Energy efficient MAC protocol with spatial reusability for wireless ad hoc networks

Hrishikesh Gossain

Mesh Networks Product Group,
Motorola, Inc., FL 32751, Maitland, USA
E-mail: Hrishikesh.Gossain@motorola.com

Carlos de M. Cordeiro

Philips Research,
Wireless Communication and Networking Department,
Briarcliff Manor, NY 10510, USA
E-mail: carlos.cordeiro@philips.com

Dharma P. Agrawal*

Department of Electrical and Computer Engineering and Computer Science,
University of Cincinnati, 816 Engineering Research Centre Building,
OH 45221-0030, Cincinnati, USA
E-mail: dpa@ececs.uc.edu
*Corresponding author

Abstract: In this paper we propose a Spatial Reuse MAC (SRM) protocol based on the IEEE 802.11 which employs a combination of power control and a fully distributed scheme of transmission sneaking to achieve energy efficiency and spatial re-use in wireless ad hoc networks without using a separate control channel. Through extensive performance evaluation, we show that SRM considerably improves the total amount of bytes delivered per unit of energy as compared to existing solutions.

Keywords: 802.11; dominating transmission; energy saving; MAC; power control; sneaking transmission; spatial reuse; wireless ad hoc networks.

Reference to this paper should be made as follows: Gossain, H., Cordeiro, C. de M. and Agrawal, D.P. (2005) 'Energy efficient MAC protocol with spatial reusability for wireless ad hoc networks', *Int. J. Ad Hoc and Ubiquitous Computing*, Vol. 1, Nos. 1/2, pp.13–26.

Biographical notes: Hrishikesh Gossain is a Senior Systems Engineer in Mesh Networks Product Group in Motorola Inc. He received his MS and PhD from the Department of ECECS, University of Cincinnati and BE in Electronics Engineering from Motilal Nehru Regional Engineering College, India, where he was Undergraduate Gold-Medalist of the College. He has several approved and pending patents in the areas of wireless and mobile computing, access network design, QoS and e-media. He has previous work experience in Nortel Networks in Richardson, Texas and Center for Development of Telematics (C-DoT), India.

Carlos de M. Cordeiro is a Senior Member Research Staff of Philips Research USA, Briarcliff Manor, NY. In his current capacity at Philips Research, Dr. Cordeiro is involved with research of PHY and MAC aspects in the area of cognitive radios. He participates in the IEEE 802.22 standardisation effort, and amongst other responsibilities serves as the Chair of the MAC subcommittee in IEEE 802.22. Dr. Cordeiro received his PhD in computer science and engineering in 2003 from the University of Cincinnati, OH, USA, where he won the honorable *Outstanding Doctoral Dissertation Award* and the prestigious *2003/2004 The National Dean's List Award*. He is also listed in the 2005 Edition of *Marquis Who's Who in America*.

Dharma P. Agrawal the Ohio Board of Regents Distinguished Professor of Computer Science and Computer Engineering and the founding director for the OBR Research Center for Distributed and Mobile Computing in the Department of Electrical & Computer Engineering and Computer Science, University of Cincinnati, OH. His current research interests include wireless and mobile networks, distributed processing, and scheduling techniques. Dr. Agrawal is an Editor for the *Journal of Parallel and Distributed Systems and the International Journal of High Speed Computing*. He has served as an Editor of the *IEEE Computer magazine, and the IEEE*

Transactions on Computers. He has been the Program Chair and General Chair for numerous international conferences and meetings. He was selected for the Third Millennium Medal by the IEEE for his outstanding contributions. Four of his patents in wireless networking area have also been approved recently. Dr. Agrawal is a Fellow of the IEEE, ACM, AAAS and WIF.

1 Introduction

Power control is a determinant technique for energy conservation and thus, is of fundamental importance to wireless ad-hoc stations which primarily rely on limited battery power. Besides energy saving, power control can also increase the capacity of the network by enhancing spatial re-use of the wireless channel. Various strategies for achieving power control can be classified based upon the presence of symmetric or asymmetric links between nodes. In the context of IEEE 802.11 (IEEE Std 802-11, 1997) networks, link symmetry is assumed in its design while communication in asymmetric networks has been shown to be a relatively hard task (Prakash, 1999; Narayanaswamy et al., 2002).

Several protocols for power control over IEEE 802.11 have been suggested which are based on the RTS-CTS exchange (Agarwal et al., 2001; Gomez et al., 2001; Karn, 1990; Pursley et al., 2000). To alleviate the problem of link asymmetry, RTS and CTS are transmitted at the highest power level whereas DATA and ACK use the minimum power level needed for communication between the nodes and are referred to as the BASIC scheme (Jung and Vaidya, 2002). It has been shown that the BASIC scheme has many underlying deficiencies, and an improved protocol called Power Control MAC (PCM) has been introduced (Jung and Vaidya, 2002). PCM periodically increases the transmit power during DATA transmission so as to overcome major limitations such as increased number of collisions and retransmissions, higher energy consumption, and throughput degradation. However, these schemes fail to explore spatial-channel-re-use to its maximum possible potential, as either the entire radio range as in PCM is blocked, or stations access medium without any coordination, thus increasing the number of collisions and energy consumption (Jung and Vaidya, 2002).

In this paper we introduce a novel Spatial Reuse MAC (SRM) based on IEEE 802.11 which explores spatial reuse by employing a combination of power control and a distributed transmission sneaking mechanism. SRM follows the approach of the BASIC scheme for RTS-CTS and DATA-ACK exchanges while suitably managing the IEEE 802.11 network allocation vector (NAV), so as to overcome deficiencies in the BASIC protocol. In order to accomplish wireless-channel-spatial-re-use, we introduce a technique of transmission sneaking whereby a pair of nodes in the neighbourhood of an on-going transmission can communicate if they have the knowledge that their transmission is not going to collide with any of the on-going transmissions. SRM is observed to considerably improve the energy consumed per unit of successfully transmitted byte as compared to PCM and IEEE 802.11.

The rest of the paper is organised as follows. The basics of the IEEE standard 802.11 and some fundamental concepts are provided in Section 2. Next, Section 3 presents our proposed SRM protocol in detail, while Section 4 describes the simulation environment and the results. Section 5 gives an overview of the related work, and Section 6 provides a discussion on some implementation issues of SRM. Finally, the paper is concluded in Section 7.

2 Overview of the IEEE 802.11 MAC protocol

In this work, we consider the IEEE 802.11 DCF access method. We define the terms transmission range, carrier-sensing range, interfering range, carrier-sensing zone (C-Zone) and sneaking zone (S-Zone) which are used extensively throughout this paper. In the following description we assume *A* as the source and *B* as the recipient of an on-going transmission.

2.1 Transmission range

This represents the range within which a packet can be successfully received, provided there is no interference from other nodes.

2.2 Carrier-sensing range

The range within which a transmission can be detected is termed as carrier-sensing range. This is always larger than the transmission range, and may be more than two times the size of the transmission range (Xu and Saadawi, 2001). In our simulations we set the transmission range and carrier sensing range as 250 m and 550 m, respectively, when utilising the highest power level. It is to be noted that different power levels result in different sizes for the transmission and carrier-sensing ranges. In addition, we define the *Carrier-sensing Zone (C-Zone)* (Jung and Vaidya, 2002) as the area where a signal can be detected, but cannot be decoded.

2.3 Interfering range

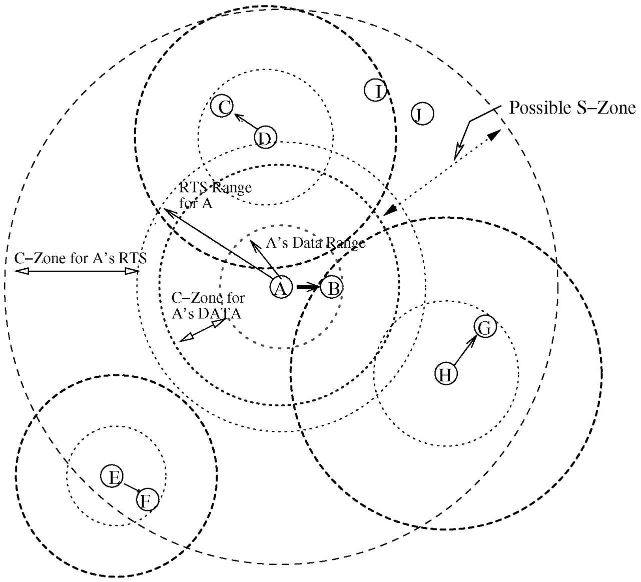
This represents the range within which a node in receiving mode can be interfered by another transmission. As outlined in Cesana et al. (2003) interfering range may vary depending upon the distance between *A* and *B*, the power at which the packet is transmitted, and the number of transmissions going on in the neighbourhood.

2.4 Sneaking zone (S-Zone)

Assuming that nodes A and B transmit RTS-CTS at full power ($p_{\max}$) and DATA-ACK at p_{desired} (p_{desired} is defined as the minimum power needed for a successful communication between two nodes), we define the S-Zone as the area within the carrier-sensing range of RTS-CTS, where a transmission (called sneaking transmissions or STs) is possible without interfering with A–B's transmission. It should be noted that this area is generally blocked in IEEE 802.11 because all the packets are transmitted at full power. In SRM, transmissions starting with RTS-CTS handshake (e.g., between A and B), are termed as dominating transmissions (DTs). The ST is done without RTS-CTS handshake. However in both the cases DATA and ACK are sent at p_{desired}. Nodes involved in DT and ST are termed as Dominating Nodes (DNs) and Sneaking Nodes (SNs) respectively.

Figure 1 illustrates the C-Zone and S-Zone for A's RTS and DATA transmissions. It should be noted that the size of S-zone may be larger than C-Zone as it may also include a part of RTS-CTS transmission range, which becomes free because of the low power DATA-ACK transmission (which reduces the size of carrier-sensing range).

Figure 1 Channel spatial re-usability in the SRM protocol



2.4.1 Impact of transmission power level on receiver interference range

It is necessary to understand the relationship between transmission power and corresponding interfering range at a receiver. For a given transmission power, ignoring the multi-path fading and shadowing (assuming they are minor factors in open space environment), the receiving power is mostly decided by the distance between the transmitter and receiver. There are different propagation model available to model this loss, which largely depends on the distance d between the transmitter and receiver. Let us assume a communication between two nodes A and B, where B is the receiving node at a distance d_{AB} of the transmitter node A and there is an interfering node C at a distance d_{CB} from B. Assuming that interference is contributed by C only, the signal to interference and noise ratio (SINR) equation at B can be simplified as (Rappaport, 1996):

$$\text{SINR}_B = \frac{P_{t-AB}}{P_{t-CB}}\left(\frac{d_{CB}^4}{d_{AB}^4}\right) \geq \text{SINR\_THRESHOLD} \qquad (1)$$

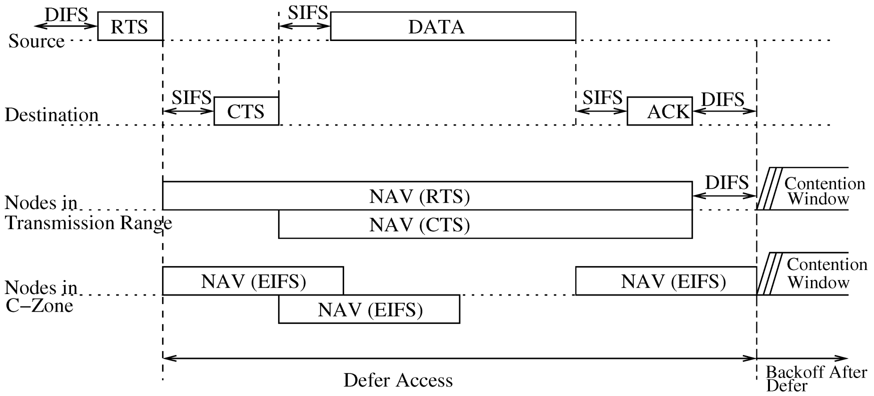
where P_{t-AB} and P_{t-CB} are the transmission power of node A and C respectively. Initially, let us fix the value of P_{t-CB} and analyse the effect of change of P_{t-AB} (the case when P_{t-AB} is same as P_{t-CB} has been studied in Xu et al. (2002). When node A starts its DATA transmission at $P_{t-AB} = p_{\text{desired}}$ to node B, node C, which is now out of C-Zone (Figure 1) of node A's DATA transmission, after waiting for EIFS (defined in next section) period, initiates a RTS transmission which, as we know, is transmitted at full power (i.e., $p_{\max}$). As a result, this RTS transmission from C will increase the overall interference level, decrease the SINR at B, and hence may compromise its packet reception. Thus, nodes in the neighbourhood of A–B should refrain from transmitting the RTS-CTS at full power (as done in the BASIC scheme). Rather, they should select P_{t-CB} so that its effect on the SINR at node B is minimal. Given all this, in SRM the sneaking transmission is not preceded by RTS/CTS.

2.4.2 Node behaviour in the IEEE 802.11 C-Zone

The DCF in IEEE 802.11 performs two forms of carrier-sensing: physical (by listening to the wireless shared medium) and virtual. Virtual carrier-sensing employs the duration field which is included in the MAC frames. Using the duration information, nodes update their Network Allocation Vector (NAV) whenever they receive a packet. The channel is considered to be busy if either physical or virtual carrier-sensing (by the NAV) so indicates.

Figure 2 gives an example on how nodes within the transmission range and C-Zone adjust their NAVs during RTS-CTS-DATA-ACK transmission. IEEE 802.11 defines four IFSs, namely, SIFS (short inter-frame space), PIFS (PCF inter-frame space), DIFS (DCF inter-frame space), and EIFS (extended inter-frame space). Basically, IFSs provide priority levels for channel access.

Figure 2 Node behaviour in the transmission range and carrier sensing range



In Figure 2, nodes in transmission range correctly set their NAVs when receiving RTS or CTS. However, since nodes in the C-Zone cannot decode the packet, they do not know the duration of the packet transmission. To prevent a collision with the ACK reception at the source node, nodes within the C-Zone set their NAVs for the EIFS duration. The main purpose of the EIFS is to provide enough time for a source node to receive the ACK frame, so the duration of EIFS is longer than that of an ACK transmission. As per IEEE 802.11, the EIFS is obtained using the SIFS, the DIFS, and the length of time to transmit an ACK frame at the physical layer's lowest mandatory rate, and is given by IEEE Std 802-11 (1997):

$$\text{EIFS} = \text{SIFS} + \text{DIFS} + [(8 \times \text{ACKsize}) + \text{PreambleLength} + \text{PLCPHeaderLength}]/\text{BitRate}$$

where ACK*size* is the length (in bytes) of an ACK frame, *BitRate* is the physical layer's lowest mandatory rate, *PreambleLength* is 144 bits, and PLCPHeaderLength is 48 bits (IEEE Std 802-11, 1997).

3 The spatial reuse MAC (SRM) protocol

Our proposed Spatial Reuse MAC (SRM) protocol is similar to the BASIC scheme in that it transmits RTS and CTS at $p_{\max}$, and DATA and ACK at p_{desired}. However, contrary to the BASIC scheme that does not have any mechanism to coordinate spatial re-use of the channel capacity during the low power DATA-ACK transmission, SRM implements a fully distributed *transmission sneaking technique* so as to enable channel spatial re-use, which is accomplished without the need for a separate channel. SRM appropriately adjusts the EIFS period of those stations within the C-Zone to overcome the drawbacks of the BASIC scheme, and at the same time prevent blocking of the entire C-Zone as in PCM.

To illustrate the overall idea of SRM, let us reconsider Figure 1 where node *A* transmits a RTS to node *B* which, in turn, sends CTS back to *A*. These transmissions are carried out at $p_{\max}$, while the DATA-ACK are transmitted at p_{desired}. Figure 1 depicts the various ranges and zones of the RTS-CTS and DATA-ACK transmission between nodes *A* and *B*. As mentioned in Section 2, we call these as a *Dominating Transmissions* (DT).

In SRM, we assume that every node maintains a *neighbor distance table* (NDT) to reach each of its neighbours (Agarwal et al., 2001). There are several ways in which this can be achieved. One possible solution is to exchange hello packets between neighbouring nodes, either at the MAC or at the network layer. Since protocol efficiency is of paramount importance in wireless networks, and given that many routing protocols for ad hoc networks already employ a form of hello packets to maintain network connectivity (Perkins et al., 2001), we follow a cross-layer design in SRM with the network layer assisting the MAC layer in the determination of the various distances amongst neighbour nodes. Network layer hello packets are always transmitted as MAC layer broadcast, therefore always sent at $p_{\max}$ SRM builds on the assumption that signal attenuation between neighbouring nodes is the same in both the directions and employs the Received Signal Strength Indicator (RSSI) model to estimate the distance between the transmitter node *A* and the receiver *B* based on the power transmitted (i.e., $p_{\max}$) and the power received (p_r) at *B* as:

$$\text{distance}(p_{\max}, p_r) = \begin{cases} \sqrt{\dfrac{p_{\max} \times G_t \times G_r \times \left(\dfrac{3\times10^8}{4\times\pi\times f}\right)^2}{L\times p_r}}, \\ \text{if} \left(\sqrt{\dfrac{p_{\max} \times G_t \times G_r \times \left(\dfrac{3\times10^8}{4\times\pi\times f}\right)^2}{L\times p_r}}\right) \\ \le \left(\dfrac{4\times\pi\times f\times H_t\times H_r}{3\times10^8}\right) \\ \sqrt[4]{\dfrac{P_{\max}\times G_t\times G_r\times H_r^2\times H_t^2}{L\times P_r}}, \quad \text{otherwise} \end{cases} \tag{2}$$

where G_t and G_r are the transmitter and receiver antenna gains, respectively, *f* is the operating frequency band, *L* is the system loss, and H_t and H_r are the transmitter and receiver antenna heights, respectively. This model can approximately determine the distance between two nodes. With equation (2), whenever a node receives either a broadcast or RTS-CTS, it can determine its distance from the transmitter in question.

We now discuss the steps taken for a DT in SRM. Before sending a RTS packet, a sender node A calculates the minimum power level, say $p_{\text{recv}-A}$, it needs to correctly receive a packet. This is done based on node *A*'s current interference profile (generally, this power level is higher than the power level needed when there is no surrounding interference). Next, node *A* includes both $p_{\text{recv}-A}$ and the SINR at *A* in its RTS packet before transmission. Essentially, the value of $p_{\text{recv}-A}$ is calculated as follows:

$$P_{\text{recv}-A} = SINR_A \times P_i^A \tag{3}$$

In equation (3), SINR$_A$ is the SINR at node *A* and P_i is the corresponding interference. Upon receiving the RTS packet coming from node *A*, with help of NDT, node *B* first calculates p_{desired} (the power level needed to send back the ACK packet to *A*). Next, node *B* calculates its own $p_{\text{recv}-B}$ (the minimum power needed at *B* to correctly receive a packet) and includes it together with the SINR at *B* in its CTS back to *A*. When node *A* receives the CTS back from node *B*, it is important to node that its original estimate of p_{desired} may now change, given the SINR at node *B*. Basically, node *A* may have to increase its power level so as to achieve the desired signal quality at node *B*. A similar mechanism has been employed in Xu et al. (2002) but it does not consider power control.

Once the DT is in place, we now turn our attention as to how the ST is performed in SRM. As outlined in Section 2, ST is performed by the nodes which are not able to capture the channel as a DT and are within the carrier-sensing range of the DT. In SRM, nodes can only sneak the on-going DT if they ensure that their ST will not collide at the DNs. For that, a potential sneaking node needs to determine the amplitude of its ST. In other words, nodes in the C-Zone need to estimate both the transmission range and carrier-sensing range of their potential SN and make sure that the DNs are outside of this range. Here, we assume that if a node *X* is outside the carrier-sensing range of a transmitter Y, it is not going to be affected by any packet transmission from Y. Mathematically node *D*, in Figure 1, can sneak a packet at p_{desired} to node *C* during the DT between nodes *A* and *B* if:

- distance(p_{desired}, CSThresh) < distance$_{D,A}$
- distance(p_{desired}, CSThresh) < distance$_{D,B}$

where distance$_{D,A}$, and distance$_{D,B}$ are the distances (in meters) between nodes *D* and *A*, *D* and *B*, respectively, and CSThresh is the minimum power level below which a signal cannot interfere with any potential on-going reception, and is defined in the IEEE 802.11 specifications (1997). In other words, CSThresh can be used to determine the boundary of the carrier-sensing range, the same way R × Thresh can be employed to determine the transmission range boundary. Therefore, if relations (i) and (ii) are satisfied, we can guarantee that a possible ST from D will not collide either with the receiver or with the transmitter of the DT. Node *C* also does a similar check before sending its ACK packet. Similarly from Figure 1, we can see that nodes *H* cannot communicate with *G* at a low power level as their transmission would collide at *B*.

Note that node *D* in Figure 1 is not a neighbour of either node *A* or node *B* given that it is located within the C-Zone with respect to these nodes. Therefore, an important issue is how a node (e.g., node *D* in Figure 1), in the C-Zone set their NAV so that they will not transmit RTS-CTS and collide with the on-going low power DT (as in the BASIC scheme). In the next subsection we elaborate on the node behaviour within the C-Zone for SRM.

3.1 Node behaviour within the C-Zone

Nodes located in the C-Zone of both nodes *A* and *B* will only be able to sense a transmission, but cannot decode it. The reason why it is crucial for SRM to determine whether a given transmission is due to an RTS or CTS is that this is the only way a node can infer when the actual DATA transmission of this ongoing DT will start. Therefore, packet type determination for nodes in the C-Zone is crucial, while the distance is not an issue and can still be obtained through equation (2). To overcome this, we implement a scheme in SRM in which a node can determine with high probability, the type of packet (if RTS, CTS, or neither) that is currently being transmitted over the wireless medium based on the on the duration of the transmission (similar to Li et al., 2004). In SRM, the size of the RTS packet is 22 bytes and of the CTS is 16 bytes (here, we use 1 byte to encode p_{desired} and 1 byte to encode the SINR level) as these packets include the p_{desired} and the SINR information. Hence it is possible to deduce with high probability whether the transmission was due to a RTS or CTS.[1]

In case node receives RTSs and CTSs from different transmitters consecutively, it always keeps track of the DT which is closest, in terms of distance as given by equation (2), to itself. In other words, nodes always consider the worst case scenario. Moreover, an important issue in SRM is how nodes in the C-Zone set their NAVs. In SRM we rename the EIFS as SRM_EIFS and redefine its duration for nodes in the C-Zone as:

$$\text{SRM\_EIFS} = \text{SIFS} + \text{DIFS} + [(8 \times \text{Average DATAsize})/\text{DataRate}] + [(8 \times \text{ACKsize}) + \text{Preamble Length} + \text{PLCPHeaderLength}]/\text{BitRate}, \tag{4}$$

where *Average*DATA*size* is the average size (in bytes) of a DATA transmission, *DataRate* is the rate at which DATA packets are sent (here, assumed to be the same at all stations). To estimate the value of *Average*DATA*size*, we have run several simulations (discussed next) by varying the AvereageDATAsize, each of which gives a different value for SRM_EIFS. We then evaluate the effect of this parameter on the total data delivered per Joule, and estimate the most suitable *Average*DATA*size* (we have simulations for different packet sizes too).

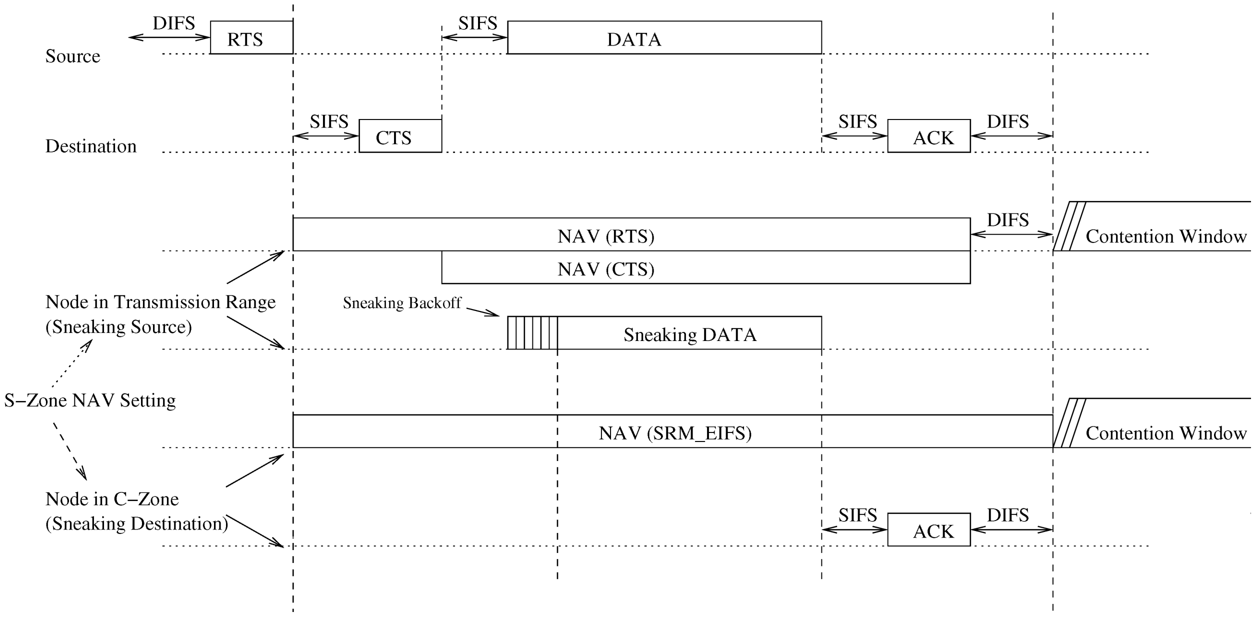
3.2 Sneaking procedure

We now describe a fully distributed sneaking procedure in SRM. Sneaking in SRM can be divided into two phases: sneaking in DT's C-Zone and sneaking at DT's transmission range.

3.2.1 Sneaking in DT's C-Zone

Let us first focus on the sneaking procedure in the C-Zone of the DT's RTS/CTS. In SRM, whenever a node has DATA to send and its NAV is set (meaning there is an ongoing DT), it may transmit the DATA directly if constraints (i) and (ii) defined earlier are satisfied. However, to guarantee that the sneaking DATA will not collide with the ongoing DT's RTS or CTS at $p_{\max}$, the sneaking node can only start its sneaking DATA transmission once the low power DT's DATA transmission has started (see Figure 3). Furthermore, as we can see from Figure 3, the length of the DATA packet that a sneaking source can transmit (i.e., the Sneaking DATA) has to be proportional to the sneaking source's NAV (which is, in turn, set for the duration of SRM_EIFS if the node is within the DT's C-Zone, or is set for the duration field contained in the RTS-CTS header if the node sits in the transmission range of the DT's source, destination, or both), since the NAV of a node indicates the remaining duration for which the medium will be busy. That is, the length of DATA part of a node's sneaking transmission is essentially decided, based on its current NAV length and the data transmission speed. Thus, a sneaking source can determine how big the DATA packet can be. In this calculation, the sneaking source also accounts for the time taken by the sneaking ACK to arrive back at the source. In our existing implementation of SRM, sneaking may result in fragmentation and reassembly of the packet at the MAC layer. However, since fragmentation has been extensively employed in the context of IEEE 802.11 with little overhead (Lettieri and Srivastava, 1998), we believe this is not a major roadblock. A more efficient solution could be to have a separate queue for small size packets (please see Section 6). This way, fragmentation and re-assembly would not be needed.

Figure 3 Channel spatial re-usability in the SRM protocol (nodes within C-zone use SRM_EIFS for their NAVs)



Finally, note in Figure 3 that at the sneaking source we employ a back-off mechanism called *sneaking backoff*. Before any sneaking node tries to sneak the medium, it has to back-off for a random duration between [20, $20 \times N$] μs, where N is an estimate of the average number of neighbours a node has, and is dynamically obtained through the routing protocol in our simulations (Li and Yu, 2002). The reason why the sneaking back-off is a multiple of 20 μ is because this is the time required for a node to sense medium activity (Jung and Vaidya, 2002). This is implemented in SRM to provide for the case where multiple nearby nodes try to sneak the medium simultaneously, hence causing collisions. This way, a node can interrupt its sneaking transmission if it detects that the medium has become busy during the sneaking back-off period. When sneaking is interrupted, the node returns to regular IEEE 802.11 algorithm (with RTS-CTS) as if transmission sneaking had never been attempted. Sneaking may be tried again in the next DT only.

3.2.2 Sneaking in DT's transmission range

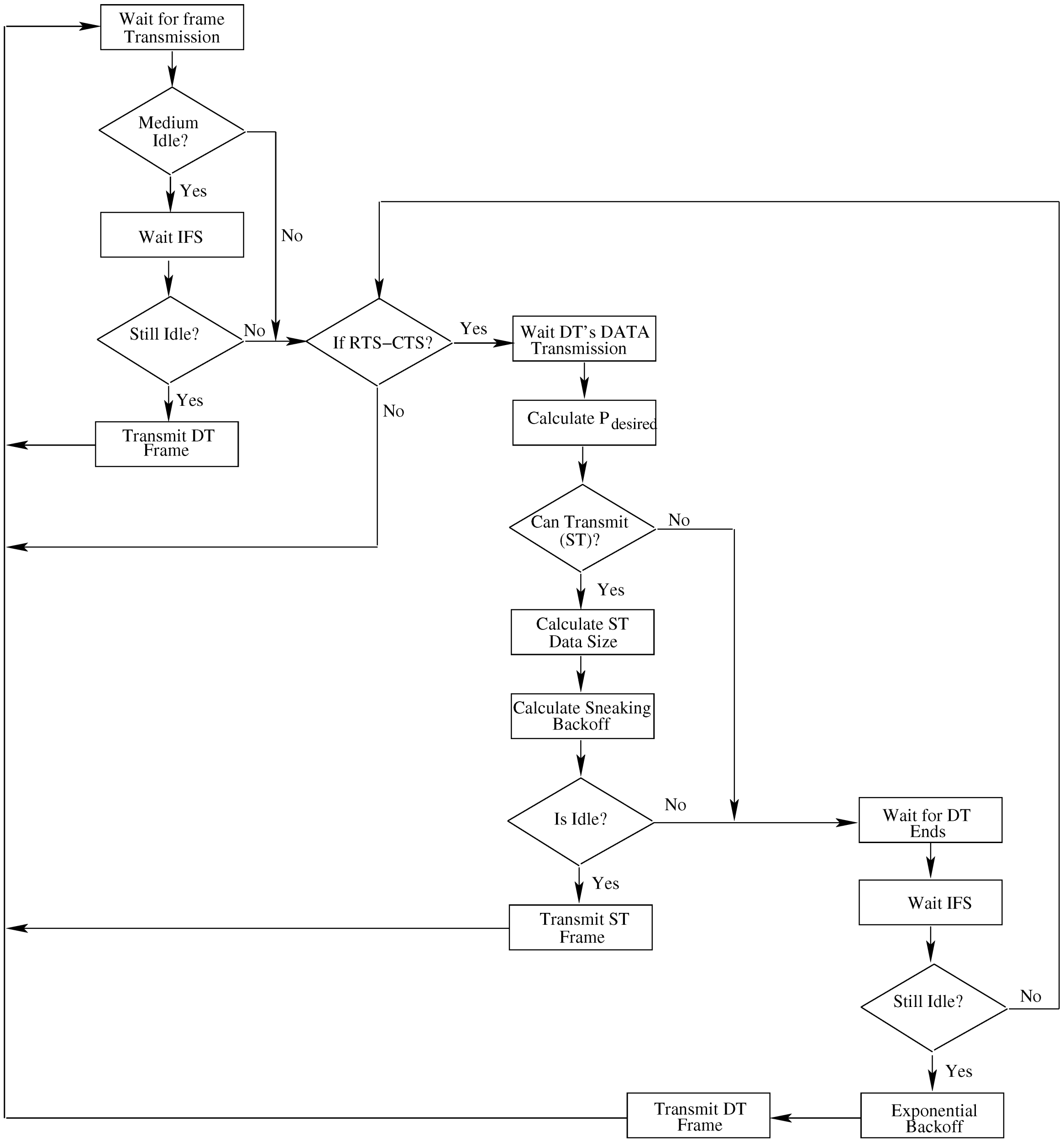
Let us now focus on the sneaking procedure for the nodes which have correctly received any of the DT's RTS-CTS. As explained before, if the p_{desired} used by DNs is below certain levels it is also possible to obtain a sneaking opportunity within the transmission range of the DT. First let us assume that a given node X has correctly received both RTS and CTS packets from the DNs. In this case, node X becomes aware of SINR at both S and R and also of the expected DATA-ACK receiving power (based on the exchanged $p_{\text{recv}-S}$ and $p_{\text{recv}-R}$). Thus, rather than estimating its carrier-sensing zone (as done in the previous subsection), node X can precisely determine if its transmission at p_{desired} is going to cause any collision at either S or R. Mathematically, node X can transmit its packet at p_{desired} iff:

- $\text{SINR}_s = \left(P_{\text{recv}-S}^{\text{ACK}} / P_{i-S} + P_{\text{recv}-X}^{\text{DATA}}\right) \geq \text{SINR\_THRESHOLD}$
- $\text{SINR}_R = \left(P_{\text{recv}-R}^{\text{DATA}} / P_{i-R} + P_{\text{recv}-X}^{\text{DATA}}\right) \geq \text{SINR\_THRESHOLD}$

where $P_{i-S} = P_{\text{recv}-S}^{\text{ACK}} / \text{SINR}_{\text{S}}^{'}$ and $P_{i-R} = P_{\text{recv}-R}^{\text{DATA}} / \text{SINR}_{\text{R}}^{'}$ represent the interfering powers at S and R respectively and is calculated based on received RTS and CTS packets.

However, if node X receives only one of RTS or CTS, it will not be able to determine the SINR profile at one of the DNs. In other words, node X is in the transmission range of only one of the DNs. Therefore, for the other DN (i.e., node S or R in our example) that node X is not able to decode the packet, it employs a similar scheme as described previously in subsection 3.2.1 (estimating the carrier-sensing range) before starting its sneaking transmission. A flow chart describing SRM sneaking procedure is shown in Figure 4.

Figure 4 Flow chart for SRM DT and ST packet transmission



4 Simulation environment and results

For our simulations, we use ns-2 (ns-2.26) (http://www.isi.edu/nsnam/ns/index.html) with the CMU wireless extension and compare IEEE 802.11, PCM, and SRM. Since the BASIC scheme has been studied and compared with PCM in Jung and Vaidya (2002) where PCM has been shown to be superior to BASIC in all scenarios, we do not consider the BASIC scheme in our study. We have used the following metrics to assess the performance of our considered MAC protocols:

- Aggregate throughput over all flows in the network.
- Total data delivered per unit of transmit energy consumption (or, Mbits delivered per Joule). This is calculated as the total data delivered by all the flows divided by the total amount of transmit energy consumption over all nodes (Mbits/Joule). The energy consumed in packet reception is not taken into consideration in this metric.

We use 1 Mbps for the channel bit rate. The application packet size is of 512 bytes unless otherwise specified, and each flow in the network transmits CBR traffic. We have also carried out simulations for different packet sizes and various network loads. We do not consider mobility in our simulations. For the radio propagation model, a two-ray path loss model is used. We do not consider fading in our simulations. As for the routing protocol, we have employed DSR (Dynamic Source Routing) and the various p_{desired} among the nodes are evaluated during route discovery phase, thus incurring no extra overhead to SRM.

We consider that carrier-sensing range is about two times larger than the transmission range as it is mostly the case in IEEE 802.11 stations (http://www.isi.edu/nsnam/ns/index.html). More specifically, in our simulation we consider the transmission range to be 250 m and the carrier-sensing range to be 550 m, at the highest transmit power level (p_{max}). All simulation results are the average of 30 runs, and each simulation runs for 70 seconds of simulation time.

4.1 Simulation topology

We use both a simple chain and random topologies. For the chain topology, we consider seven transmit power levels, 1.35 mW, 3.05 mW, 7.25 mW, 18 mW, 36.6 mW, 75.8 mW, and 281.8 mW, which roughly correspond to the transmission ranges of 50 m, 75 m, 100 m, 125 m, 150 m, 180 m, and 250 m, respectively. As for the random topology, we consider four power levels, namely, 1.35 mW, 7.25 mW, 36.6 mW, and 116 mW, which approximately correspond to the transmission ranges of 50 m, 100 m, 150 m, and 200 m. The transmission range at power level p_{max} is 250 m in our simulations for both topologies.

- *Chain topology*: Figure 5 shows our chain topology, which consists of 30 nodes with 15 single hop flows. Nodes are shown as a circle, and an arrow between two nodes indicates a traffic flow. The distance between adjacent node pairs in Figure 5 is uniform. In our simulations, we vary the distance from 50 m to 250 m.
- *Random topology*: For the random topology, we place 50 nodes randomly within a 1,500 × 1,500 m^2 flat area. One flow originates at 25 of these nodes with the nearest node as its destination. We simulated ten different random topologies (scenarios). Table 1 shows the number of flows using different distances for each of the scenarios. For example, scenario one indicates that there are 16 transmitters whose recipient is at distance 50 m, six transmitters whose recipient is at 100 m, and three transmitters have a recipient at 150 m. This particular scenario does not have any flow at 200 m.

Figure 5 Chain topology with a total of 30 nodes and 15 flows

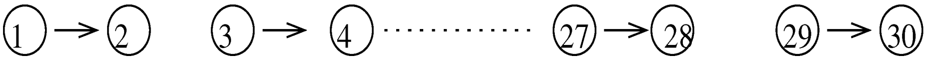


Table 1 Number of flows for various distances and scenarios

Scenario	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
50 m	16	15	15	9	9	8	15	10	13	9
100 m	6	5	5	9	10	11	4	9	5	9
150 m	3	4	3	6	4	3	3	3	5	6
200 m	0	1	2	1	2	3	3	3	2	1
Total	25	25	25	25	25	25	25	25	25	25

4.2 Simulation results

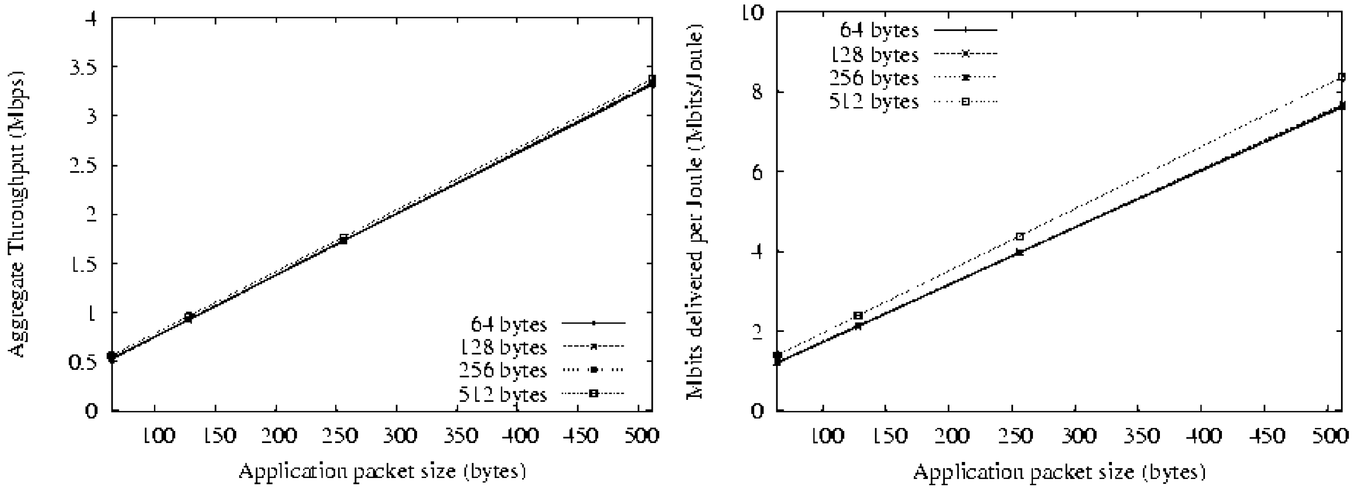
In this subsection, we discuss our simulation results. Results for the chain topology are presented first, followed by the results of the random topology.

4.2.1 Chain topology: varying combination of application packet size and SRM_EIFS average data size

Figure 6 shows the simulation results for 30 nodes with 15 flows in a chain topology. Each flow generates traffic at the rate of 200 Kbps. In this figure, the x-axis represents the packet size generated by the application (i.e., CBR) whereas each curve in the graph represents a different value for *Average*DATA*size* as given by equation (4). We have considered packets of size 64, 128, 256, and 512 bytes. This study is of paramount importance as the analysis allows the nodes within the C-zone to select different values of *Average*DATA*size* than the actual application data size employed by the ongoing DT.

As we can see from both Figures 6(a) and 6(b) that all curves for *Average*DATA*size* of 512 bytes is observed to give the best results. When *Average*DATA*size* is smaller than the application packet size, the net result is that SRM will sneak the DT for a reduced amount of time while its performance is still superior to the other protocols under study (see the next subsections). However, when *Average*DATA*size* is greater than the application packet size, there is a small chance (inferior to SRM_EIFS) that collisions with the ST may take place. In our simulations, we observed that during the period of time the DT is over and the ST is going on, nodes in the interfering range of the sneaking source and/or receiver (but who cannot detect the low power ST) are either backing off or waiting for DIFS so as to access the medium. Therefore, collisions may still occur occasionally. In spite of this fact, we observe (see next subsections) that the benefits resulted from sneaking in SRM surpass the drawbacks of the increased number of collisions. As a consequence of this analysis, otherwise noted the application packet size is considered to consist of 512 bytes. For this packet size, the value of SRM_EIFS is equal to 4450 µs.

Figure 6 Aggregate throughput and total data delivered per Joule for varying combination of packet sizes for chain topology (15 flows) (a) Aggregate throughput and (b) Total data delivered per Joule

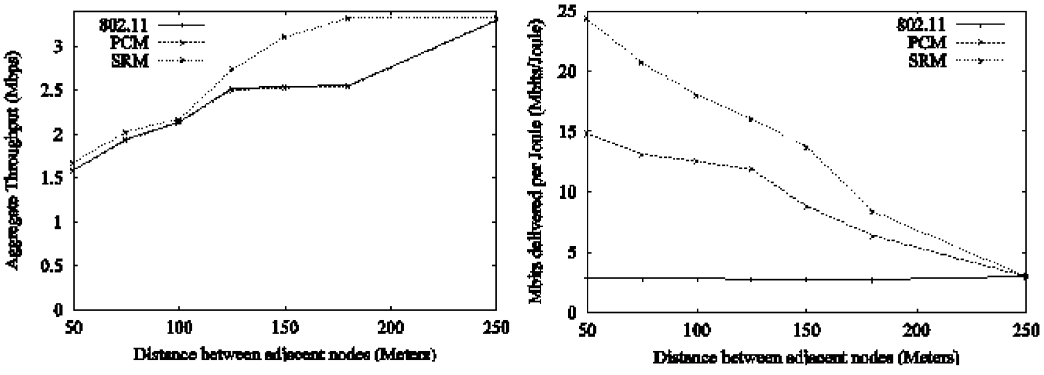


(a) **(b)**

4.2.2 Chain topology: varying node distance

Similar to the previous study, Figure 7 shows the simulation results for 30 nodes with 15 flows in a chain topology. Each flow generates a traffic at the rate of 200 Kbps. As the distance between two neighbours increases in Figure 7(a), the aggregate throughput increases in all schemes. This is because when nodes are far apart, a larger number of nodes can transmit simultaneously. As expected, PCM and IEEE 802.11 achieve comparable throughput (their curves overlap) given that PCM does not utilise spatial reuse. SRM, on the other hand, outperforms both PCM and IEEE 802.11 for all node distances because of its transmission sneaking, while improvement is noticeable starting from 125 m separation between nodes as a larger number of nodes can carry out sneaking.

Figure 7 Aggregate throughput and total data delivered per Joule for varying node distances for chain topology (15 flows) (a) Aggregate throughput and (b) Total data delivered per Joule



(a) (b)

The total data delivered per Joule in SRM has considerable improvement over the two other protocols. This is due to improved throughput possible by the SRM, coupled with its modified SRM_EIFS for nodes lying within the C-zone. PCM is observed to be more energy efficient than IEEE 802.11, but it is less efficient than SRM, given it requires periodic increments in power level. When the adjacent nodes are 250 m apart, PCM performs nearly the same as the IEEE 802.11 since it cannot reduce the transmit power level and has to use $p_{\max}$. A similar situation is also observed in SRM as it now has to transmit at p_{max}. With this separation, SRM improvement is negligible in terms of throughput and energy saving is negligible as there is hardly any opportunity for transmission sneaking.

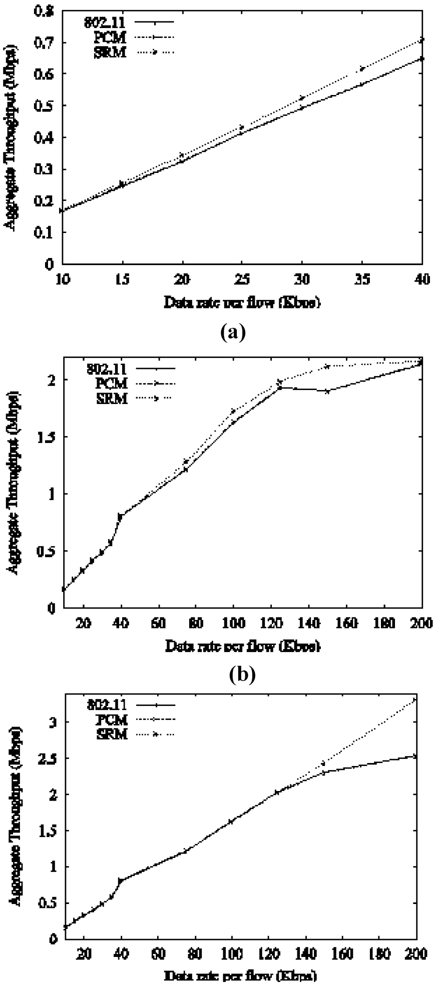
Finally, note that the absence of sneaking would make SRM throughput comparable to the IEEE 802.11 and the PCM, but its energy efficiency would still be superior to the PCM as the SRM does not employ any changes in periodic power level.

4.2.3 Chain topology: varying network load

Figures 8 and 9 show simulation results for three different node distances (50 m, 100 m, and 150 m) in the chain topology, with a varying data rate (load) per flow. In all the scenarios, when the network is lightly loaded, the aggregate throughput is almost identical for all three protocols (Figure 8). This is specially the case as nodes are farther apart (Figures 8(b) and (c)) as transmission sneaking in SRM becomes less effective. However, with increment in network load the SRM throughput shows considerable improvement, as the number of transmission sneaking opportunities is improved.

Figure 9 compares the data delivered per Joule in SRM, PCM, and IEEE 802.11 with increasing network load. It is important to note that the total data delivered per Joule in SRM is higher than PCM and IEEE 802.11 even when the aggregate throughput for all protocols are the same as shown in Figure 8. This is due to the fact that SRM does not change the power level periodically as done in PCM, and hence its energy saving is higher. Needless to mention that the IEEE 802.11 which always transmits at $p_{\max}$. Additionally we can also see that as the node distance increases, the total data delivered per Joule of SRM and PCM protocols decreases as p_{desired} starts approaching $p_{\max}$. Nevertheless, SRM is observed to deliver more data per Joule as compared to PCM and IEEE 802.11 in all scenarios.

Figure 8 Aggregate throughput for varying network load for chain topology (15 flows)

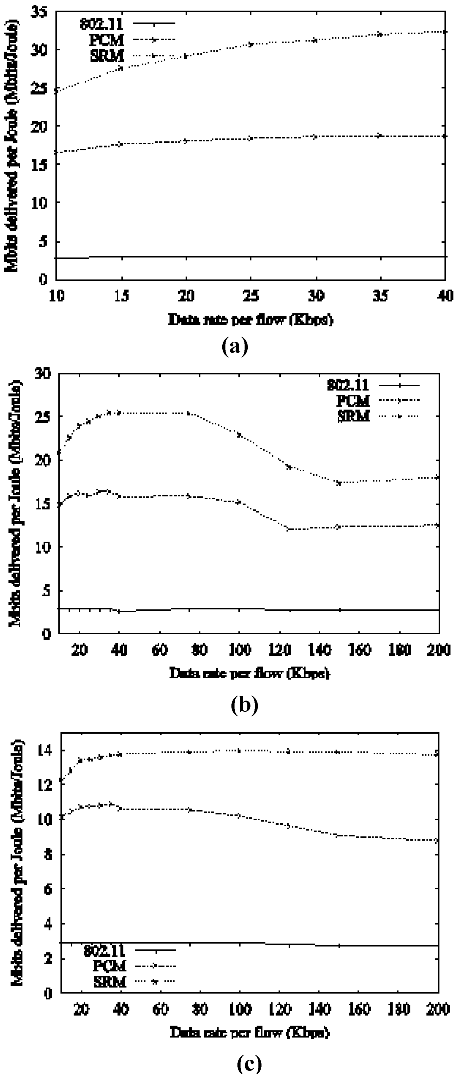


(a)

(b)

(c)

Figure 9 Total data delivered per Joule for varying network load for chain topology (15 flows) (a) 50 m, (b) 100 m and (c) 150 m



(a)

(b)

(c)

4.2.4 Random topology: varying network load

Figure 10(a) shows the simulation result for one particular scenario in the random topology for varying the data rate. In this case, simulation results are also similar to those for the case of chain topology. The aggregate throughput of SRM outperforms both IEEE 802.11 and PCM (IEEE 802.11 and PCM curves overlap).

Results for the data delivered per Joule are given in Figure 10(b). Both PCM and SRM show considerably improved performance over IEEE 802.11, with SRM providing the highest amount of data delivered per Joule.

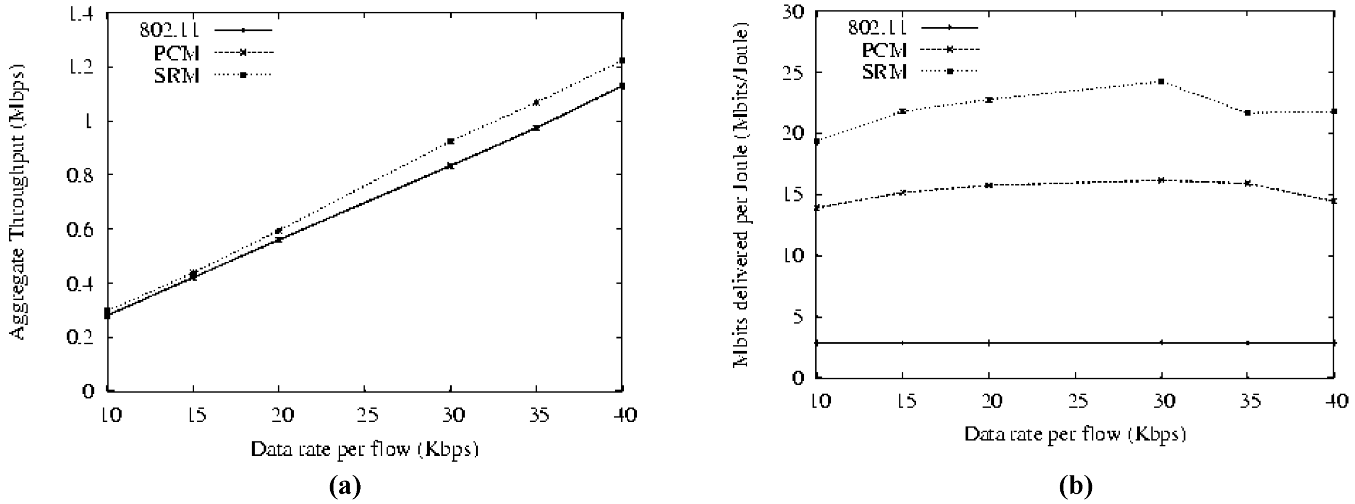
4.2.5 Random topology: ten different topologies

Figure 11(a) presents the simulation results for a random topology with 25 flows. Each flow generates data at the rate of 30 Kbps. The number in the horizontal axis indicates the ten different scenarios simulated (see Table 1). As shown in the Figure 11, the aggregate throughput of SRM surpasses that of PCM and IEEE 802.11.

4.2.6 Random topology: varying packet size

Results for varying packet size in a random topology are given in Figure 12. We have simulated packet sizes of 64, 128, 256, and 512, where SRM_EIFS is modified to reflect each packet size. Each flow generates traffic at the rate of 30 Kbps. Figure 12(a) indicates that the aggregate throughput of all the schemes increases with an increase in the packet size. However, the performance of SRM is constantly superior to the PCM and IEEE 802.11. As shown in Figure 12(b), the total data delivered per Joule for SRM surpasses PCM and IEEE 802.11. Larger packet size means that nodes can sneak more data. Therefore, the gap between SRM and both PCM and IEEE 802.11 widens with increasing packet size.

Figure 10 Aggregate throughput and total data delivered per Joule with increasing load (random topology) (a) Aggregate throughput and (b) Total data delivered per Joule



(a)

(b)

Figure 11 Aggregate throughput and total data delivered per Joule for different scenarios (random topology) (a) Aggregate throughput and (b) Total data delivered per Joule

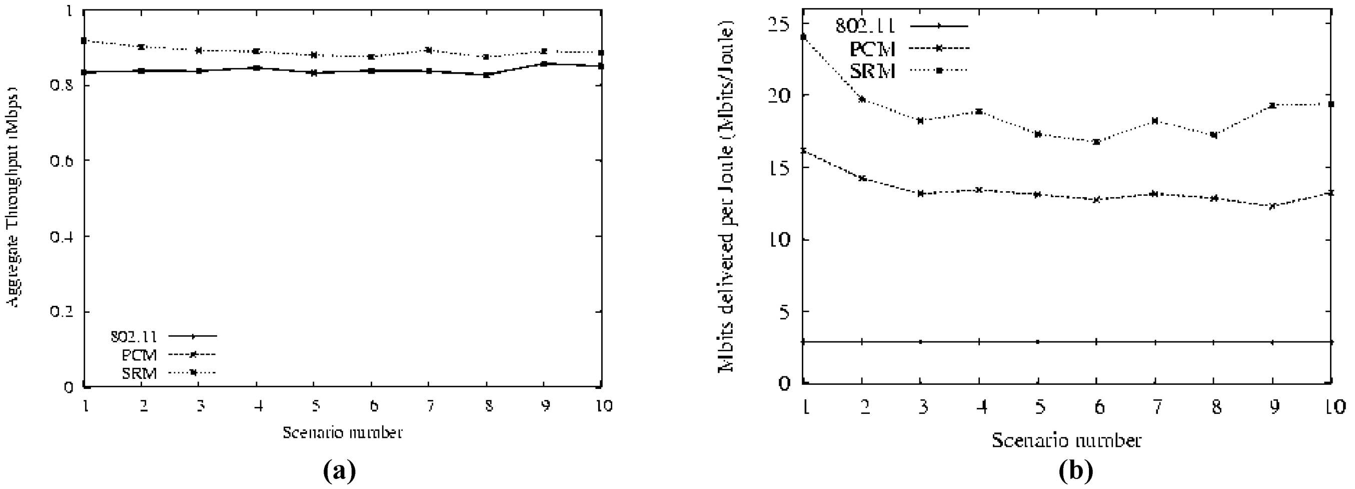
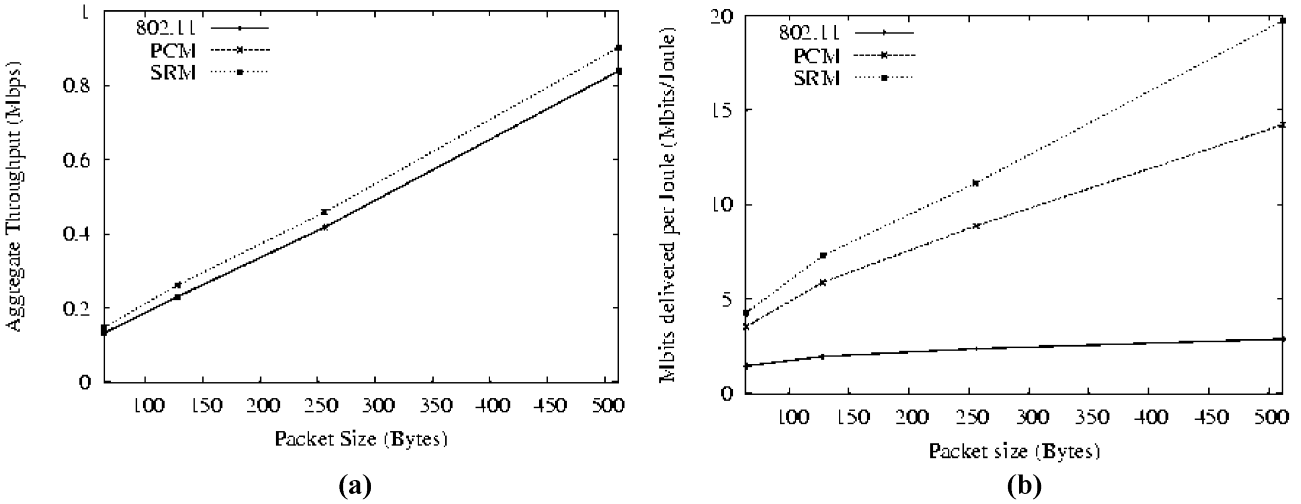


Figure 12 Aggregate throughput and total data delivered per Joule for different packet sizes (random topology) (a) Aggregate throughput and (b) Total data delivered per Joule



5 Related work

Current research on IEEE 802.11-based power control MAC protocols using omni-directional antennas concentrate their efforts in implementing efficient transmit power management schemes for the sake of energy efficiency. These schemes (Agarwal et al., 2001;Gomez et al., 2001; Karn, 1990; Pursley et al., 2000) focus mainly on suitably varying transmit power in order to reduce energy consumption.

The issue of spatial re-usability in IEEE 802.11 has been considered in Cesana et al. (2003) where a protocol named as Interference Aware MAC (IA-MAC) has been proposed. IA-MAC modifies the CTS packet header so as to include information on the SINR and on the power level at which a RTS is received, so that neighbouring nodes overhearing the RTS/CTS handshake can eventually attempt a concurrent transmission. However, it does not take power control into consideration, which limits the gains of the protocol and also does not improve on energy efficiency. IA-MAC only handles the case when nodes can successfully understand (i.e., decode) the RTS/CTS packets, while those nodes which can sense the packet but not decode it, have not been considered.

Finally, power control with the aim of accomplishing spatial reusability has been introduced in the context of the Power Controlled Dual Channel (PCDC) protocol (Muqattash and Krunz, 2003). PCDC suggests a cross-layer solution between the MAC and routing layers so as to allow multiple simultaneous transmissions in the neighbourhood of a node, which is done by appropriately estimating the power required for the transmission of data packets. However, PCDC is a multi-channel protocol with separate control and data channels. PCDC can only improve spatial re-use when neighbour nodes are able to successfully receive the RTS/CTS packet. In other words, nodes who do not understand these packets may not be capable to take advantage of this feature and can still cause interference with the ongoing transmission.

6 Discussions

The motivation behind introducing transmission sneaking steams from the fact that approximately one-third of packet transmissions in the internet today, are of size 48 bytes or less (http://www.nlanr.net/). Therefore, transmission sneaking has been specifically designed as an efficient mechanism for the transmission of small packets. This is especially advantageous in the case of wireless networks where a large overhead is put into transmitting control packet such as RTS and CTS.

There are some implementation issues related to SRM worth discussing here. In SRM, *Average*DATA*size* could always be set as being the maximum allowed MAC DATA size of 2346 octets (IEEE Std. 802-11, 1997). The side effect of this assumption is that if the DT's DATA size is larger than *Average*DATA*size*, SRM will not exploit (i.e., sneak) the DT in its entirety. However, if DT's DATA transmission is smaller than *Average*DATA*size*, there is a very small chance that collisions may take place which, in the worst case, could reduce the protocol efficiency to that of BASIC. The rationale behind including the average DATA size in the calculation of SRM_EIFS is to protect the DT from potential RTS-CTS transmissions from nodes sitting in the DT's C-Zone. By doing this, we can overcome the deficiency of the BASIC protocol without having to vary the transmit power level as in PCM, and thus enhance energy saving. In addition, a novel enhancement of SRM over existing power control protocols is that nodes in SRM can transmit (i.e., sneak) in the medium even if their NAVs are set (we elaborate on this issue in the next subsection).

In SRM, there may be situations where a node is simultaneously in the C-Zone of two different DTs. Clearly, this may result in overlapping of RTS and CTS packets received at this particular node, and hence it may not be able to detect the presence of any of them. In this case, SRM behaves similar to the BASIC scheme. That is, after the current transmissions (regardless of the frame type) are over, the node in the C-Zone will assume the medium to be idle and will try to send a RTS with full power, which may eventually cause collision. By simulation we have observed, however, that this situation is the exception and not the rule.

Another issue worth mentioning here is the behaviour of SRM in networks where nodes transmit at different data rates, given that the basic rate (i.e., the rate at which RTS/CTS/ACK packets are transmitted) is always the same as mandated by the IEEE 802.11 specifications (IEEE Std. 802-11, 1997). In this scenario, the calculated SRM_EIFS will either be larger (in case DT is transmitting at a higher rate) or be smaller (in case DT is transmitting at a lower rate) than what it should be. In the former case, the node has to wait for longer than it should (more opportunity for transmission sneaking), whereas in the latter case SRM behaves similar to the BASIC scheme.

Finally, in all the discussion above we have assumed that the wireless medium is shared by IEEE 802.11 compliant stations only. In other words, no external sources of interference have been considered. If external sources are present, sneaking may not always succeed and SRM performance may approach that of the IEEE 802.11.

7 Conclusions and future work

In this paper we propose a Spatial Re-use enabled Power Control MAC (SRM) protocol without the need for a separate control channel. Extensive simulations show that SRM provides higher throughput as compared to IEEE 802.11 and PCM, and enhances energy saving in all scenarios investigated. Overall, SRM throughput is at least as good as PCM and IEEE 802.11.

Concerns with SRM mainly concentrate on the determination of RTS-CTS transmissions for nodes within the interfering zone. Future research focuses on extending SRM for efficiently handling different data rates amongst stations, and on considering potential external sources of interference that could adversely affect the sneaking procedure.

Acknowledgement

This work has been supported by the Ohio Board of Regents Doctoral Enhancement Funds and the National Science Foundation under grant CCR-113361.

References

Agarwal, S., Krishnamurthy, S. Katz, R. and Dao, S. (2001) 'Distributed power control in Ad-hoc wireless networks', *IEEE PIMRC*, Vol. 2, pp.F-59–F-66.

Cesana, M., Maniezzo, D., Bergamo, P. and Gerla, M. (2003) 'Interference aware (IA) MAC: an enhancement to IEEE802.11b DCF', 58th *IEEE VTC,* Fall, Vol. 5, pp.2799–2803.

Gomez, J., Campbell, A., Naghshineh, M. and Bisdikian, C. (2001) 'Conserving transmission power in wireless ad hoc networks', *9th International Conference on Network Protocols, ICNP*, November, pp.24–34.

IEEE Std 802-11 (1997) *IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, June.

Jung, E.S. and Vaidya, N. (2002) 'A power control mac protocol for Ad Hoc networks', *Proc. of the ACM Mobicom*, pp.36–47.

Karn, P. (1990) 'MACA A new channel access method for packet radio', *in Proc.ARRL/CRRL Amateur Radio 9th Computer Networking*, 1990, pp. 134-140.

Lettieri, P. and Srivastava, M. (1998) 'Adaptive frame length control for improving wireless link throughput, range, and energy efficiency', *Proc. IEEE INFOCOM*, March, Vol. 2, pp.564–571.

Li, H. and Yu, D. (2002) 'A statistical study of neighbor node properties in ad hoc network', In *Int. Conf. on Parallel Processing Workshops*, August, pp.103–108.

Li, Z., Nandi, S. and Gupta, A. (2004) 'Improving MAC performance in wireless ad hoc networks using enhanced carrier sensing (ECS)', *IEE Proceedings – Communication*, October, Vol. 151, No. 5, pp.467–472.

Muqattash, A. and Krunz, M. (2003) 'Power controlled dual channel (PCDC) medium access protocol for wireless ad hoc networks', *Proc. of IEEE INFOCOM*, March, pp.470–480.

Narayanaswamy, S., Kawadia, V., Sreenivas, R. and Kumar, P. (2002) 'Power control in ad hoc networks: theory, Architecture, Algorithm and Implementation of the COMPOW protocol', *European Wireless Conference 2002*, February.

Perkins, C., Royer, E. and Das, S. (2001) 'Ad Hoc on demand distance vector routing (AODV)', *Internet Draft*, March (work in Progress).

Prakash, R. (1999) 'Unidirectional links prove costly in wireless Ad Hoc networks', *Proc. of the Third Int. Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications*, August, pp.15–22.

Pursley, M., Russell, H. and Wysocarski, J. (2000) 'Energy-efficient transmission and routing protocols for wireless multiple-hop networks and spread-spectrum radios', *Proc. of the EUROCOMM Conference*, pp.1–5.

Rappaport, T. (1996) *Wireless Communications: Principles and Practice*, Prentice Hall, New Jersey.

Xu, C.K., Gerla, M. and Bae, S. (2002) 'How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks?', *IEEE Global Telecommunications Conference*, Vol. 1, pp.72–76.

Xu, S. and Saadawi, T. (2001) 'Does IEEE 802.11 MAC protocol work well in multi-hop wireless networks?', *IEEE Communications Magazine*, June, Vol. 39, No. 6, pp.130–137.

Note

[1] The idea of detecting the type of a control packet based on the duration of the signal on the medium has also been suggested in Li et al. (2001) for the sole purpose of setting the NAV, while power control and spatial reusability have not been considered. Nevertheless, it is shown in Li et al. (2001) that a node in the C-Zone can determine, with high probability, the type of the transmitted packet based either on the physical layer header or the total time a signal is sensed in the wireless medium. This serves the further validate our claim.

Websites

National Laboratory for Applied Network Research, http://www.nlanr.net/.

NS-2 Network Simulator, http://www.isi.edu/nsnam/ns/index.html.