Winter 12-1-2004

SHUSH: A MAC Protocol for Transmit Power Controlled Wireless Networks ; CU-CS-986-04

Anmol Sheth
University of Colorado Boulder

Richard Han
University of Colorado Boulder

SHUSH: A MAC Protocol For Transmit Power Controlled Wireless Networks

Anmol Sheth, Richard Han
Department of Computer Science
University of Colorado, Boulder
Boulder, CO 80309
Email: anmol.sheth@colorado.edu rhan@cs.colorado.edu

Technical Report CU-CS-986-04
December 2004

SHUSH: A MAC Protocol For Transmit Power Controlled Wireless Networks

Anmol Sheth, Richard Han
Department of Computer Science
University of Colorado, Boulder
Boulder, C0 80309
Email: anmol.sheth@colordo.edu rhan@cs.colorado.edu

***Abstract*— A large number of MAC protocols have been proposed that allow transmit power control on a per packet basis to reduce power consumption of the nodes in a wireless ad-hoc network. Power control leads to the undesirable effect of increasing the number of hidden terminals in the network as well as increasing the unfairness in channel access. A common solution proposed by power controlled MAC protocols to date is to transmit the RTS/CTS frames at maximum transmit power. This approach partially solves the problem of reducing the number of hidden terminals, but sacrifices spatial reuse of the network and also reduces the aggregate throughput of the network. In this paper we present a new power controlled MAC protocol, SHUSH, which as the name suggests SHUSHes the interferer of an ongoing conversation. We evaluate the performance of SHUSH in comparison to four other transmit power controlled MAC protocols and demonstrate that SHUSH achieves superior aggregate goodput, spatial reuse, fairness, and minimal energy consumption while overcoming the general hidden terminal effect.**

***Index Terms*— System design, Simulations, Network measurements, Experimentation with real networks/Testbeds**

I. INTRODUCTION

Transmit power control is a highly effective technique for minimizing interference and energy consumption in wireless networks. If two communicating nodes can lower their transmission powers and corresponding transmission radii to the minimal values that maintain communication between the two nodes, then the conversation between the two nodes will minimize interference with other nodes' conversations, enabling higher aggregate throughput and greater spatial reuse than wireless networks that lack power control. Transmit power control has further value in terms of minimizing energy consumption due to transmission. Portable wireless access devices such as laptops, PDAs, and cell phones have extremely limited battery lifetimes. Energy constraints are also severe in wireless sensor networks. Transmit power control offers an effective technique for prolonging the lifetime of these wireless access devices by communicating at the minimum power that still maintains connectivity.

A key emerging trend is the integration of transmit power control into RF radios for cellular networks, wireless 802.11 LANs, and wireless sensor networks. The use of transmit power control can be traced back to digital cellular communication systems. In these systems, the main advantages of power control are to reduce co-channel interference and to overcome the drawbacks of the near-far effect [1]. For wireless ad-hoc networks, transmit power control reduces the power consumption of the mobile devices and also increases the capacity of the network [14]. Wireless 802.11 NICs are increasingly supporting transmit power control capabilities. For example, the Cisco Aironet 350 card supports 6 different levels ranging from 0 dBm to 20 dBm [4]. Wireless sensor networks are also integrating power control. MICA2 mote-based sensor networks support the Chipcon CC1000 radio, which allows fine-grained control of 256 different transmit power levels [5].

A critical issue that is encountered by MAC layer design given asymmetric transmit powers is the *general hidden terminal problem*, which can result in increased collisions and degraded throughput. We define the general hidden terminal problem as any situation in which an interferer is unable to hear a hidden ongoing conversation and then interrupts that hidden conversation. We assume that the interferer is equipped to hear all conversations, but may not hear some for any of a variety of reasons as explained below. The *specific hidden terminal problem* addressed by MACA is a subset of the general problem and assumes symmetric transmit powers, i.e. that all nodes have essentially the same coverage range. In a symmetric transmit power environment, the only way that an interferer is unable to hear an ongoing conversation and then interrupts that conversation is if the interferer cannot hear the sender and then interrupts the receiver by transmitting. In this case, the sender is hidden from the interferer, hence the classic hidden terminal terminology. The hidden terminal solution is the well-known RTS/CTS exchange in which a sender first transmits a Request-To-Send (RTS) and the receiver acknowledges with a Clear-To-Send (CTS) that informs other potential senders of the current sender, possibly hidden [3]. MACAW enhanced this solution with an ACK, to form an RTS-CTS-DATA-ACK exchange [6].

Asymmetric transmit powers introduce new and more general hidden terminals. For example, in Figure 1, nodes A and B are unable to hear the low power transmission of data from C to D. Nodes A and B have set their transmit powers to higher power in order to communicate. If node A transmits data to B, then the A-B conversation will unwittingly interfere with the C-D conversation. In this case, nodes C and D constitute *general hidden terminals* that have a hidden ongoing conversation that is interfered with by nodes A and B. Note that the interfering terminals are no longer confined to be within the carrier sense range of receiver D, as in the case of symmetric transmit powers. Instead, these new interfering terminals can be located anywhere outside of the union of C and D's carrier sense ranges (shown) yet within the union of carrier sense ranges formed at maximum transmit power from C and D (not shown), e.g. where A and B are located. Let us term this region the expanded interfering terminal zone. The interfering nodes collide with the hidden conversations, forcing retransmissions and degrading throughput. The increase in collisions caused by transmit power controlled hidden terminals was also observed in [13], [2].

SHUSH provides the first complete solution that is both fair and efficient to the problem of general hidden terminals introduced by asymmetric transmit powers in wireless 802.11 LANs. This general solution should preserve many of the original motivations for asymmetric transmit power, namely minimal energy consumption and minimal interference to enhance throughput and spatial reuse. The MACA/MACAW solution to the specific hidden terminal problem provides a starting point for developing a general solution. A key principle underlying MACA/MACAW's RTS/CTS exchange is the proactive informing of potential interferers of an impending DATA/ACK conversation. Potential interfering transmissions are thereby suppressed *a priori*. Following this principle, in order to ensure complete suppression of all potential interferers in advance given asymmetric transmit powers, the hidden terminals should exchange RTS/CTS at maximum power. For example, since nodes C and D do not know which nodes may interfere a priori, and since these interfering nodes may be located throughout the expanded interfering terminal zone, then the worst case must be addressed, namely that potential interfering nodes are the maximum distance away. Hence, RTS/CTS should be sent at maximum transmission power.

A solution predicated upon sending RTS/CTS at maximum power leads to poor spatial reuse and poor aggregate throughput and is at odds with our original motivations for transmit power control. Consider the BASIC protocol, which transmits the RTS/CTS at maximum power to address hidden terminals and transmits the DATA/ACK at optimum (minimal) power to conserve energy. This BASIC protocol was proposed as PARO in [10], and a similar protocol was proposed in [11]. PARO was subsequently renamed as BASIC [2]. The basic problem with BASIC is that the RTS/CTS reserves a large floor space for the subsequent DATA/ACK conversation that is carried on in a much smaller floor space. In BASIC's zeal to suppress potential interferers, RTS/CTS max also suppresses other concurrent conversations that would not interfere with the low power DATA/ACK conversation. These non-interfering concurrent conversations would enhance spatial reuse and throughput. For example, when node C sends its RTS at maximum power, it may suppress a very low power impending conversation between B and B' (not shown) that is nearly colocated with B. The B-B' conversation could have occurred concurrently with the C-D conversation. The problem with large floor space reservations is exacerbated in 802.11 by the fact that the RTS/CTS frames have extended range compared to data packets transmitted at the same power, because

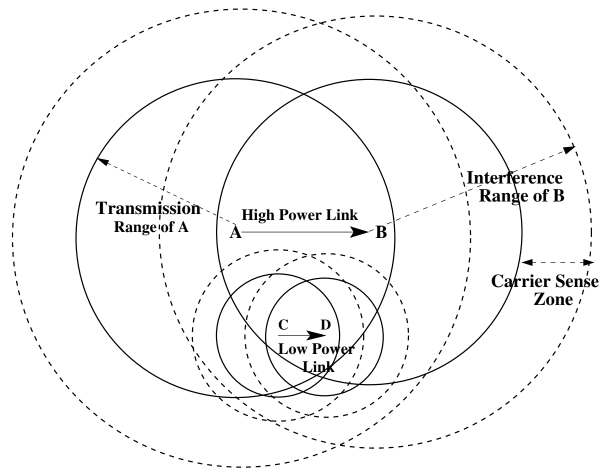

Fig. 1. Example of Low Power Link hidden from a High Power Link

RTS/CTS frames are sent at a lower "basic" data rate, which is 1Mbps for 802.11b. The Cisco Aironet 350 data sheet lists the typical range for packets sent at a constant transmit power for different data rates: indoor 130 ft at 11 Mbps, 350 ft at 1 Mbps; outdoor 800 ft at 11 Mbps, 2000 ft at 1 Mbps. Thus, RTS/CTS frames travel and suppress three times the distance of data packets at constant power. The overall effect is that considerable floor space is reserved by RTS/CTS, reducing the number of concurrent transmissions and limiting spatial reuse.

Ideally, if a node could identify future interferers of its impending conversation, then its RTS/CTS could be set at the optimal transmit power needed to suppress the furthest future interferer, rather than at the maximum transmit power. This would reserve the minimum floor space needed to suppress interferers and maximize spatial reuse. Possible techniques for obtaining the intent of future interferers could include mining historical behavior to make a prediction, as well as having nodes signal their intent early. At first glance, both approaches appear complicated and problematic.

An alternative approach taken by SHUSH is to be reactive rather than proactive in an asymmetric power control environment. In this approach, nodes such as C and D initially conduct their RTS-CTS-DATA-ACK exchange at optimum power. Only after there is interference do the nodes react by identifying the source of the interference via the header fields in the interfering packets. Nodes will then calculate the optimal transmit power needed to reach the interferer, and send only the first frame of the interrupted conversation at optimal power to SHUSH the interferer *a posteriori*. All subsequent frames are transmitted again at the power level sufficient to communicate with node D. The benefits of this reactive approach are that only the optimal (minimum) floor space is reserved, instead of the maximum floor space, and the interferer is identified and suppressed. As a result, spatial reuse is increased and more concurrent conversations can take place. As we will show, the aggregate throughput is considerably enhanced despite interruptions to ongoing conversations. Moreover, this reactive approach conserves energy by sending every transmission at the minimal transmit power necessary.

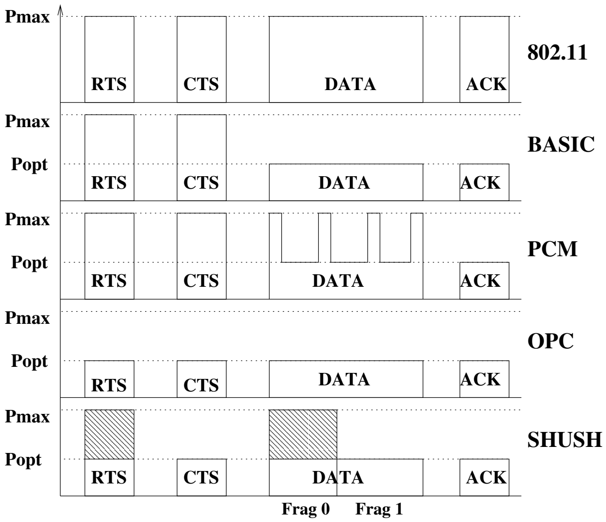

Fig. 2. Overview of transmit power controlled MAC protocols

By SHUSHing the interferer after the fact, SHUSH's principle is to respond to concrete information about interference rather than to anticipate worst-case interference. Mobility would further complicate the design of the SHUSH protocol and we evaluate the protocol for a stationary ad-hoc network.

We summarize the behavior of several transmit power controlled MAC protocols, including plain 802.11, BASIC, and SHUSH in Figure 2. In plain 802.11 without power control, RTS, CTS, DATA and ACK are all sent at a default maximum transmit power P_{max}. Asymmetric transmit powers allows variation across these four packet types. BASIC sends RTS and CTS at P_{max} and sends DATA and ACK at optimum power P_{opt}. OPC refers to a minimum-energy strategy of optimal power control (OPC), in which all four packet types are sent at minimum transmit power needed to maintain connectivity. OPC was depicted in Figure 1 as being susceptible to the general hidden terminal problem. In reality, overall energy costs of OPC may be higher due to retransmissions caused by collisions from the general hidden terminal problem.

A power controlled MAC (PCM) protocol was proposed for 802.11 [2]. PCM provides a mechanism to avoid collisions from nodes in the carrier sense zone. In PCM, RTS/CTS packets are transmitted at maximum power and data is periodically also transmitted at maximum power; the data is otherwise sent at optimum power to conserve energy. The periodic maximum power data transmissions enable nodes in the sender's carrier sense zone to stay suppressed throughout the sender's transmission. A drawback, as noted earlier, is that the RTS/CTS transmission at maximum power suffers from poor spatial reuse and degraded throughput in transmit power controlled environments. PCM is also focused on limiting interference from nodes in the carrier sense zone, while SHUSH addresses a broader issue of interference from nodes throughout the expanded interfering terminal zone.

A second critical issue encountered by MAC layer design given asymmetric transmit powers is *fairness* of medium access. There are two mechanisms of unfairness introduced by transmit power control. First, because of the general hidden terminal effect, high power conversations can inherently and arbitrarily interrupt hidden low power conversations, forcing retransmissions and unfairly degraded throughput for low power conversations. Meanwhile, the high power conversations will continue to gain access to the medium and achieve high throughput. Second, this inherent unfairness favoring high power conversations over low power conversations is exacerbated by the backoff algorithm. After a collision, the backoff algorithm manages how long nodes delay before retransmitting, typically increasing the backoff interval after repeated collisions. For example, the IEEE 802.11 protocol employs the Binary Exponential Backoff (BEB) algorithm [3]. The unfairness caused by BEB in 802.11 is a well-known problem [8], [9]. BEB favors the last node that was successful in transmission. This exacerbates the fairness problem in heavy traffic as the unsuccessful nodes do not gain access to the channel [28]. In our case, the unsuccessful nodes are repeatedly the nodes transmitting at low power. For example, if the nodes in Figure 1 employ 802.11's BEB algorithm, then the successful transmission of packets from A to B allows node A to reduce its backoff window to CWmin. The A-B conversation leads to repeated collisions at C and/or D, so that node C's backoff timer increases exponentially. Thus node C will have a much larger backoff interval when competing with node A for medium access. Furthermore, instead of deferring for DIFS, node C needs to defer for an EIFS period, which is much larger than the DIFS period. With high probability, node A would continue to gain access to the channel, while the backoff interval of the node C would keep increasing until it reaches the maximum of CWmax.

A variety of algorithms have been proposed to overcome the unfairness of the IEEE 802.11 protocol [7], [6], [20], [21]. One of the seminal solutions was the Multiplicative Increase Linear Decrease (MILD) algorithm, proposed in the MACAW protocol [6]. The essence of the work in these algorithms is to achieve global state in the ad-hoc network by exchanging local information about fairness between neighboring nodes. These methods suffer from the overhead required to communicate fairness state. Also, since the channel state information is intended to be shared by nodes that are within the transmission range, then low power nodes again would be at a disadvantage with respect to high power nodes, because low power fairness information would not be shared with as many nodes. To improve sharing, an alternative would be to employ a multi-hop routing protocol to forward fairness information many hops away, possibly even flooding the entire network. Such a method introduces additional overhead.

To demonstrate the unfairness of 802.11, we constructed a testbed consisting of four nodes following the topology of Figure 1. Two nodes communicating at low power were hidden from two other nodes communicating at high power. Each node consisted of a Soekris 802.11 test board using a transmit power-programmable CISCO Aironet 350 series cards with external antennae. Each sender introduced CBR traffic and packet sniffers were deployed to observe the data flowing in the network and to calculate the throughput. The packet sniffer collected the entire trace and the throughput was calculated. Figure 3 illustrates the resulting throughput of each pair of simultaneously communicating nodes. Clearly, the low power nodes communicating at 0dBm suffer a dramatically lower throughput than the higher powered nodes operating at 20dBm. Similar results were reported in [27], where a difference as small as 2dB was sufficient to prevent a weaker node from accessing the channel, while the stronger node achieves reliable consistent throughput.

To address the unfairness issue, SHUSH employs a simple stateful strategy that is grafted into the reactive strategy of SHUSHing the interferer. SHUSH employs the principle that a node N that has been interrupted has a higher priority to access the medium than typical nodes, since node N had been communicating beforehand. Let us term this principle the *interruption principle*. Therefore, after an interruption of an ongoing conversation, the interrupted node should be able to access the medium *sooner* than other nodes. SHUSH employs the additional principle that the interrupted node waits until after the interrupter has finished before grabbing the channel sooner than other nodes. This second principle avoids immediately interrupting the interrupter, on the theory that continued interruptions will cause a domino effect leading to decreased throughput. Let us term this second principle the *patience principle*. This is analogous to being interrupted during a discussion, politely allowing the interrupter to finish, and then asserting oneself in a vocal manner immediately after the interrupter has finished in order to grab the medium and finish the interrupted discussion. A specific instantiation of these principles in 802.11 would be to allow an interrupted node to grab the channel during the DIFS interval immediately following completion of the interferer's conversation. We demonstrate that SHUSH's reactive strategy combined with SHUSH's two principles of interruption and patience achieve fairness while maintaining high throughput in the presence of asymmetric transmit powers.

In the rest of the paper, Section II explains the SHUSH MAC protocol in detail. Section III provides an in-depth analysis and evaluation of the goodput, fairness, spatial reuse, and energy consumption of SHUSH compared to 802.11, BASIC, PCM, and OPC transmit power controlled MAC protocols. Section IV provides the background related work and Section V concludes the discussion of SHUSH.

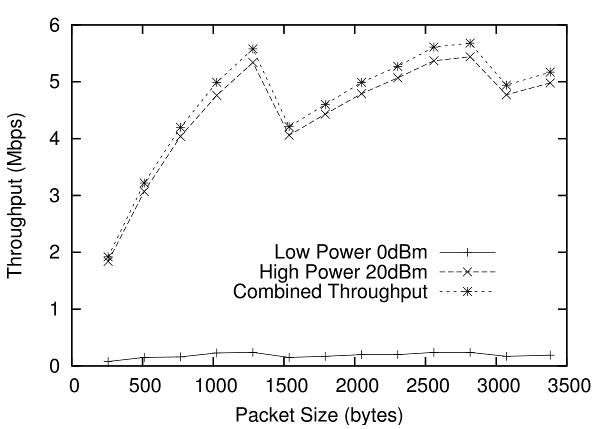

Fig. 3. Unfairness due to high power links in 802.11.

II. SHUSH PROTOCOL

As discussed in Section 1, transmit power control increases the number of hidden terminals in the network and exacerbates the unfairness of medium access for the less powerful links in the network. Current solutions proposed to overcome the hidden terminal problem rely on transmitting the RTS/CTS frames at maximum power and/or periodically stepping up the transmit power while transmitting the data frames. Both the approaches reduce the spatial reuse of the network and reduce the aggregate throughput of the network. The solutions proposed also do not take into consideration the unfairness introduced by transmit power control. SHUSH provides the first comprehensive solution to the problem of general hidden terminals which is both fair as well as efficient. The main goals of the SHUSH protocol are to provide a unified solution that addresses hidden terminal effects while also achieving the following:

- Enhanced spatial reuse and improved aggregate throughput throughout the wireless network
- Fair sharing of the channel between low powered and high powered links
- Achieving the above without enforcing RTS/CTS based collision avoidance
- Minimizing overhead of the protocol in the absence of transmit power control and hidden nodes
- Reducing power consumption
- Minimizing modifications to the standard

SHUSH maintains a conservative philosophy with respect to transmission power in an environment with asymmetric transmit powers. All conversations begin at the optimal transmit power, with the intent of minimizing interference and maximizing spatial reuse and aggregate throughput. There are a large number of algorithms that have been proposed to achieve transmit power control in 802.11 [32] [12] ,[16]. Some algorithms implement power control by modifying the MAC frame headers and others implement power control by out of band signaling. The upcoming IEEE 802.16 protocol, which specifies a metropolitan-area networking protocol, supports transmit power control and channel quality measurements as well as additional tools to support cell planning and efficient spectrum use [34]. Each MAC frame contains the information required for power control. Thus SHUSH is agnostic to exact implementation of transmit power control and any of the existing techniques can be used to achieve power control.

In the event that an ongoing low power conversation is interrupted by a high power conversation that is unable to hear the hidden conversation, then SHUSH initiates a protocol for the interrupted node(s) to contact and SHUSH the interferer(s). By notifying the high power nodes of the interruption, the interrupted nodes gain access to the channel and reserve the channel for the duration of the incomplete communication. This notification can either take the form of a control message (RTS/CTS) or a DATA fragment packet, as discussed below. This sequence of events is graphically depicted in the SHUSH timeline of Figure 4. The timeline assumes the topology as shown in Figure 1. In this case both the low power nodes are withing range of the high power nodes. The figure shows the

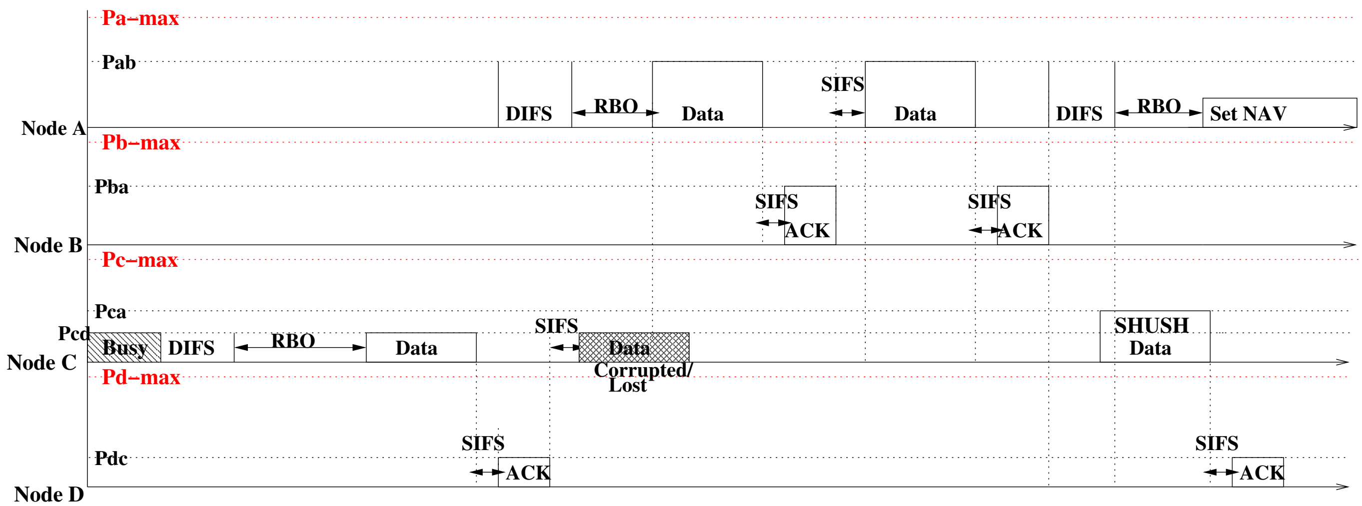

Fig. 4. Timeline of SHUSH protocol in the context of 802.11. Nodes A and B are the high power sender and receiver respectively and nodes C and D are low power sender and receiver respectively.

SHUSH data frame being transmitted by node C at a power level $P_{ca} > P_{cd}$.

Before we describe the details of the SHUSH protocol, we explain the interframe spaces and fragmentation as proposed by the IEEE 802.11b MAC protocol. Although SHUSH is not confined to the IEEE 802.11b standard, we evaluate the protocol and compare the protocol against already proposed transmit power control protocols based on 802.11b. The IEEE 802.11b standard defines 3 different interframe time intervals, *SIFS*, *DIFS* and *EIFS*. The *SIFS* is the shortest of the interframe spaces and is used for a station to retain access of the channel once acquired. The *DIFS* is used by stations to transmit data/management frames. A station is allowed to transmit a frame only if it senses the medium to be free at the end of the *DIFS* interval and its backoff timer has expired. The *EIFS* is used by stations which sense the carrier to be busy but cannot decode the frame. Hence nodes in the carrier sense zone (Figure 1) need to defer for *EIFS* rather than *DIFS* before transmitting the frame. According to the Direct Sequence Spread Spectrum (DSSS) PHY specification, a slot time is 20μsec and the *SIFS* is defined to be 10μ sec. The *DIFS* and *EIFS* are derived by the following equations.

$$DIFS = SIFS + 2 * SlotTime = 50\mu sec$$

$$EIFS = SIFS + (8 * ACKFrameLength) + DIFS +$$

$$aPreambleLength + aPLCPHeaderLength = 364\mu sec$$

The IEEE 802.11 protocol specification defines a fragmentation mechanism in which network level packets greater than a pre-defined *fragmentation threshold* are partitioned into smaller MAC frames. These fragmented frames are transmitted in a *fragment burst* i.e. once the node has gained access to the channel it shall continue to send fragments until all fragments of a network level packet have been transmitted or it does not receive an acknowledgment. In the presence of hidden terminals in the network, fragmentation assists in faster recovery as well as lower power consumption of the nodes that experience interference/collisions. However fragmentation adds some overhead as each data fragment frame needs to be separately acknowledged. Several adaptive algorithms [31] are designed to enable or disable fragmentation based on channel conditions. The firmware of most 802.11 client adapters automatically enable fragmentation when the link quality drops below a threshold.

In order for SHUSH to operate correctly, SHUSH must be able to determine:

- the source address of the interferer whose transmission caused the collisions/interference
- the optimum power with which to SHUSH the interferer
- when the interrupting conversation has completed
- which interrupted node gets to SHUSH which interferer if there is more than one of each, and when

In the following, we explain how SHUSH determines these elements.

A. Obtaining information about the interferer

After experiencing interference, at least one of the interrupted nodes will be able to hear at least one of the interferer(s). This interrupted node must be able to acquire the address of the interferer, the optimum power needed to reach the interferer, and also the time when the interferer has completed its conversation.

A variety of interference scenarios may occur. Consider the topologies shown in Figure 5, which shows only three of the possible fifteen interference scenarios as enumerated in Figure 6. Here nodes A and B are the high power sender (HPS) and high power receiver (HPR) respectively. Nodes C, C', C", are the low power senders (LPS) and D, D', and D" are the low power receivers (LPR) that are hidden from the nodes HPR and HPS. C and D are within the transmission range of both nodes A and B. Nodes C' and D" are within the transmission range of only node B. Nodes D' and C" are outside the transmission range of both nodes A and B.

For reasons described in the next subsection, SHUSH needs to obtain the MAC address of the interferer. The interferer may

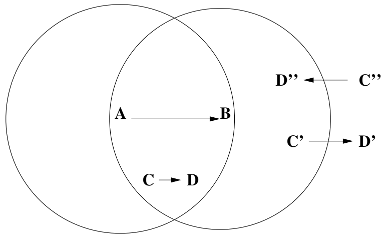

Fig. 5. Example of three different topologies of the high power nodes A and B and low power nodes C, C’, C”, D, D’ and D”.

Node ’B’ Interfering With \ Node ’A’ Interfering With	C	D	CD	~CD
C			✓	
D				
CD				
~CD				

Fig. 6. Topologies of nodes A-B and nodes C-D. The box representing the topology in Figure 1 is checked. The shaded box represents that links AB and CD do not interfere with each other.

be either the HPS or the HPR, or in some cases both. If the interferer is HPS, then every data frame header in the IEEE 802.11 MAC protocol would have the source address encoded in the frame. If the interferer is HPR, then ideally we would like the address of the HPR to be encoded in the ACK frames. However, 802.11 only includes the destination address in ACK frames, i.e. only the HPS’ address is encoded in the ACK frames transmitted by HPR. While SHUSH is more general than 802.11, the specific implementation of 802.11 SHUSH in this paper uses the HPS’ address in place of the HPR’s address i.e. it uses the address of the node who transmitted the ACK frame.

Since the MAC address information is obtained from the MAC data and control frame headers, one caveat is that this approach depends upon there being at least two MAC frame headers transmitted between the HPR and HPS i.e. there must be atleast one more frame header following the frame that caused the interference in order for the low power interrupted nodes to receive the MAC address information. In the case where the data frames are not fragmented, or the data is too small for fragmentation, then an extra data frame with zero payload (just the MAC header frame) is transmitted which is also ACKed by the HPR. Thus the default DATA-ACK handshake is modified to DATA-ACK-DATA_HEADER-ACK. This modified DATA-ACK sequence enables the interrupted low power node to gain all the information required to SHUSH the high power nodes. A 802.11b data frame header is 28 bytes long and the ACK frame is 14 bytes long and these frames unlike the RTS/CTS control frames are transmitted at the same rate as the data frames. The trailer header mechanism adds a very small overhead to the default DATA-ACK handshake. The semantics of transmitting the extra trailer header with it’s acknowledgement is similar to fragmentation enabled with the exception that the data payload of the trailer fragment is set to 0. The 802.11 protocol already supports fragmentation and this requires minimal modifications to the existing protocol. The benefits of the extra trailer header mechanism tackling the aggravated hidden terminal problem are analyzed in detail in Section III where SHUSH is compared with other collision avoidance schemes.

In the case where fragmentation is enabled, then the extra trailer header is not required as the data fragment train and the corresponding ACKs provide the necessary information for the low power nodes to SHUSH the high power nodes.

SHUSH depends upon the MAC layer packets to have embedded information concerning the transmit power of each packet. Typically, the MAC layer header is modified to include field(s) required for transmit power control like RSSI and TxPower. Several transmit power control algorithms have proposed modifying the 802.11 header to incorporate such power control information [12], [16]. Given the transmit power of the interferer and the RSSI at the interrupted node, the interrupted node can calculate the optimal transmit power required to SHUSH the interferer. SHUSH is agnostic of the specific implementation of transmit power control and can leverage off any of these protocols to achieve transmit power control.

The next important issue is to determine how the interrupted nodes know when the fragment burst between the high power interfering nodes has completed, i.e. exactly when the ACK frame for the last data fragment would be transmitted. In the case that HPS is the interferer, the 802.11 data fragments would have embedded within their headers information about the duration of the transmission. When HPR is the interferer, the 802.11 ACKs will also have the duration information embedded within their headers. Thus, the lower nodes will be able to determine when the interference from HPS/HPR will cease.

B. SHUSHing the interferer

The next task is to SHUSH the interferer and then resume the interrupted low power conversation. Normally, an 802.11 node that has been interrupted by interference will backoff using the BEB algorithm. As observed earlier, this leads to unfair medium access, especially for low power conversations. In SHUSH, the interrupted node does not exponentially back off, and instead waits until the HPS/HPR conversation has completed. At this point, the interrupted node is poised to SHUSH the interferer and gain control over the medium.

SHUSH takes advantage of the fact that there is a DIFS waiting interval enforced after the completed conversation i.e. after the ACK for the last data fragment is received, in which HPS and HPR are idle. After a successful transmission, the high power nodes defer for an interval of $DIFS+RBO$ where RBO is the random backoff. The RBO is calculated as:

$$RBO = Random() * aSlotTime$$

where $Random()$ is a pesudorandom integer drawn from a uniform distribution over the interval $[0, CW]$ and $aSlotTime$

is 20μsec for the DSSS PHY specification of 802.11b. To regain access to the channel the low power node reinitiates the interrupted conversation during the DIFS interval, before the high power node starts the random backoff (RBO). On a successful transmission node A (HPS) would set its CW to CWmin which is defined to be 31 for the DSSS PHY. Hence the RBO generated ranges from 0 to 620μsec. To gain a fair share of the wireless medium, the low power nodes (node C) need to SHUSH the high power source nodes (node A) before the high power node starts the RBO, as the RBO could also be set to 0μsec. SHUSH adheres to the interruption principle, which gives priority to a node that has been interrupted by a high power conversation, i.e. it is only fair that the interrupted conversation be given first priority to resume.

SHUSH divides the DIFS interval into 2 parts $aSlotTime$ and $aSlotTime + SIFS$ as shown in figure 7. This division orders the SHUSH responses based on whether the LPS or LPR was interfered with. For example, in Figure 5, node C corresponds to LPS and node D corresponds to LPR. The *DIFS* interval was defined to be $SIFS + 2 * aSlotTime$. If LPS has been interrupted, it has all the information necessary to SHUSH the interferer. LPS will then initiate a SHUSH within the first half of the DIFS interval. If instead only the LPR is interfered with, then the LPR does not know whether the LPS has been interfered with. For this reason the LPR waits during the first half of the DIFS to see if the LPS initiates a SHUSH. If no such SHUSH is detected, then the LPR initiates a SHUSH in the second half of the DIFS.

A random backoff from the interval of [0-20]μs is selected before transmitting the SHUSH. This ensures that multiple low power nodes that have been interrupted do not transmit the SHUSH frame simultaneously. Without the random backoff, the SHUSH frames would result in a collision at the high power nodes as every low power interrupted node would transmit the SHUSH at the same instant. It is also possible for multiple low power nodes that are interrupted to be hidden from each other. In this case, the SHUSH frames transmitted by the LPR/LPS would collide at the HPS which would lead to the high power node to set its NAV to EIFS and backoff. Thus in this case the channel reservation of the low power nodes would not be communicated to the high power nodes.

The last issue concerns what kind of SHUSH message gets sent to the interferer. An important design constraint of SHUSH was to make minimal modifications to the existing MAC protocol. Rather than design a new control frame, we make use of the existing RTS, CTS, and DATA frames to signal a SHUSH. If LPS has been interrupted, then the message sent by LPS will depend on whether RTS/CTS is enabled. If RTS/CTS is enabled, then the SHUSH frame consists of an RTS sent at the optimum power. If RTS/CTS is not enabled, then the SHUSH frame consists of the data frame that was interfered with. Thus unlike BASIC and PCM SHUSH does not enforce the use of the RTS/CTS based collision avoidance. If only LPR was interrupted, then the SHUSH frame consists of an unsolicited CTS sent at optimum power. All SHUSH frames contain a duration field that indicates how long to backoff. This will cause HPR/HPS to set their NAV fields and back off. The LPS on receiving this unsolicited CTS frame resumes the interrupted conversation at optimal power after a SIFS interval. The mechanism used by LPR to SHUSH the high power nodes by transmitting the unsolicited CTS frame is similar to the protection mechanism used by 802.11g devices when operating in a mixed mode network comprising of 802.11b devices. Before starting transmission, an 802.11g device needs to inform the 802.11b devices by transmitting the CTS-to-self to avoid collisions/interference. Similarly, the LPR by transmitting the unsolicited CTS frame avoids collisions/interference from the high power nodes.

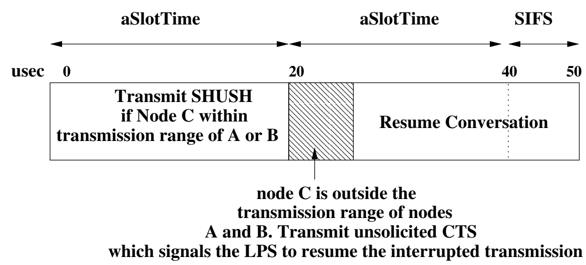

Fig. 7. The synchronization during the DIFS time interval

III. SHUSH Protocol Evaluation

To evaluate the SHUSH protocol, we compare the performance of the protocol with 4 other transmit power control 802.11 based MAC protocols. We implement and compare SHUSH with Optimal Power Control (OPC), BASIC [10] and Power Controlled MAC (PCM) [2]. We also compare the performance of these protocols with 802.11b (802.11) without any transmit power control. Figure 2 provides an overview of the behavior of the 5 different transmit power protocols that we evaluated.

A. ns2 Simulation Setup

We implement the above mentioned protocols in the ns2 simulator (ns-2.26) with the CMU wireless extensions [33]. The channel bit rate was set at 2Mbps for the data frames and control frames were transmitted at the basic rate of 1 Mbps. Packet size was set to 800 bytes with the fragmentation threshold set at 400 bytes. Hence each network level packet was fragmented into 2 data fragments. With fragmentation enabled we evaluated the trace files generated and observe an improvement of aournd 6% in the goodput as compared to the trailer header mechanism. However, the fairness and capacity of the network are the same for both the techniques. We use a CBR traffic source for each pair of nodes (flow) in the network. The 2-Ray ground reflection model was used. We do not consider mobility in our simulations. We evaluate the protocols for the chain and random topologies over a flat grid of $500m^2$. The random topology was generated by setting up CBR traffic between any 2 random nodes in the network. The nodes were selected such that they are within transmission range of each other. Figure 15 is an example of a 20 node random topology consisting of 10 CBR traffic flows. The receive threshold for 1Mbps, 2Mbps. 5.5Mbps and 11Mbps were set at -92dB, -90dBm, -85dBm and -80dBm respectively.

The chain topology was generated by setting up CBR traffic flows between 2 adjacent nodes in a chain. The distances between adjacent nodes in the chain were randomly selected. An example of a chain is $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \cdots$. Here node 2 is a source of a CBR traffic as well as a sink for the CBR source node 1.

The maximum distance between adjacent nodes for the chain as well as the random topology was set at 200m. This is the farthest that a node could communicate at the maximum transmit power. We used 10 different power levels similar to those used in [2]. At maximum transmit power a node can communicate with another node at a maximum distance of 200m.

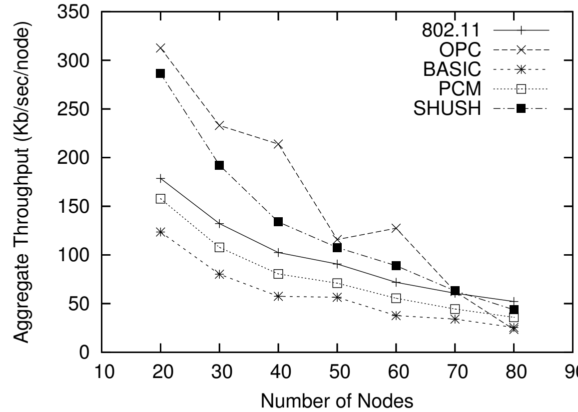

Fig. 8. Aggregate Goodput with RTS/CTS signaling (Error bars not shown)

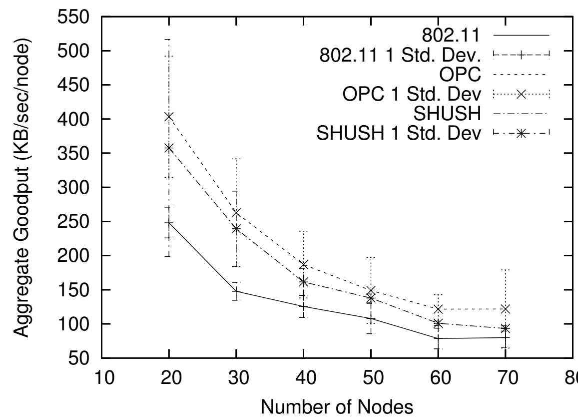

Fig. 9. Aggregate Goodput without RTS/CTS signalling with error bars of 1 std. dev.

B. Simulation Results

1) Goodput: We first compare the five protocols by measuring the aggregate goodput of the network. Goodput is a measure of the amount of useful application layer data received by the node, and hence all the MAC layer and network layer control signaling is considered overhead that reduces goodput. We generated 10 different random topologies and for each topology we divide the total goodput of the network by the number of active flows in the network ($Kbits/sec/node$). We measure the aggregate goodput of the network for each of the five protocols. We also varied the number of nodes in the network from 20 to 80, i.e. varied the number of active flows in the network from 10 to 40.

Figure 8 shows the aggregate goodput of the network with RTS/CTS signaling enabled. OPC outperforms all the other protocols. This is because the high power transmissions experience no interference from the smaller low power transmissions. Thus the high power nodes always have their backoff window at CW_{min} and dominate the medium by saturating the link between them. On the other hand the low power nodes are constantly interrupted and their backoff window keeps on increasing exponentially. However, as the number of flows increase in the network, the aggregate goodput of OPC drops and approaches that of the other protocols. This is because as the number of flows increase, the number of high power transmissions that interfere with each other also increase. We also observe that SHUSH does better than 802.11, BASIC and PCM. This is because 802.11, BASIC and PCM all transmit the RTS/CTS at maximum power and hence result in a lower spatial reuse. SHUSH transmits the RTS/CTS at optimal power and only on a collision does it require to step up the power as described in II.

Figure 9 shows the goodput of 802.11, SHUSH and OPC without RTS/CTS negotiation. PCM and BASIC enforce the use of RTS/CTS based collision avoidance and hence cannot be compared. We observe similar results here and also an improvement in the aggregate goodput of all the 3 protocols in the absence of RTS/CTS.

We also simulate the chain topology and calculate the aggregate goodput. Figure 10 shows the aggregate goodput of the chain topology. Again, OPC outperforms all other protocols. BASIC has the lowest aggregate goodput and PCM and 802.11 nearly show the same aggregate goodput across all the chain lengths. These results are consistent with those observed in [2]. SHUSH again outperforms BASIC, PCM and 802.11.

2) Fairness: One of the objectives of the SHUSH protocol is to provide a fair share of the medium to low power and high power nodes in the network. To evaluate fairness, we measure the standard deviation of the goodput of the individual flows in the network. This standard deviation is aggregated over 10 different random topologies. Thus a high standard deviation implies that the protocol is unfair by providing unequal share of the medium across the individual flows. A low standard deviation implies that all flows in the network are provided nearly equal share of the medium and hence the protocol is more fair. Figure 11 shows the aggregate standard deviation with the RTS/CTS signaling for all 5 of the MAC protocols for increasing number of flows in the network. Clearly, OPC is the most unfair protocol in sharing the channel. This is because the high power transmissions dominate the channel in OPC as explained above, starving low power conversations. PCM, BASIC and SHUSH show comparable fairness. Figure 12 shows similar results of the aggregate standard deviation without RTS/CTS signaling with OPC again being the most unfair and SHUSH performing better than 802.11 as well as OPC.

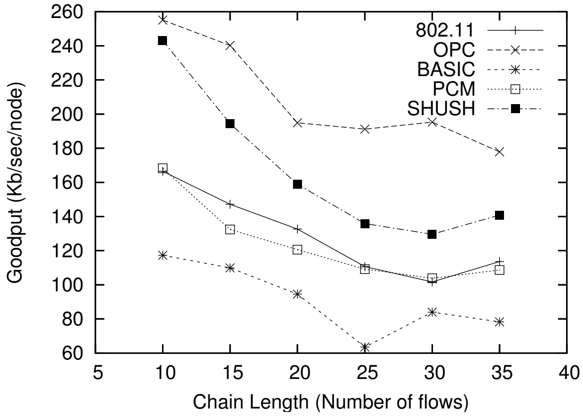

Fig. 10. Aggregate Goodput of a Chain topology (Error bars not shown)

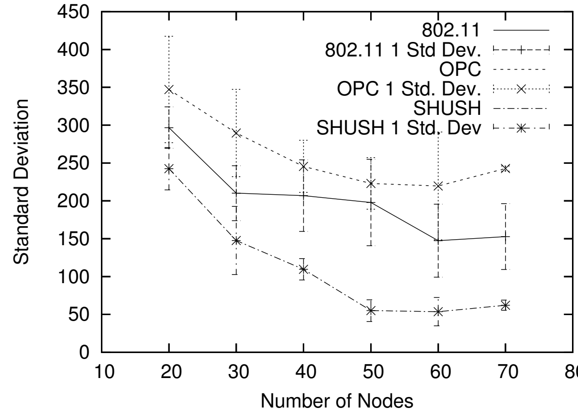

Fig. 12. Std. Dev. in goodput of individual flows without RTS/CTS signalling

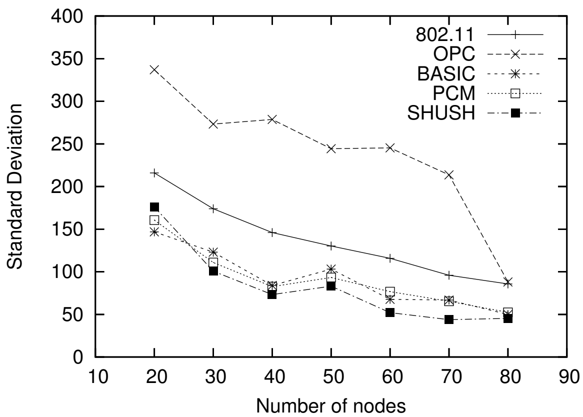

Fig. 11. Std. Dev. in goodput of individual flows with RTS/CTS signalling (Error bars not shown)

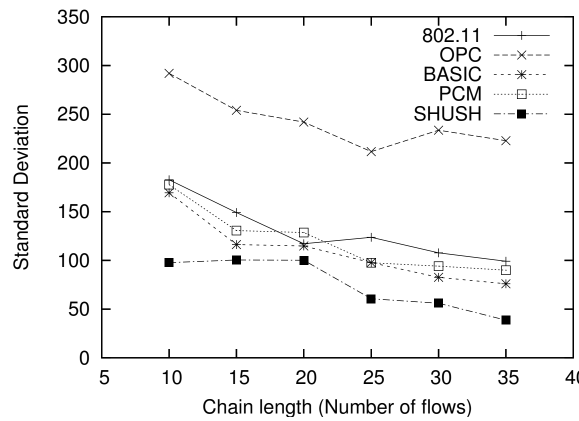

Fig. 13. Std. Dev. of goodput with Chain topology (Error bars not shown)

Figure 13 compares the fairness of the 5 protocols for the chain topology. Again, OPC is the most unfair while SHUSH achieves the fairest sharing of the medium.

As observed from the results of the chain and random topologies, even though OPC provides a higher aggregate goodput, it is the most unfair of all the protocols. Figure 14 shows the OPC goodput of the individual flows in a 20 node network (10 flows). The height of the bars demonstrate the goodput of the individual flows and the line graph at the bottom plots the distance between the source and destination node for every flow. Figure 15 shows the topology of this network. Clearly, flow 8 is the most powerful transmission and dominates flows around it i.e. flows 3,6,7,9. Similarly, flow 2 dominates flow 1 and 10. This explains the high goodput obtained by flow 2 and 8. These high power transmissions constantly force the less powerful nodes to backoff as explained in section II and hence the goodput of flows 3,6,7,9,1 and 10 is very low. Even though flow 5 is a low power transmission, it achieves a high goodput since it is isolated from all the other flows in the network. Hence, flow 5 does not experience any interference/collisions from the other flows. This clearly demonstrates the drawback of OPC in which hidden terminals are forced to backoff and are continuously interfered with when transmitting.

Figure 16 gives an estimate of the spatial reuse of the network obtained by SHUSH, OPC and 802.11. The spatial reuse also reflects the fairness of the MAC protocols. The spatial reuse is calculated as the number of active transmissions per unit time interval of the trace. The time interval was set to $0.5 sec$ and for each time interval we measure the number of unique nodes that receive an application layer packet. The graph plots the spatial reuse of a 70 node network. The x-axis plots the time intervals and the y-axis measures the pairs of nodes that receive an application layer packet in that time interval. Clearly, SHUSH outperforms 802.11 due to the *patience principle* employed by SHUSH. Hence, unlike OPC which does not provide any chance for the low power nodes to transmit, SHUSH provides a much improved spatial reuse of the network. BASIC and PCM achieve similar spatial reuse as that obtained by 802.11.

3) Energy Consumption: We evaluate the energy consumption of the 5 different protocols based on the metric joules/byte transmitted. Figure 17 and Figure 18 show the energy consumption for the random and the chain topologies respectively. 802.11, which lacks power control, consumes the maximum energy and is constant across increasing nodes in the network. OPC, which sends every frame at the optimal transmit power has the minimum power consumption. Our results confirm with the results obtained in [2] where BASIC

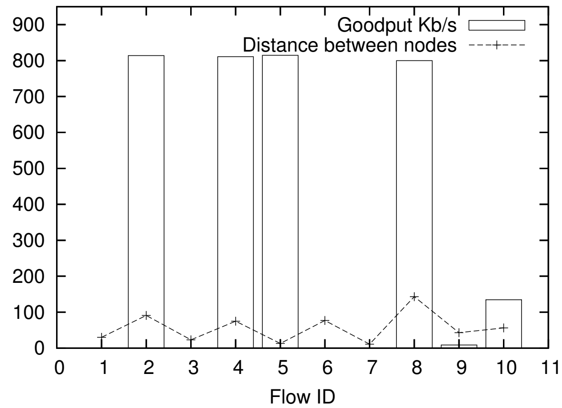

Fig. 14. Goodput of a 20 Node random topology network using OPC

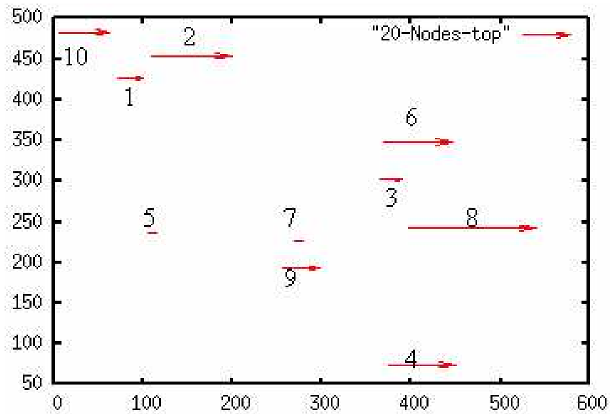

Fig. 15. Random topology of the 20 Node network

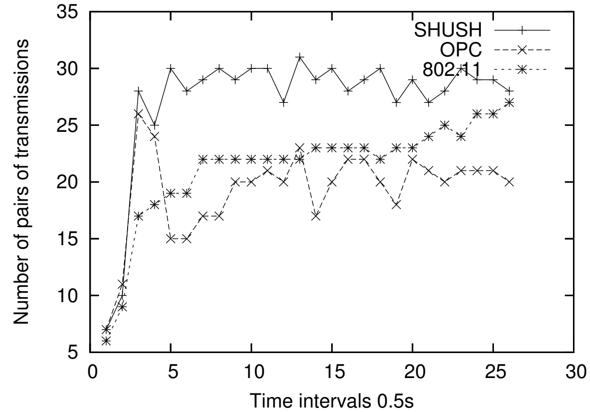

Fig. 16. Spatial reuse of the network (70 node random topology with 35 pairs)

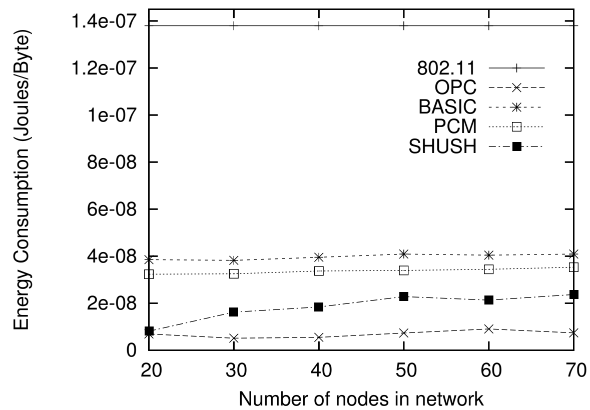

Fig. 17. Energy consumption for random topology

consumes more power as compared to PCM. However it is interesting to note that the power consumption for both BASIC and PCM remains constant even with increasing number of nodes in the network. This is mainly because BASIC and PCM are not reactive to the collisions and interference caused by the high power nodes. BASIC and PCM always transmit the RTS/CTS at maximum power and PCM always steps up its transmit power periodically irrespective of the number of hidden terminals in the network. SHUSH on the other hand is reactive to the number of nodes in the network. When the number of flows in the network are small, SHUSH nearly performs as well as OPC. With increasing number of hidden terminals in the network, SHUSH needs to step up the transmit power and inform the high power nodes of the interference caused. Hence, the power consumption increases with increasing number of hidden terminals and thus SHUSH is more reactive as compared to PCM and BASIC.

IV. Related Work

The COMPOW [15] protocol maintains that the network capacity is asymptotically maximized by selecting a common minimum transmit power for all nodes equal to the minimum power at which the network maintains connectivity. [19] uses a similar approach but builds clusters so as to maintain connectivity with only a limited number of neighbor nodes. Both the above approaches have the drawback that a single distant node could cause the entire network to transmit at a higher power level.

Several solutions discuss the implementation of the OPC method of transmit power control in IEEE 802.11 [12], [16]. The proposals discuss how the frame formats would need to be changed. However, as shown in Figure 1, OPC transmit power control in ad-hoc networks increases the number of hidden terminals in the network, which in turn results in increased interference and retransmissions.

Busy tone multiple access BTMA [25] proposes to combat hidden terminals in CSMA. BTMA requires a data channel and a control channel. The base station transmits a busy tone signal on the control channel as long as it senses a carrier on the data channel. A busy tone power control protocol was proposed in [26] where the sender transmits the data and the busy tone at the minimum power and the receiver transmits the busy tone at maximum power. A neighbor estimates the channel gain from the busy tone and is allowed to transmit if its transmission would not cause interference with the ongoing transmission. Similar solutions [22] and [23] are proposed which use this dual channel approach. Though the above protocols do not tradeoff spatial reuse, the solution requires two channels. [35] is a single channel solution which embeds

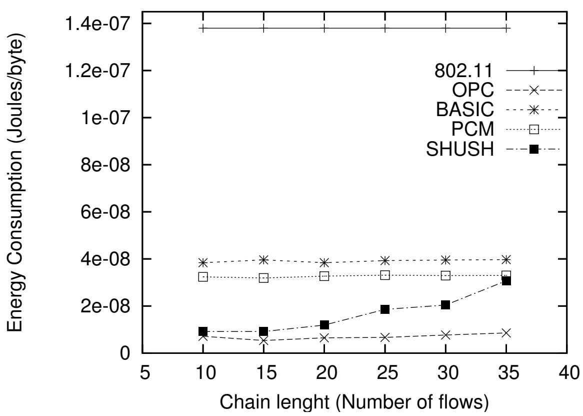

Fig. 18. Energy consumption for chain topology

the information about the interference margin into the CTS frame. This information used to bound the transmission power of potentially interfering nodes.

FAMA is a protocol developed for single-channel packet radio networks [24]. FAMA employs the RTS/CTS handshake and is based on implementing a busy tone mechanism using a single channel by making the receiver send multiple CTSs that last long enough so that the hidden nodes backoff. FAMA requires the receiver to transmit $(2N+1)$ CTS's in response to an RTS, where N is the number of hidden terminals in the network.

Unfairness in the RTS/CTS exchange due to asymmetric transmit powers was addressed in [13]. The solution proposed is to propagate the CTS frame of a low power node a reasonable number of times so as to avoid collisions caused by the higher power nodes. If the minimum transmit power has range 1 unit and maximum transmit power node has a range of N units, the protocol requires the CTS frame to be transmitted 2N-1 times for a chain topology with nodes less than 1 unit apart. The drawback of the extended RTS/CTS scheme is the overhead of forwarding the CTS frames multiple hops. The scheme is also confined to RTS/CTS, and does not apply when RTS/CTS is disabled, as occurs in many 802.11 deployments.

An alternate solution to overcome the unfairness due to the BEB algorithm in 802.11 is to provide service differentiation among the traffic flows with different priorities [29], [30]. In this approach each station will listen to the priority limit value sent by a master station to determine whether it can contend for the medium. Thus a station is allowed to contend for the medium only if it has a priority assigned greater than the priority limit. For ad-hoc networks, which do not have any central control point, explicit cluster topologies would need to be set up and a master needs to be elected as the cluster head.

MiSer [36] proposes a per frame transmit power control and rate control algorithm. It pre-computes the optimal $\{$rate, power$\}$ table for a given $\{$data payload, path loss, frame retry count$\}$ and the lookup is performed at runtime. However, this solution is restricted to 802.11a and 802.11h protocols and also requires the RTS/CTS based collision avoidance mechanism.

Topology control/management and cross-layer optimization address how heterogeneous transmit powers affect the connectivity of a multi-hop wireless ad-hoc network [17],[18] and [19].

V. Conclusions

SHUSH is a MAC layer protocol for transmit power controlled wireless networks. SHUSH addresses two critical issues that are introduced by asymmetric transmit powers: the general hidden terminal problem; and unfairness of medium access. SHUSH addresses the general hidden terminal problem in a reactive manner, first identifying the interferer to an ongoing conversation and then sending a SHUSH signal to the interferer at the optimum power needed to reach the interferer and no further. The SHUSH signal can be in the form of an RTS, DATA, or unsolicited CTS. This reactive approach efficiently reserves the minimum floor space necessary to deal with the interferer and resume the ongoing conversation. To address fairness, SHUSH operates on two principles: the interruption principle enables interrupted nodes to access the medium sooner than other nodes, i.e. it's only fair that the interrupted conversation be given first priority to resume; the patience principle forces the interrupted nodes to wait for the interrupter to finish, thereby avoiding a domino effect of interruptions and preserving throughput. We compared SHUSH against four other transmit power controlled MAC protocols, and demonstrated that the resulting SHUSH protocol achieves superior aggregate throughput, spatial reuse, fairness, and minimal energy consumption in almost all cases.

References

[1] D.M. Novakovic,M.L. Dukic, ”Evolution of the Power Control Techniques for DS-CDMA Toward 3G Wireless Communication Systems” In Proc of IEEE Communications Surveys and Tutorials,2000.

[2] E.-S. Jung and N. H. Vaidya, ”A power control MAC protocol for ad-hoc networks,” in ACM MOBICOM, 2002.

[3] P. Karn, “MACA, a New Channel Access Method for Packet Radio”, ARRL/CRRL Amateur Radio 9th Computer Networking Conference, 1990.

[4] Cisco Aironet 350 Series WLAN card, www.cisco.com

[5] Chipcon CC1000 Radio, www.chipcon.com

[6] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, ”MACAW: A Media Access Protocol for Wireless LAN's,” ACM SIGCOMM, 1994.

[7] Z. J. Haas and J. Deng, ”On Optimizing the Backoff Interval for Random Access Schemes,” IEEE Transactions on Communications, vol. 51, no. 12, pp. 2081-2090, December 2003.

[8] C. E. Koksal, H. I. Kassab, H. Balakrishnan, ”An Analysis of Short-Term Fairness in Wireless Media Access Protocols,” Extended version of short paper to appear in Proc. ACM SIGMETRICS, June 2000.

[9] Harshal S. Chhaya and Sanjay Gupta,”Performance modeling of asynchronous data transfer methods of IEEE 802.11 MAC protocol”,Wireless Networks 3(3): 217-234 (1997)

[10] . Gomez, A. T. Campbell, M. Naghshineh, and C. Bisdikian, ”Conserving transmission power in wireless ad hoc networks,” in Proc. of IEEE Conference on Network Protocols (ICNP'01), Nov. 2001.

[11] S. Agarwal, S. Krishnamurthy, R. H. Katz, and S. K. Dao. ”Distributed Power Control in Ad-hoc Wireless Networks” In PIMRC01, 2001.

[12] J. Ebert and A. Wolisz, ”Combined tuning of rf power and medium access control for wlans,” Mobile Networks and Applications (Monet), vol. 1, pp. 1–11, July 2000.

[13] N. Poojary, S. Krishnamurthy, S. Dao, “Medium Access Control in a Network of Ad Hoc Mobile Nodes with Heterogeneous Power Capabilities,” IEEE Interenational Conference on Communications (ICC) 2001, vol. 3, pp. 872-877.

[14] P. Gupta and P. Kumar,”Capacity of wireless networks,” Technical report, University of Illinois, Urbana-Champaign, 1999

[15] S. Narayanaswamy, V. Kawadia, R. S. Sreenivas, and P. R. Kumar, Power Control in Ad-Hoc Networks: Theory, Architecture, Algorithm and Implementation of the COMPOW Protocol, In Proceedings of the European Wireless Conference pages 156–162, Florence, Italy, Feb. 25-28 2002.

[16] Luciano Bononi, Marco Conti, and Lorenzo Donatiello." A Distributed Contention Control Mechanism for Power Saving in Random-Access Ad Hoc Wireless Local Area Networks". In Proceedings of IEEE Intl. Workshop on Mobile Multimedia Communication - MoMuC'99, pages 114-123, San Diego, USA, November 1999.

[17] Vikas Kawadia and P. R. Kumar," Clustering by Power Control in Ad Hoc Networks", in IEEE Milcom, Volume 2, pages 1424-1428, 1999

[18] R. Ramanathan and R. Rosales-Hain. "Topology Control of Multihop Wireless Networks using Transmit Power Adjustment". Proceedings of the IEEE Conference on Computer Communications (INFOCOM), pages 404-413, Tel Aviv, Israel, March 2000.

[19] T. A. ElBatt, S. V. Krishnamurthy, D. Connors, and S. Dao. "Power Management for Throughput Enhancement in Wireless Ad hoc Networks". Proceedings of the IEEE International Conference on Communications (ICC), pages 1503–1513, New Orleans, LA, June 2000

[20] Zuyuan Fang, Brahim Bensaou, Yu Wang "Performance evaluation of a fair backoff algorithm for IEEE 802.11 DFWMAC". MobiHoc 2002: 48-57

[21] B. Bensaou, Y. Wang, and C. C. Ko, "Fair medium access in 802.11 based wireless ad-hoc networks," in Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc), August 2000.

[22] . Monks, V. Bharghavan, and W. Hwu, "A power controlled multiple access protocol for wireless packet networks," in Proceedings of IEEE Conference on Computer Communications (INFOCOM), Apr. 2001, vol. 1, pp. 1–11.

[23] A. Muqattash and M. Krunz, "Power Controlled DualChannel (PCDC) Medium Access Protocol for Wireless AdHoc Networks", INFOCOM 2003

[24] C. L. Fullmer and J.J. Garcia-Luna-Aceves, "Solutions to Hidden Terminal Problems in Wireless Networks," in Proceedings of ACM SIGCOMM '97, ACM, 1997.

[25] C. Wu and V. O. K. Li, "Receiver-initiated busy-tone multiple access in packet radio networks", in Proc. ACM SIGCOMM 87, 1987, pp. 336 342.

[26] S.-L. Wu, Y.-C. Tseng, and J.-P. Sheu. "Intelligent Medium Access for Mobile Ad Hoc Networks with Busy Tones and Power Control." IEEE Journal on Selected Area in Communications, 18(9):1647–57, 2000.

[27] C.Ware and T.Wysocki and J.F.Chicharo. "On the Hidden Terminal Jamming Problem in IEEE 802.11 Mobile Ad Hoc Networks." ICC 2001

[28] C. L. Barrett, C. Engelhart, M. V. Marathe, A. Sivasubramaniam. "Analyzing the Short-Term Fairness of IEEE 802.11 in Wireless Multi-hop Radio Networks." In Proceedings of the IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS) , October 2002

[29] M. Benveniste and G. Chesson and M. Hoeben and A. Singla and H.Teunissen and and M. Wentink. "EDCF proposed draft text." IEEE working document 802.11-01/13lrl. March 2001.

[30] L. Romdhani, Q. Ni, T. Turletti."AEDCF: Enhanced Service Differentiation for IEEE 802.11 Wireless Ad-Hoc Networks",in IEEE WCNC,New Orleans, Louisiana, March, 2003.

[31] N. Ramos, D. Panigrahi, S. Dey, "Energy-Efficient Link Adaptations in IEEE 802.11b Wireless LAN", in IASTED Intl. Conf. on Wireless and Optical Communications, pp. 578-583, Banff, Alberta, July 2003

[32] A. Sheth, R. Han "Adaptive Power Control and Selective Radio Activation for Low-Power Infrastructure-Mode 802.11 LANs." ICDCS Workshops 2003 Pages 812-817

[33] The CMU Monarch Project. The CMU Monarch Project's Wireless and Mobility extensions to NS.

[34] The IEEE 802.16 Broadband Wireless Access Working Group, "Transmit Power Control Submission to IEEE 802.16 TG4"

[35] A. Muqattash and M. KrunzThe,"A single-channel solution for transmission power control in wireless ad hoc networks" in Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing MobiHoc 2004, 210-221, 2004.

[36] D. Qiao, S. Choi, A. Jain, and Kang G. Shin, "MiSer: An Optimal Low-Energy Transmission Strategy for IEEE 802.11 a/h", in ACM MobiCom'2003, San Diego, CA, September 14 19, 2003.