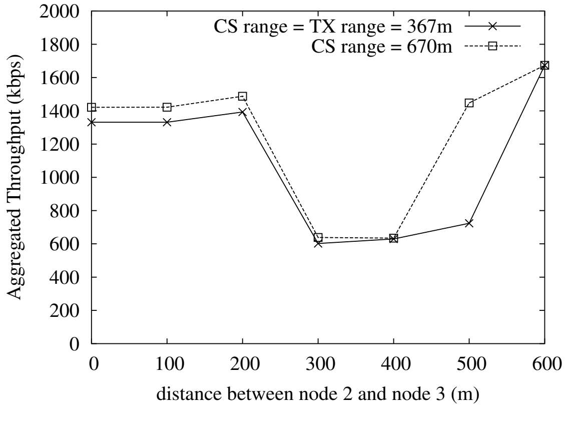


Fig. 6. Aggregated throughput vs. distance between node 2 and node 3.

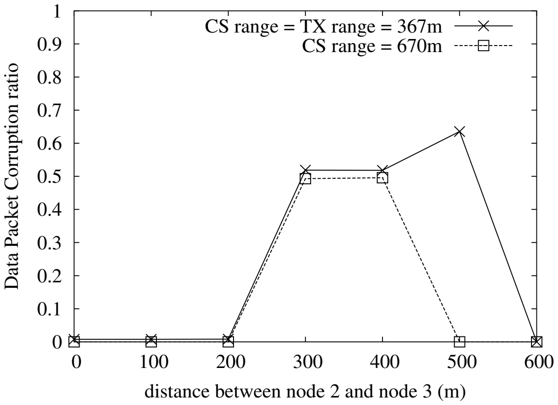


Fig. 7. Packet corruption ratio vs. distance between node 2 and node 3.

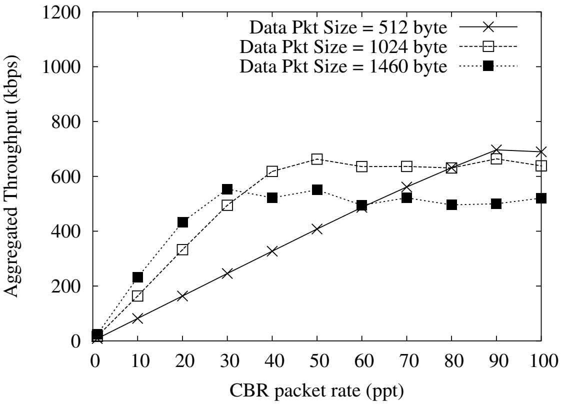


Fig. 8. Aggregated throughput vs. CBR packet rate and size.

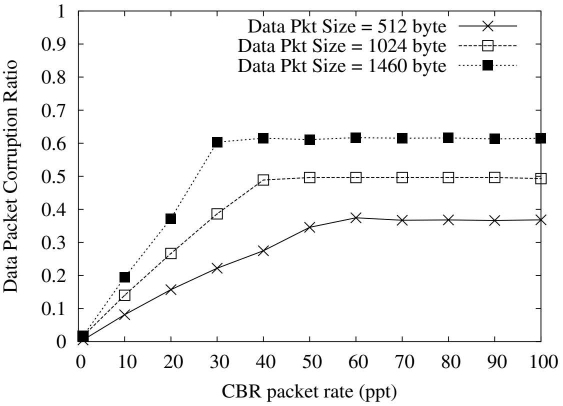


Fig. 9. Packet corruption ratio vs. CBR packet rate and size.

to utilize the full bandwidth when the two flows share the channel (e.g. the available channel bandwidth to each flow is 1.7 Mbps/2 = 850 Kbps). It is interesting to notice that when the distance between node 2 and node 3 is 300, 400 and 500 m, the aggregated throughput in Fig. 6 is dramatically decreased. This is controversial to our common impression. When node 2 and node 3 is 400 m away, they are already out of transmission range of each other. Thus, the two connections should be able to reuse the channel. However, the throughput is even worse than when the two nodes are within transmission range of each other. This is contributed by the large interference range and ineffectiveness of RTS/CTS for resolving hidden terminal problems under such situations. For example, when node 4 is out of the transmission range of node 2, it cannot successfully receive the CTS packet of node 2. However, since it is still in the interference range of node 2, transmission from node 4 will interrupt any packet reception at node 2 (same thing happens to node 1 and node 3). Only when node 3 and node 4 are all out of interference range of node 2 (e.g. distance of node 2 and node 3 is larger than 500 m), the two connections are fully separated from each other. The data packet corruption ratio shown in Fig. 7 clearly confirms this. Figs. 6 and 7 also demonstrate that physical carrier sensing cannot help reducing interference too much. Clearly, it is only helpful when distance of node 2 and node 3 is around 500 m for the investigated scenario. Under this situation, node 4 is out of interference range of node 2 and node 1 is out of interference range of node 3. However, node 2 and node 3 are still within interference range of each other. Under IEEE 802.11, node 2 and node 3 have to transmit CTS and ACK packets, although they do not transmit any data packet. Such transmissions make these two nodes also interfere with each other. With help of physical carrier sensing, node 2 and node 3 can avoid interfering with each other. However, when interference is caused by node 1 and node 4 (e.g. 300 and 400 m cases), carrier sensing range as large as 670 m cannot reduce such interference since node 1 and node 4 are too far away from each other to sense the ongoing transmissions.

We further investigate the relationship between the rates of a node sending out data packets and the MAC data packet corruption ratio due to interference. Different data packet size is also explored. In this experiment, we fixed the distance between node 2 and node 3 as 300 m. Simulation results are given in Figs. 8 and 9.

From Figs. 8 and 9 we can see that when the packet rate of CBR sessions is smaller than 10 pps, there are only little interference. This is easy to understand since when traffic is light, the probability that two nodes transmit at the same time is small. When the packet rate is increased, the data packet corruption ratio is increased quickly as shown in Fig. 9. Data packet size also affects the data packet corruption ratio greatly. Apparently, when data packet size is large, the transmission time of a data packet is also long. Then the probability a data packet is corrupted will be much higher. This leads to a dilemma that to fully utilize the channel bandwidth (e.g. reduce the overhead of RTS/CTS), larger data packet size is preferred. However, larger data packet size will waste much bandwidth since many data packets are corrupted due to large interference range. Fig. 9 clearly shows that increasing data packet size from 512 to 1024 bytes, around 15% more data packets are corrupted. This is confirmed when data packet size is further increased to 1460 bytes. The aggregated throughput in Fig. 8 also confirms our conclusion. When traffic is light, increasing the data packet size can improve the network throughput. However, when traffic is heavy, larger data packet size actually degrades the network performance due to the fact that more data packets are corrupted by interference.

In [3,10], the authors also discovered that large interference range is one of the major factors which cause poor performance and significant capture/unfairness problem of TCP flows (namely TCP unfairness). In conclusion, we would like to point out again that since IEEE 802.11 is unable to solve collisions caused by large interference range effectively, it hurts the network performance significantly in various aspects.

5. Proposed solutions

As shown in Section 3, the ineffectiveness of RTS/CTS handshake on resolving large interference range will cause significant data packet corruptions at the MAC layer and in turn wastes channel bandwidth and degrades the network performance. In this section, we propose two solutions to attack this problem. The first scheme is a simple MAC layer scheme based on the IEEE 802.11 MAC with some minor modifications. Another solution is to adopt the RBF antennas. RBF antennas are one kind of directional antennas. It can lock on the direction where the signal from for receiving. Thus ignores interference from other directions.

5.1. A simple MAC layer solution: conservative CTS reply

We propose a MAC layer scheme called conservative CTS reply (CCR) to help IEEE 802.11 MAC combat the large interference range. The main idea is that a node only replies a CTS packet for a RTS request when the receiving power of that RTS packet is larger than a certain threshold (CTS-reply-threshold) (e.g. not reply CTS to remote node since the transmission is easy to be interrupted), even if the RTS packet is received successfully and this node is idle. This CTS-reply-threshold should be larger than the threshold required for a node to successfully receive a packet. For example, let $P_{r0.56}$ denote the receiving power at a receiver which is $0.56 * R_{tx}$ away from the transmitter when there is no interference from other nodes. If we use $P_{r0.56}$ as the CTS-reply-threshold, ideally a node only replies CTS packets to those nodes which are at most $0.56 * R_{tx}$ meters away. Since when the transmitter–receiver distance is smaller than $0.56 * R_{tx}$, all interference area is covered by RTS/CTS handshakes, we can totally eliminate the data packet collisions caused by large interference range. The drawback is that our scheme actually reduces the effective transmission range to resolve the interference. Clearly this is a tradeoff. In practice, the CTS-reply-threshold can be adjusted to achieve an optimal network throughput.

Our modifications as CCR for IEEE 802.11 result an inconsistency between broadcasting and unicasting since in IEEE 802.11, broadcast packets are not protected by RTS/CTS handshake.

Unfortunately, most routing protocols in MANETs use broadcast for route discovery. Thus, an undesirable situation may happen that the routing protocols will discover a link, which may be disabled by our scheme if the two nodes of that link are too far away from each other. To solve this problem and maintain consistency of broadcasting and unicasting of IEEE 802.11, we also require a node to drop broadcast packets if the receiving power of that packet is below CTS-reply-threshold.

The major disadvantage of the CCR scheme is the reduced effective transmission range, thus lower network connectivity. This can be complemented by increasing the network density. Actually, the network density is usually decided according to the transmission range of the wireless radios. Thus, when a MANET is deployed, the network density now should take into account of the effective transmission range if our scheme is applied.

5.2. A physical layer solution: receiving beam forming antenna

Directional antennas have become a very active research field in recent several years. It is capable to eliminate undesired interference from competing stations. In this paper, we will show that by adopting directional antennas, the problem of large interference range can be reduced. The antenna we used is a simple type of directional antenna, which can lock on and receive signals from a certain direction. The transmission is still omnidirectional. We call such an antenna as a RBF antenna. RBF antennas can be used transparent to the MAC layer. In this paper, we use standard IEEE 802.11 MAC on top of the RBF antennas.

One implementation of a RBF antenna is the switched beam forming antenna. It has multiple antenna patterns, which aim to different directions. Usually, one pattern is targeting one direction and yields a higher antenna gain in that direction. The multiple patterns are combined to cover the whole 360° direction. When the radio senses a signal, it will look up the best pattern, which gives the strongest receiving power, and lock onto that pattern for the entire reception. Signals from other directions then have low antenna gains, thus unlikely to interfere with current reception unless the interfering signal is very strong or it comes from the same direction with the desired signal. An illustration of a RBF antenna is given in Fig. 10. Here, we only draws one pattern includes a main lobe and two small side lobes. In this work, for simplicity, we use an abstract model of the directional antenna as illustrated in Fig. 11. We view the directional antenna as a sector with beam width as β (e.g. we ignore the side lobes). In the

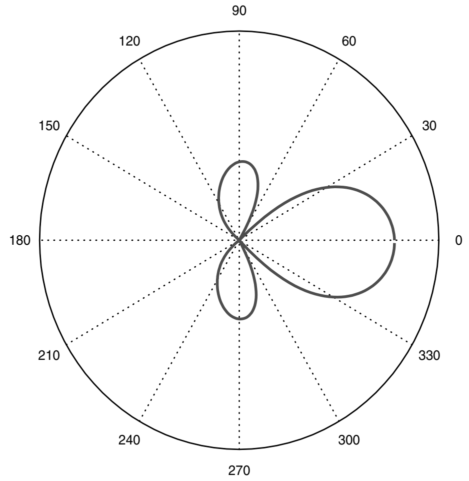


Fig. 10. A directional antenna.

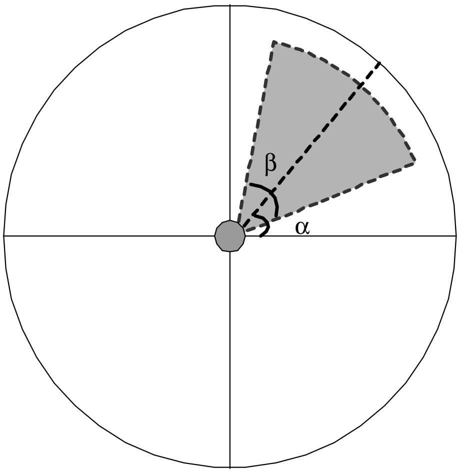


Fig. 11. Abstract model of the antenna.

abstract model, a pattern of the directional antenna is decided by two angels α and β as shown. Angle α is called the angel of direction which indicates the direction that a pattern aims to. Angle β is the width of the beam formed by the antenna. The smaller the angle β, the better it can prevent interference from other directions. Of course, the smaller it is, the more patterns a RBF antenna has to maintain, thus more overhead and more expensive as well as larger physical size.

Now, we prove that once the beam width smaller than a certain value, the interference due to larger interference range can be mostly prevented. As shown in Fig. 12, the angle γ indicates the upper bound of the beam width of a RBF antenna. S and R denote the sender and receiver of a transmission correspondingly. We draw the transmission range and the interference range of S and R as shown in Fig. 12. Nodes within the transmission ranges of S and R will hear RTS or CTS or both. Thus they would not send out packets. That area is marked as the RTS/CTS cleaned area. Nodes within the interference range of sender S will also defer when they sense the channel busy. That area is marked as physical carrier sensing cleaned area. Only those nodes in the area marked as interference area in Fig. 12 can interfere with the receiving at R. So, if the beam width of a pattern used for receiving is smaller than angle γ, we can reasonably expect that nodes in the original interference area now are prevented from interfering with current transmission. From Fig. 12, we can approximately get

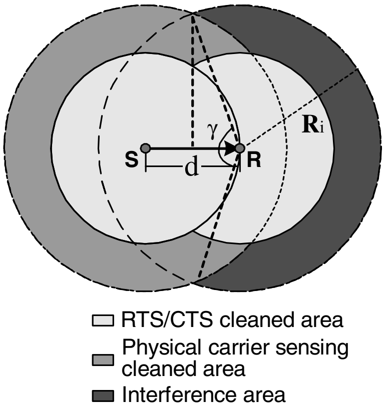


Fig. 12. Upper bound of the beam width.

$$\cos\left(\frac{\gamma}{2}\right) = \frac{d/2}{R_{\mathrm{i}}} = \frac{d}{2\sqrt[k]{T_{\mathrm{SNR}}} * d}, \tag{10}$$

$$\gamma = 2\arccos\left(\frac{1}{2\sqrt[k]{T_{\mathrm{SNR}}}}\right). \tag{11}$$

For the common open space environment, as derived in the previous sections that the interference range under TWO-RAY GROUND model is $1.78 * d$. Accordingly, we get γ as $2 * \arccos(1/(2 * 1.78)) \approx 147°$. Thus, to eliminate most interference due to large interference range, the beam width of a RBF antenna must be smaller than 147°, which is easy to fulfill in practice. In our future simulations, we use the RBF antenna with beam width as 45°.

6. Performance evaluation

6.1. Simulation platform and basic simulation scenario

All simulations in this paper are done using QualNet simulator [9], which is the successor of GloMoSim [11] simulation library. According to [12], QualNet incorporates a detailed model of the physical channel and of the IEEE 802.11 MAC layer. The TWO-RAY GROUND pathloss model and the RBF antenna are also implemented. Thus, it provides a good platform for our study of different radio ranges.

The simulation scenario configured in our experiments is consisting of 100 mobile nodes randomly deployed in a 2500 m × 1000 m field. Most physical and MAC layer parameters are set according to the open space environment following the IEEE 802.11 standard and Lucent wireless cards. The pathloss model adopted is the TWO-RAY GROUND model. Channel bandwidth is 2 Mbps. The transmission power is 15 dB m, resulting a transmission range as 367 m. The antenna sensitivity is −91 dB m yielding a carrier sensing range as 670 m. All these parameters match that of Lucent ORiNOCO wireless card listed in Section 3 very well. Routing protocol adopted is the DSDV [13] routing. Applications for generating traffic are randomly selected UDP based CBR flows with packet size as 1024 bytes and packet rate as 10 pps.

The major metrics used are (1) MAC data packet corruption ratio, (2) aggregated throughput of all CBR flows, (3) data packet delivery ratio of CBR flows, and (4) average data packet delay of the CBR flows. The MAC data packet corruption ratio has been defined in Section 4. We only count the corruption ratio of unicast data packets, thus exclude routing packets which are broadcast based. Aggregated throughput is the sum of the throughput of all CBR flows at the end of simulation. Data packet delivery ratio is the total number of data packets received at the receiver divided by total number of data packets sent out by the senders. Average data packet delay is the average end-to-end delay of data packets from senders to receivers.

6.2. Effect of large carrier sensing range

From the discussions in Section 3, we have seen that increasing the physical carrier sensing range can help reducing interference due to the large interference range. Moreover, in popular network simulators like NS2, GloMoSim, QualNet, the default carrier sensing range is usually almost twice of the default transmission range. For example, in NS2 simulator, the default transmission range is 250 m, while the default carrier sensing range is 550 m. The default values in QualNet are 367 and 670 m correspondingly. In this section, we verify that such a large carrier sensing range is helpful in terms of improving network performance. It is worth mention here that except the large interference range pointed out in previous sections, larger carrier sensing range is necessary also because the interfering noise is usually accumulated. Multiple concurrent transmitters far away may also cause strong interference if their signals are accumulated. Thus, usually the physical carrier sensing range should be larger than transmission range for detecting possible interfering signals as well as environmental noise before a node starts its own transmission. The drawback of large carrier sensing range is that it may overprevent concurrent transmissions for efficient channel utilization since all nodes within the carrier sensing range of the sender need to defer to its transmission.

In this experiment, the original IEEE 802.11 MAC protocol is examined under different carrier sensing ranges from 367 m (e.g. equal to transmission range) to 670 m (e.g. default carrier sensing range in QualNet). Further larger carrier sensing range may over the hardware limitation. Thus, we didn't further increase it. The traffic is 20 randomly selected CBR flows, which is quite high load. The experiment results are given in Figs. 13–15. The X-axis of these figures is the different carrier sensing ranges in terms of the antenna sensitivity given as power levels. Its meaning is that when the antenna senses a signal with power larger than that value, it considers the channel as busy. The corresponding carrier sensing ranges are also given in the figures.

From Fig. 13 we observe that the increase of carrier sensing range indeed can reduce MAC layer data packet corruption ratio in some degree. This is also reflected in the network performance as the increase of aggregated throughput (Fig. 14) and packet delivery ratio (Fig. 15). However, as we pointed out, since carrier sensing is detecting the transmitter, while interference happens at the receiver, increasing the carrier sensing range cannot effectively prevent all collisions. Since larger car-

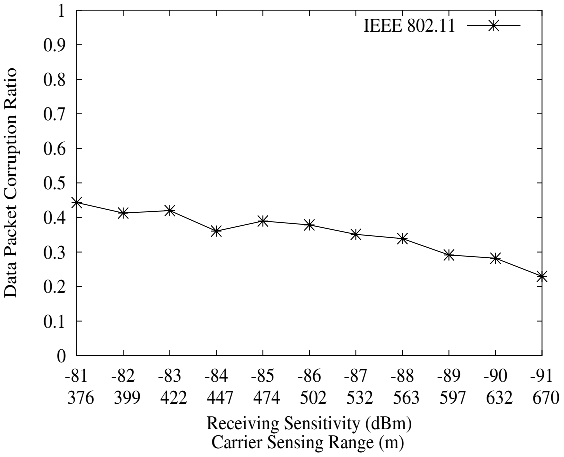


Fig. 13. Packet corruption ratio vs. CS range.

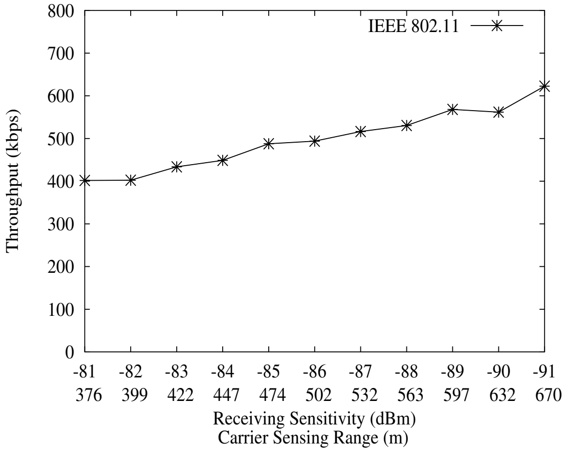


Fig. 14. Aggregated throughput vs. CS range.

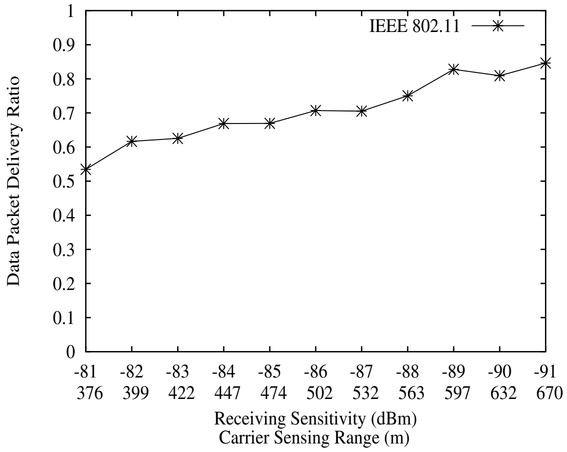


Fig. 15. Data packet delivery ratio vs. CS range.

rier sensing range is good for reducing interference, in the rest of simulations, we use the carrier sensing range as 670 m.

6.3. Optimal values of CTS-reply-threshold

In this series of experiments, we want to identify the optimal value of the CTS-reply-threshold used in the proposed CCR scheme. The higher this threshold, the better it can reduce interference. However, it also decreases the effective transmission range, resulting long-hop paths, potentially worsen the network performance. The CTS-reply-threshold is the key for this tradeoff. Thus, in these experiments, we give different values of this threshold from −81 to −72 dB m to determine the optimal threshold. −81 dB m is equal to the packet reception threshold, which means any correctly received RTS will be replied. This is same as the original IEEE 802.11. When we increase this threshold above −81 dB m, some RTS's from nodes within the transmission range but not close to the receiver will be ignored. The perfect threshold under which all potential interference are prevented is given as $P_{r0.56}$ as derived in the Section 5.1 for the TWO-RAY GROUND model. In QualNet simulator, it equals to −71.6 dB m. Thus, there is no need to further increase the CTS-reply-threshold. The experiment results are presented in Figs. 16–18. The X-axis of these figures is the different values of the CTS-reply-threshold of the CCR scheme in terms of signal reception power. The corresponding effective transmission ranges resulted from the CCR scheme using these threshold values are also given in the figures.

From Fig. 16 we observe that CCR is capable to reduce most interference once the CTS-reply-threshold exceeds −76 dB m (equal to effective transmission range as 282 m). Further increase of this threshold has no much gain and may result in degradation of network performance as observed in Fig. 17. In Fig. 17, the aggregated throughput also reaches the maximum at −76 dB m. Further

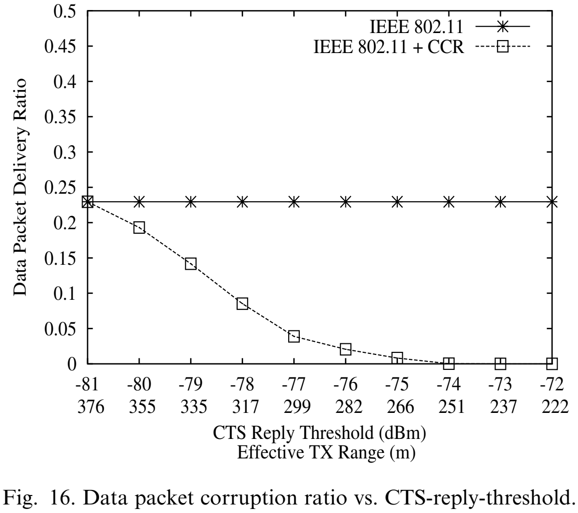


Fig. 16. Data packet corruption ratio vs. CTS-reply-threshold.

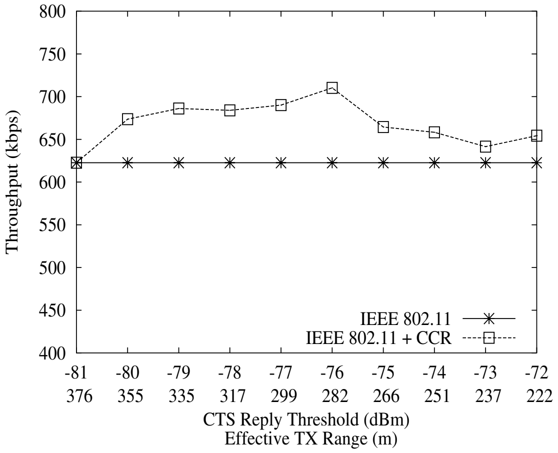


Fig. 17. Aggregated throughput vs. CTS-reply-threshold.

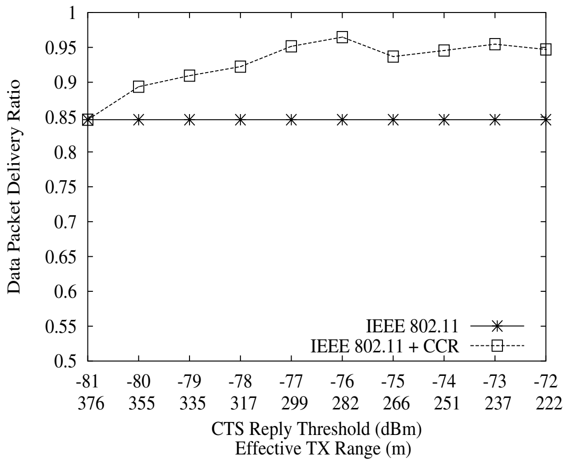


Fig. 18. Data packet delivery ratio vs. CTS-reply-threshold.

increase of the threshold gives less throughput. This is due to the increase of path length from end to end as a result of the decrease of the effective transmission range. Longer paths (in terms of number of hops) trigger more packet forwarding at the intermediate nodes consuming more bandwidth. Thus, too higher threshold values may actually degrade the network performance. This is also confirmed in Fig. 18, where the packet delivery ratio reaches the highest point also at −76 dB m although further increase of the threshold does not trigger too much degradation. From this series of experiments, we conclude that the optimal value of the CTS-reply-threshold is around −76 dB m. Further increase of the threshold may cause too much overhead without visible gain. In the rest of the simulations in the next section, we will set the value of the CTS-reply-threshold as −76 dB m. The corresponding effective transmission range is then 282 m.

6.4. Comparison of CCR and RBF antennas

After the optimal value of the CTS-reply-threshold of the CCR scheme is decided, in this section, we compare the CCR scheme and RBF antennas for investigating their usefulness of eliminating interference due to large interference range. The simulation scenario used here is same to previous experiments. We fix the CS range as 670 m and the CTS-reply-threshold as −76 dB m. We then vary the traffic load from 2 CBR flows to 20 CBR flows to compare the two proposed solutions. Experiment results are presented in Figs. 19–22.

In these figures, the curve titled "IEEE 802.11" represents the results using original IEEE 802.11 MAC. Curve titled "IEEE 802.11 + CCR" is the results using IEEE 802.11 with the CCR scheme. Curve with title "IEEE 802.11 + RBF antenna" represents experiment results using original IEEE 802.11 at MAC layer and RBF directional antenna model at the physical layer. From Fig. 19, we can see that the original IEEE 802.11 encounters a lot

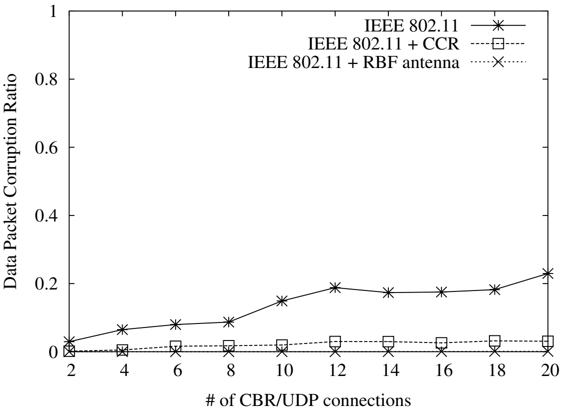


Fig. 19. Data packet corruption ratio vs. # of CBR pairs.

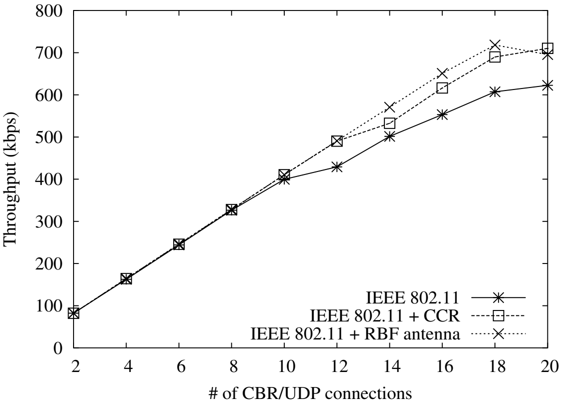


Fig. 20. Aggregated throughput vs. # of CBR pairs.

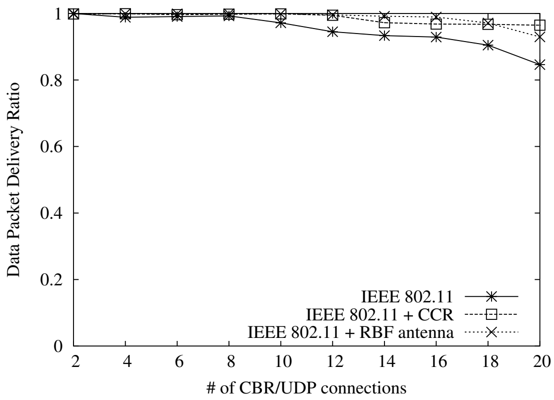


Fig. 21. Data packet delivery ratio vs. # of CBR pairs.

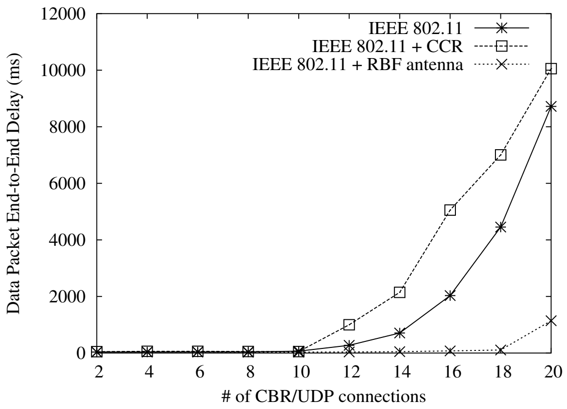


Fig. 22. Average data packet end-to-end delay vs. # of CBR pairs.

of MAC data packet corruptions due to interference when the network load is increased. The CCR scheme and the RBF antenna are both capable to prevent such data packet corruptions. More precisely, CCR scheme shows corruption rate always below 3% under heavy load, while that of the RBF antenna is always nearly zero. For network performance as aggregated throughput (Fig. 20) and data packet delivery ratio (Fig. 21), similar results are observed. CCR scheme and RBF antenna both capable to improve the network throughput and data packet delivery ratio. RBF antenna is only slightly better than CCR scheme. However, in Fig. 22, we observe that CCR scheme shows much longer average data packet delay even longer than that of the original IEEE 802.11 MAC. This is mainly due to the increase of the path length from end to end since the effective transmission range is reduced nearly 1/4 (e.g. from 367 to 282 m). The RBF antenna on the country shows very good performance with short packet delays. This is because it prevents a lot of interference which will cause longer packet delay when no RBF antenna is used (IEEE 802.11 adopts the binary exponential backoff scheme. The MAC layer delay increases quickly for packet retries). Its transmission range is also kept same to the original.

From the network performance aspect, RBF antenna outperforms the CCR scheme although both of them are capable to prevent interference due to large interference range. However, RBF antennas require additional hardware. The directional antennas are usually more expensive and with larger physical size. The CCR scheme in contrast is a pure MAC layer scheme without any special requirement of the hardware. It is much cheaper to implement and deploy. In conclusion, if the performance is the major concern and antenna size is not a big issue, then RBF antennas should be a good choice. If the expense and compatibility as well as antenna size is the major concern, then CCR scheme is preferred.

7. Conclusion

This paper has three major contributions. First, we analyze the interference range for the open space environment in detail. The effectiveness of RTS/CTS handshake in terms of resolving such kind of interference is also explored. We believe that such a quantified analysis would be helpful to research in ad hoc networks, especially those works targeting the network capacity, scheduling and TCP fairness etc. in ad hoc networks. Second, frequent data packet corruptions due to large interference range are verified through simulation experiments. The relationship between data packet corruption ratio and data packet size as well as traffic intensity is also investigated. Third, two schemes are proposed to combat the large interference range. The main advantages of each scheme are also discussed and investigated. RBF directional antennas give best network performance. However, it requires additional hardware, which are not easy to deploy. The CCR scheme is simple and only has trivial modifications to IEEE 802.11 standard. Thus, although more sophisticated MAC layer schemes (e.g. adjusting the transmission power, etc.) can be proposed, our scheme would be simpler and more practical. Simulation experiments also show that both solutions can eliminate most packet collisions due to large interference range.

Acknowledgements

This work is supported in part by ONR "MINUTEMAN" project under contract N00014-01-C-0016 and TRW under a Graduate Student Fellowship.

References

[1] F.A. Tobagi, L. Kleinrock, Packet switching in radio channels. Part II: The hidden terminal problem in carrier sensing multiple access and busy tone solution, IEEE Trans. Commun. COM-23 (12) (1975).

[2] J. Li, C. Blake, D. Couto, H. Lee, and R. Morris, Capacity of ad hoc wireless networks, in: Proceedings of ACM MobiCom'01, July 2001.

[3] S. Xu, T. Saadawi, Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks? IEEE Commun. Mag. 39 (6) (2001) 130–137.

[4] IEEE-802.11, Wireless LAN media access control (MAC) and physical layer (PHY) specifications. Available from <http://standards.ieee.org/getieee802>, 1999.

[5] C. Wu, V. Li, Receiver-initiated busy-tone multiple access in packet radio networks, ACM SIGCOMM'87 Workshop: Frontiers in Computer Communications Technology, August 1987.

[6] J.P. Monks, J.P. Ebert, A. Wolisz, W.W. Hwu, A study of the energy saving and capacity improvement potential of power control in multi-hop wireless networks, in: Proceedings of Workshop on Wireless Local Networks, November 2001.

[7] T. Rappaport, Wireless Communications: Principles and Practice, Prentice Hall, Englewood Cliffs, NJ, 1996.

[8] Hardware specifications of Lucent ORiNOCO wireless PC card. Available from <http://www.orinocowireless.com>.

[9] Qualnet simulator. Available from <http:www.qualnet.com>.

[10] K. Xu and M. Gerla, TCP over an IEEE 802.11 ad hoc network: Unfairness problems and solutions, UCLA Computer Science Department Technical Report TR020019, May 2002.

[11] X. Zeng, R. Bagrodia, M. Gerla, GloMoSim: a library for parallel simulation of large-scale wireless networks, in: Proceedings of PADS'98, May 1998.

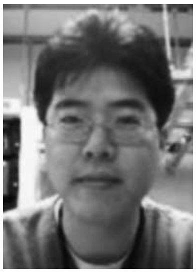
[12] M. Takai, J. Martin, R. Bagrodia, Effects of wireless physical layer modeling in mobile ad hoc networks, in: Proceedings of ACM MobiHoc'01, October 2001.

[13] C. Perkins, P. Bhagwat, Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers, in: Proceedings of ACM SIGCOMM'94, August 1994.

Kaixin Xu is a Ph.D. student of the computer science department at UCLA. He joined the Network Research Laboratory (NRL) of UCLA at 2000. His research focuses on the ad hoc wireless networking especially protocols at MAC, Network and Transport layers. His recently work includes enhancing TCP performance in multihop ad hoc networks, TCP performance in IEEE 802.11 MAC based ad hoc networks, as well as MAC protocols for utilizing directional antennas and mobility track. He is also working on network protocols for building hierarchical ad hoc networks.

Mario Gerla was born in Milan, Italy. He received a graduate degree in engineering from the Politecnico di Milano, in 1966, and the MS and Ph.D. degrees in engineering from UCLA in 1970 and 1973, respectively. He joined the Faculty of the UCLA Computer Science Department in 1977. His research interests cover the performance evaluation, design and control of distributed computer communication systems; high speed computer networks; wireless LANs (Bluetooth); ad hoc wireless networks. He has been involved in the design, implementation and testing of wireless ad hoc network protocols (channel access, clustering, routing and transport) within the DARPA WAMIS, GloMo projects

and most recently the ONR MINUTEMAN project. He has also carried out design and implementation of QoS routing, multicasting protocols and TCP transport for the Next Generation Internet. He is currently an associate editor for the IEEE Transactions on Networking.



Sang H. Bae is a Principal Engineer, Communications Networks, Boeing Phantom Works. Presently conducting simulation study of QoS-based composite routing for Joint Tactical Radio System (JTRS) system. Prior to Boeing, five years as researcher at Network Research Laboratory in UCLA responsible for wireless network systems development and designing, experimental studies of TCP and wireless MAC interaction and system engineering. Developed and implemented On Demand Multicast Routing Protocol. He received the Ph.D. form Computer Science, UCLA, and MS in Computer Science, California State University, and BS in Information and Computer Science, California State University.