How Effective is the IEEE 802.11 RTS/CTS Handshake in Ad Hoc Networks?

Kaixin Xu, Mario Gerla, Sang Bae
University of California, Los Angeles
Computer Science Department
Los Angeles, CA 90095, 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. Then, a simple MAC layer scheme is proposed to solve this problem. Simulation results verify that our scheme can help IEEE 802.11 resolve most interference caused by large interference range.**

I. INTRODUCTION

In wireless networks, interference is location based. Thus, the hidden terminal problem may happen frequently [10]. 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 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. 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 solve this problem, a simple MAC layer scheme is proposed to help IEEE 802.11 combat the large interference range. Simulation results show that our scheme is a great improvement over IEEE 802.11 MAC.

The rest of this paper is organized as following. In section II, 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 III, we identify the problems caused by large interference range. In Section IV, a simple MAC layer scheme based on IEEE 802.11 is proposed and evaluated. Related work is given in section V and we conclude the paper in section VI.

II. EFFECTIVENESS OF RTS/CTS HANDSHAKE

As we have pointed out the RTS/CTS handshake of IEEE 802.11 does not work well as we expected in theory. It cannot prevent hidden terminal problems completely. In this section, we explain this through a theoretical analysis. For better explanation, we first review the three radio ranges: 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 (ie, 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.

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

- **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.

A. *Large Interference Range and the Interference Area*

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. In this subsection, we investigate the interference range and its relationship to the transmission range. 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, the receiving power is mostly decided by path loss over the transmitter-receiver distance, which models the signal attenuation over the distance. Here we ignore multipath fading and shadowing since they are minor factors in the open space environment. In the open space environment, path loss of a signal is usually modeled as the **TWO-WAY GROUND** model. Assume **d** is the distance between receiver and receiver. When the transmitter is close to the receiver (e.g. within the Freznel zone [3]), receiving signal power is inverse proportional to $\mathbf{d^2}$. When their distance is larger (e.g. outside of Freznel zone), the receiving signal power is then inverse proportional to $\mathbf{d^4}$ [3].

According to [3], the receiving power of a signal at the receiver can be modeled as equation (1) (equation 3.52 of [3]).

$$P_r = P_t G_t G_r \frac{h_t^2 h_r^2}{d^4} \quad (1)$$

Here, P_t is the transmission power. G_t and G_r are antenna gains of transmitter and receiver respectively. h_t and h_r are the height of both antennas. d is the distance between the transmitter and the receiver. We assume that the ad hoc network is homogeneous, that is all the radio parameters are same at each node. A signal arriving at the receiver is assumed to be valid if the **Signal to Noise Ratio (SNR)** is above a certain threshold (SNR_THRESHOLD). Now, we assume a transmission is going from a transmitter to a receiver 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 $SNR=P_r/P_i$. Here, we ignore the thermal noise since it is ignorable comparing to interference signal. Under the assumption of homogeneous radios, we get equation (2).

$$SNR = P_r / P_i = (\frac{r}{d})^4 \geq SNR\_THRESHOLD$$

$$r \geq \sqrt[4]{SNR\_THRESHOLD} * d \quad (2)$$

This implies that to successfully receive a signal, the interfering nodes must be $\sqrt[4]{SNR\_THRESHOLD} * d$ 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. In practice, SNR_THRESHOLD is usually set to 10. Thus, we get R_i as

$$R_i = \sqrt[4]{10} * d = 1.78 * d \quad (3)$$

From equation (3) we can see that when the transmitter-receiver distance d is larger than $R_{tx}/1.78=0.56*R_{tx}$ (R_{tx} is the transmission range), interference range then exceeds the transmission range. This is easy to understand that power level needed for interrupting a transmission is much smaller than that of successfully delivering a packet. The interference area around a receiver is defined as $A_i = \pi R_i^2$. All nodes located in the interference area are called hidden nodes of the receiver.

B. *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 ($E_{RTS/CTS}$) as below:

A_i = Total interference area.
$A_{iRTS/CTS}$ = Part of the interference area where nodes can receive RTS or CTS successfully.
$E_{RTS/CTS} = A_{iRTS/CTS} / A_i$. (4)

According to equation (4), when $d <= 0.56*R_{tx}$, apparently $A_{iRTS/CTS}$ is equal to A_i since transmission range is larger than the interference range. Thus, $E_{RTS/CTS}$ is equal to 1. When d increases beyond $0.56*R_{tx}$, $A_{iRTS/CTS}$ becomes smaller than A, resulting the $E_{RTS/CTS}$ smaller than 1. $E_{RTS/CTS}$ 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 $0.56*R_{tx}$ and smaller than R_{tx} is illustrated in **Fig. 1**

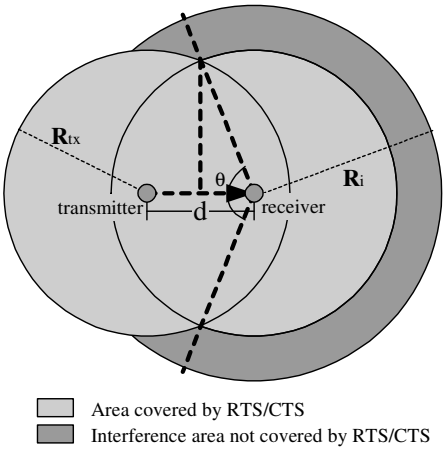

Fig. 1. Effectiveness of RTS/CTS handshake when d is larger than $0.56*R_{tx}$ and smaller than R_{tx}.

From **Fig. 1**, we can approximately calculate the $E_{RTS/CTS}$ when d is within $[0.56*R_{tx}, R_{tx}]$. The dark shaded area in **Fig. 1** represents part of the interference area which is not covered by RTS/CTS handshake (e.g. $A_i - A_{iRTS/CTS}$). To calculate this area, we should first calculate the angle θ as shown in **Fig. 1**.

$$\cos(\theta/2) = \frac{d/2}{R_{tx}} \Rightarrow \theta = 2\cos^{-1}(\frac{d/2}{R_{tx}})$$

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

$$A_{iRTS/CTS} = \pi R_i^2 - \frac{2\pi-\theta}{2\pi}(\pi R_i^2 - \pi R_{tx}^2)$$

The total interference area is given as

$$A_i = \pi R_i^2 = \pi(1.78*d)^2 = 3.1684*\pi*d^2$$

Thus, we get

$$E_{RTS/CTS} = \begin{cases} 1, & 0 \le d \le 0.56*R_{tx} \\ 1-(\pi-\cos^{-1}(\frac{d}{2R_{tx}}))\frac{3.1684d^2-R_{tx}^2}{3.1684\pi d^2}, & 0.56*R_{tx} \le d \le R_{tx} \end{cases} \quad (5)$$

To see the effectiveness of RTS/CTS handshake clearly, we plot equation (5) in **Fig. 2**. The X axis of **Fig. 2** is the transmitter-receiver distance d. Y axis is the effectiveness of RTS/CTS handshake. Clearly when d exceeds $0.56*R_{tx}$, 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.

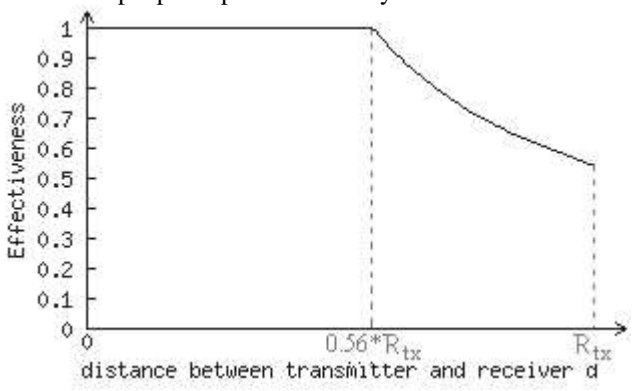

Fig. 2. Effectiveness of RTS/CTS handshake

C. *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**.

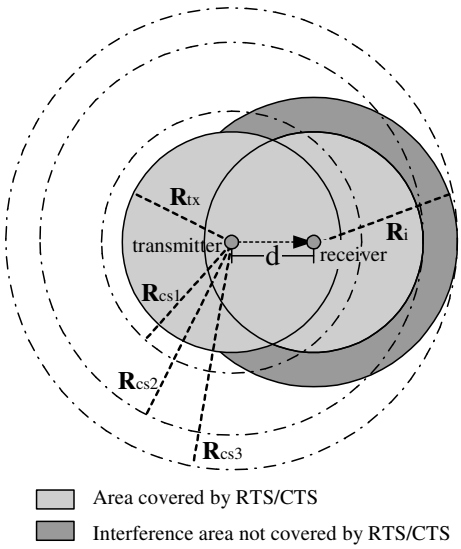

Fig. 3. Illustration of how physical carrier sensing help reducing interference

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 $d + R_i$) as shown in **Fig. 3**, we can now totally cover the interference area. Interestingly, when the carrier sensing range exceeds R_{cs2} (equal to $d + R_{tx}$), 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 $(d+R_{tx})$, RTS/CTS is no longer 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 would be complex. Thus, the maximum values of R_{cs2} and R_{cs3} should be taken, which are $2*R_{tx}$ and $R_{tx}+ 1.78*R_{tx} = 2.78*R_{tx}$ respectively. **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 won't 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 $0.56*R_{tx}$.
- 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 2Mbps [2].

Table 1. Hardware Characteristics of the Lucent ORiNOCO Wireless Card

Transmission Rate	2Mbps
Transmission Power (P_t)	15dBm
Transmission Range (R_{tx})	400m
Receiver Sensitivity	-91dBm
Carrier Sensing Range (R_{cs})*	670m

III. 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 [4], where NS2 simulator is used and the transmission range and interference range are set to 250m and 550m respectively. The topology of a single chain is illustrated as in **Fig. 4** and the distance between neighbor nodes is 200m. Clearly, if not considering the large interference range, the capacity of this single chain is 1/3 of the channel bandwidth, which is 2Mbps (Considering the overhead of RTS, CTS, etc, the authors of [4] give the achievable channel bandwidth as 1.7Mbps). The reason is the spatial reuse constrain. When node 1 is transmitting to node 2, node 2 and node 3 can not 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 550m is used in [4]). This is certainly a significant reduction to the network capacity.

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

Several things need to be noticed with above discussion. **First**, in [4] a fixed interference range as large as 550m is used, which is more than twice of the transmission range (e.g. 250m). 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. Thus, for the topology in **Fig. 4**, the interference range is around 356m. 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 150m, 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 [7] (More detailed description of QualNet is provided at section IV.). 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 300m. Transmission range of the wireless radio is 367m with channel bandwidth as 2Mbps following the standard. We vary the vertical distance between node 2 and node 3 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.

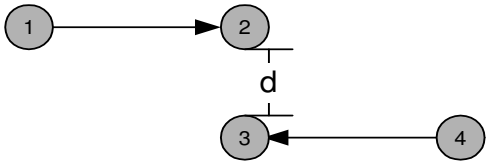

Fig. 5. Scenario for simulation investigation of collisions caused by large interference range

Metrics we selected for our investigation are the aggregated throughput of the two flows and the data packet corruption ratio. Data packet corruption ratio is defined as the portion of data packets transmitted at the MAC layer which 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

* Not directly from Lucent. We calculated it according to other parameters.

experiments, we only count those data packet drops corrupted by interference at the receiver. Experiment results are reported from **Fig. 6** to **Fig. 9**.

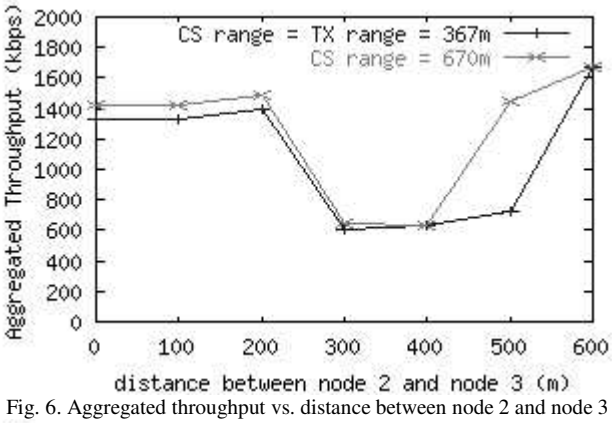

Fig. 6. Aggregated throughput vs. distance between node 2 and node 3

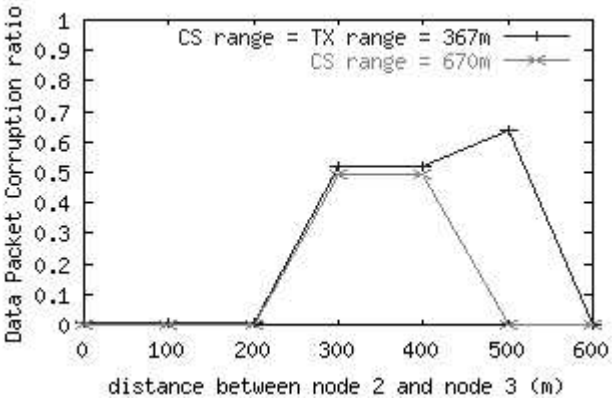

Fig. 7. Data packet corruption ratio vs. distance between node 2 and node 3

In **Fig. 6** and **Fig. 7**, the packet rates of two CBR flows are set to 800Kbps with packet size 1024 bytes (thus 100 packets per second). The packet rate of CBR is selected as to utilize the full bandwidth when the two flows share the channel (e.g. the available channel bandwidth to each flow is 1.7Mbps/2=850Kbps). It is interesting to notice that when the distance between node 2 and node 3 is 300m, 400m and 500m, the aggregated throughput in **Fig. 6** is dramatically decreased. This is controversial to our common impression. When node 2 and node 3 is 400m 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 larger 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 500m), the two connections are fully separated from each other. The data packet corruption ratio shown in **Fig. 7** clearly confirms this. **Fig. 6** and **Fig. 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 500m 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 don't 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. 300m and 400m cases), carrier sensing range as large as 670m 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 a node sending out data packets and the 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 300m. Simulation results are given in **Fig. 8** and **Fig. 9**.

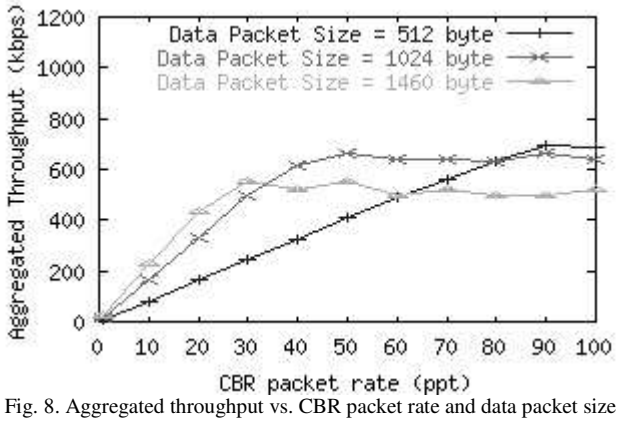

Fig. 8. Aggregated throughput vs. CBR packet rate and data packet size

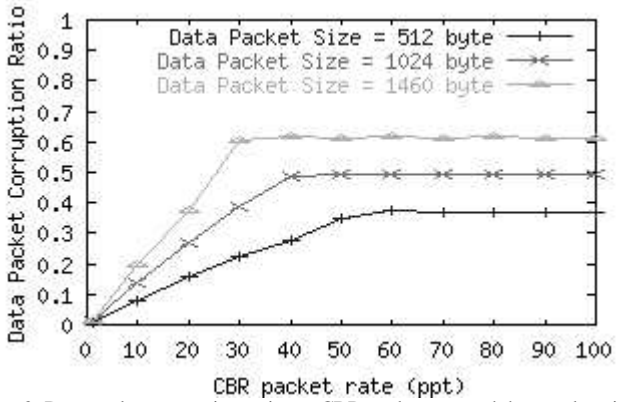

Fig. 9. Data packet corruption ratio vs. CBR packet rate and data packet size

From **Fig. 8** and **Fig. 9** we can see that when the packet rate of CBR sessions is smaller than 10pps (packet per second), 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 bytes 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 [6], the authors also mentioned that large interference range is one of the major factors which cause poor performance and significant capture/unfairness problem of TCP flows. 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.

IV. PROPOSED SCHEME AND SIMULATION EVALUATION

A. Proposed Scheme

As shown in section III, the ineffectiveness of RTS/CTS handshake on resolving large interference range will cause significant data packet corruptions at the MAC layer. Thus, waste channel bandwidth. In this section, we propose a MAC layer scheme called **Conservative CTS Reply (CCR)** to help IEEE 802.11 MAC solving this problem. The main idea is that a node only replies a CTS packet for a RTS quest when the receiving power of that RTS packet is larger than a certain threshold (CTS-REPLY-THRESHOLD), 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. In detail, our scheme actually reduces the effective transmission range to resolve the interference. Clearly this is a tradeoff. In practical, the CTS-REPLY-THRESHOLD can be adjusted to achieve an optimal network throughput.

Our modifications as conservative CTS reply for IEEE 802.11 result an inconsistency between broadcasting and unicasting since in IEEE 802.11, broadcast packets are not protected by RTS/CTS. 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 our proposed scheme is a reduced effective transmission range, thus a 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.

B. Simulation Platform

All simulations in this paper use QualNet™ [7] simulator, a packet level simulator developed by Scalable Network Technologies Inc. It is the successor of GloMoSim (Global Mobile Information Systems Simulator) [8]. According to [9], QualNet incorporates a detailed and accurate model of the physical channel and of the IEEE 802.11 MAC layer. The Two-way ground path loss model used for our derivation is also implemented in QualNet. Most of the physical and MAC layer parameters of QualNet are following the IEEE 802.11 standard and Lucent WaveLAN wireless card. The transmission power is 15dBm, resulting a transmission range as 367m. The antenna sensitivity is -91dBm yielding a carrier sensing range as 670m. All these parameters match that of Lucent ORiNOCO wireless card listed at section III very well.

C. Simulation Evaluation

We did a simple experiment to verify that our proposed scheme is capable to eliminate collisions caused by large interference range. 100 nodes are randomly deployed in a 1500mX1500m terrain and randomly selected CBR/UDP sessions are used to generate traffic. The path loss model is set to Two-Ray Ground model. Channel bandwidth is 2Mbps. We vary the number of CBR pairs to check how effective our scheme can avoid interference. The CBR data packet size is 1024 byte and packet rate is 10pps. DSDV [13] routing is used here. The data packet corruption ratio defined in section III is again used here as the major metric. We only count the corruption ratio of unicast data packets, thus exclude routing packets which are broadcasting based. Experiment results are given in **Fig. 10**. Clearly, when we increase the number of CBR sessions, the data packet corruption ratio of the original

802.11 is increased greatly. By applying our proposed scheme, the data packet corruption ratio is always smaller than 3%. This verifies that our scheme can effectively avoid the collisions due to large interference range.

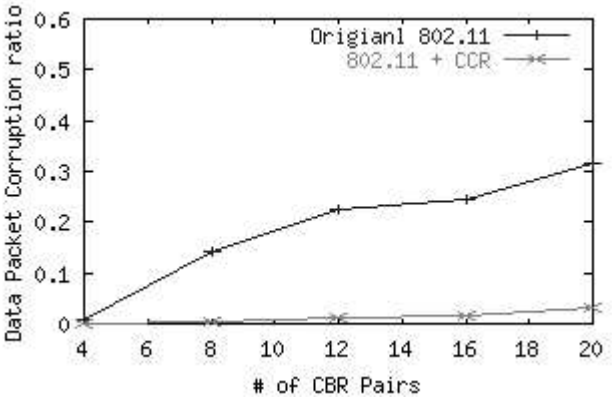

Fig. 10. Data packet corruption ratio vs. # of CBR pairs

V. RELATED WORK

Large interference range has been realized by more and more researchers in recent years [4][6]. In [4], the influence of large interference range to the ad hoc network capacity is studied. In [6], 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 [1]. 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* (PRN), a receiver-initiated busy-tone scheme was proposed to solve the hidden terminal problems [10][11]. 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 power control MAC schemes. By adjusting the transmission power, a node is able to reduce its interference to other transmissions [12]. 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 scheme to those power control schemes, we have different targets. Our scheme focuses on eliminating the collisions due to large interference range, not power consumption. Our scheme is simpler and has no additional requirement to the wireless devices.

VI. 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 in theory. We believe that such a quantified analysis would be helpful to research in ad hoc networks, especially those works targeting the ad hoc network capacity and TCP fairness problems [6]. **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**, a simple MAC layer scheme is proposed to combat the large interference range. The main advantage of our proposed scheme is that it is simple and only has a trivial modification to IEEE 802.11 standard. Thus, although more sophisticated schemes (e.g. adjusting the transmission power etc.) can be proposed, our scheme would be simpler and more practical. Moreover, simulation experiments show that our scheme can eliminate most packet collisions due to large interference range.

REFERENCE

[1] IEEE Std. 802.11, "Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications," 1999. Downloadable at http://standards.ieee.org/getieee802/.

[2] Hardware specifications of Lucent ORiNOCO wireless pc card. http://www.orinocowireless.com/

[3] T. Rappaport, "Wireless Communications: Principles and Practice," Prentice Hall, New Jersey, 1996.

[4] J. Li, C. Blake, D. Couto, H. Lee, and R. Morris, "Capacity of Ad Hoc Wireless Networks," In *Proceedings of ACM MobiCom 2001*, Rome, Italy, July 2001.

[5] J. Weinmiller, H. Woesner, J. Ebert, and A. Wolisz, "Analyzing the RTS/CTS Mechanism in the DFWMAC Media Access Protocol for Wireless LAN's," In *Proceedings of IFIP TC6 Workshop Personal Wireless Communications (Wireless Local Access)*, Prague, Czech Republic, April 1995.

[6] S. Xu, and T. Saadawi, "Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks*?" IEEE Communications Magazine*, Volume 39 Issue 6, Jun. 2001 pp. 130-13.

[7] QualNet simulator. http://www.qualnet.com

[8] M. Takai, L. Bajaj, R. Ahuja, R. Bagrodia, and M. Gerla, "GloMoSim: A Scalable Network Simulation Environment," *Technical report 990027*, UCLA, Computer Science Department, 1999.

[9] M. Takai, J. Martin, and R. Bagrodia, "Effects of Wireless Physical Layer Modeling in Mobile Ad Hoc Networks," *In Proceedings of MobiHooc 2001*, Long Beach, CA, Oct. 2001.

[10] F. A. Tobagi, and L. Kleinrock, "Packet Switching in Radio Channels: Part II - The Hidden Terminal Problem in Carrier Sensing Multiple Access and Busy Tone Solution," *IEEE Trans. on Commun*., Vol. COM-23, No. 12, pp. 1417-1433, 1975.

[11] C. Wu, and V. O.K. Li, "Receiver-Initiated Busy-Tone Multiple Access in Packet Radio Networks," *ACM SIGCOMM'87 Workshop: Frontiers* in *Computer Communications Technology*, Stowe, VT, Aug. 1987.

[12] J. P. Monks, J. P. Ebert, A. Wolisz, and W W. Hwu, "A Study of the Energy Saving and Capacity Improvement Potential of Power Control in Multi-hop Wireless Networks," In *Proc. of Workshop on Wireless Local Networks*, Tampa, Florida, Nov. 2001.

[13] C. Perkins, and P. Bhagwat. "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In *Proceeding of the ACM SIGCOMM*, October 1994.