This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2480398, IEEE Transactions on Wireless Communications

Alleviating Hidden and Exposed Nodes in High-Throughput Wireless Mesh Networks

Sandip Chakraborty, *Member, IEEE*, Sukumar Nandi, *Senior Member, IEEE*, Subhrendu Chattopadhyay

***Abstract*—This paper proposes an opportunistic approach to mitigate the hidden and exposed node problem in a high-throughput mesh network, by exploiting the frame aggregation and block acknowledgment (BACK) capabilities of IEEE 802.11n/ac wireless networking standard. Hidden nodes significantly drop down the throughput of a wireless mesh network by increasing data loss due to collision, whereas exposed nodes cause under-utilization of the achievable network capacity. The problem becomes worse in IEEE 802.11n/ac supported high-throughput mesh networks, due to the large physical layer frame size and prolonged channel reservation from frame aggregation. The proposed approach uses the standard 'Carrier Sense Multiple Access' (CSMA) technology along with an 'Opportunistic Collision Avoidance' (OCA) method that blocks the communication for hidden nodes and opportunistically allows exposed nodes to communicate with the peers. The performance of the proposed CSMA/OCA mechanism for high throughput mesh networks is studied using the results from an IEEE 802.11n+s wireless mesh networking testbed, and the scalability of the scheme has been analyzed using simulation results.**

***Keywords*-IEEE 802.11n; Frame Aggregation; Hidden and Exposed Nodes; Spatial Reuse**

I. Introduction

Wireless Mesh Networking [1] technology provides a key milestone to the next generation backbone access network, where a 'mesh' of wireless routers supports the backbone connectivity to the end-users through multi-hop communications. To assist commercial, enterprise and community mesh backbone technology, IEEE 802.11s [2] is gaining significant attention among the developers for its compatibility with commercially successful IEEE 802.11 wireless networking standard. The IEEE 802.11s amendment to the wireless networking standard contributes to the medium access control (MAC) specifications for the wireless mesh access, that can operate along with any physical layer technology supported by the IEEE 802.11 task groups. The recent developments over IEEE 802.11 technology enhances wireless communications for high data rate supports, up to 600 Mbps with IEEE 802.11n, and up to 6.77 Gbps with IEEE 802.11ac [3]. Therefore the mesh networking standard along with high data rate support has exorbitant potentials to provide high-throughput backbone network connectivity to the end users, that effectively directs towards the design of 'wireless world' [4].

The IEEE 802.11 coordination function for wireless channel access relies on 'Listen before Talk' which is known as 'Carrier Sense Multiple Access with Collision Avoidance' (CSMA/CA). The clear channel assessment (CCA) in CSMA/CA uses two listen or carrier sensing (CS) mechanism - physical CS (PCS) and virtual CS (VCS). Extensive studies on IEEE 802.11 CCA technologies have revealed that PCS fails to detect nodes which are beyond the CS range (known as hidden nodes), whereas VCS reduces spatial reuse by blocking the communications which are not susceptible to interference (known as exposed nodes) [5]. The performance impacts of hidden and exposed nodes in a network is characterized by the CS range and the interference range. In PCS, a node can initiate a new communication only if all other nodes in its CS range are inactive. However, the communication becomes successful only if the receiver is not within the interference range of any other active nodes in the network. As CCA is performed at the transmitter, whereas the receiver is susceptible to interference, there is a high probability of hidden nodes in a mesh network. VCS [6] is proposed to solve the hidden node problem through a handshaking between the transmitter and the receiver before the actual communication takes place, through a pair of messages termed as 'Request to Send' (RTS) and 'Clear to Send' (CTS). The transmitter sends a RTS message only if the CCA reports no active nodes in the CS range of the transmitter. The receiver replies back with a CTS message only if there are no active nodes within the CS range of the receiver. On overhearing the RTS and the CTS messages, other nodes within the CS range of transmitter and receiver block their communication for the time duration mentioned within the RTS and the CTS messages. As a consequence, VCS introduces the problem of exposed nodes which are outside the receiver's interference range, but within the CS range of the transmitter. Though the exposed nodes are harmless for an ongoing communication, they are blocked as a result of VCS and therefore cause under-utilization of the effective network capacity.

The performance issues experienced by hidden and exposed nodes in a multi-hop and mesh network have been well studied in the literature. Most of the existing approaches design mechanisms to eliminate either the hidden nodes or the exposed nodes, such as busy tone signaling [7], use of separate control channels [8], adaptation in CS threshold and temporary disabling the CS mechanism [9] etc. However, none of these approaches can eliminate hidden and exposed nodes simultaneously. In fact, existing research [9] has shown that it

Sandip Chakraborty is with the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, Kharagpur 721302, INDIA (e-mail: sandipc@cse.iitkgp.ernet.in)

Sukumar Nandi and Subhrendu Chattopadhyay are with the Department Computer Science and Engineering, Indian Institute of Technology Guwahati, Guwahati 781039. INDIA (e-mail: {sukumar,subhrendu}@iitg.ernet.in)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2480398, IEEE Transactions on Wireless Communications

is very difficult to eliminate hidden and exposed nodes simultaneously, as these are two complementary problems. Further in general for a network with low to moderate traffic load, VCS may show negative impact (considerably less performance than PCS) because of RTS-CTS signaling overhead and large number of exposed nodes [10]. As a consequence, researchers have developed adaptive PCS mechanisms [11] where the CS range is dynamically tuned to reduce the number of hidden nodes in a network. In adaptive PCS, transmit power is tuned in such a way so that the CS range becomes almost equal to the interference range. In this way, the hidden nodes which are within the interference range, but outside the CS range of the transmitter, can be eliminated. Nevertheless, these mechanisms of dynamic CS range can not eliminate the hidden nodes which are within the CS range (or the interference range, assuming both are tuned to be same) of the receiver, but outside the CS range of the transmitter. In [12], the authors have proposed an access point (AP) cooperation method, where the APs share some common information among themselves to detect the hidden and exposed nodes. However, their scheme requires synchronization among the APs which is hard to achieve in a mesh network.

Our earlier paper [13] presents a theoretical model for the performance of IEEE 802.11n supported mesh networks in the presence of hidden and exposed terminals. The high throughput wireless networking technologies over IEEE 802.11n/ac support MAC layer frame aggregation and block acknowledgment (BACK) strategies to improve channel access performance by minimizing the MAC layer overhead [3]. The analysis reveals that the MAC layer frame aggregation and BACK are more susceptible to performance losses in the presence of hidden and exposed terminals. IEEE 802.11n supports a frame aggregation limit of 64 KB. Further in IEEE 802.11n/ac, high data rate support is obtained at the cost of higher and collocated channel losses during interference [14] due to channel bonding [1]. Though individual MAC protocol data units (MPDU) in an aggregated frame (called A-MPDU) can be recovered from random losses, a collocated loss due to collision from hidden terminals destroys a consecutive numbers of MPDUs. Further a BACK loss due to collision from hidden terminals may result in as large as 64 KB data loss, as the complete A-MPDU is required to be retransferred for a BACK loss. Similarly in VCS, a single exposed node unnecessary defers its transmission for a long time. For example with 1500 bytes MAC frame size and 32 Mbps data rate with IEEE 802.11g, the exposed node has to wait for approximately 0.04 ms, whereas with 64 KB MAC aggregated frame size and 600 Mbps data rate with IEEE 802.11n, an exposed node has to wait for approximately 0.1 ms, 2.5 times more. Possibility of an exposed nodes in a mesh network with VCS is very high. As shown in [13], reducing hidden nodes through a tunable CS threshold only is not sufficient to have a reasonable performance benefit in high throughput mesh networks, whereas pure VCS may show negative impact if number of exposed nodes crosses a limit. Considering the extortionate data loss due to hidden nodes in a high throughput mesh network with PCS, and possibility of capacity under-utilization due to exposed nodes in VCS, a scheme should be designed that reduces hidden nodes as much as possible, whereas allows communication opportunities to the exposed nodes.

This paper shows the effect of hidden and exposed terminals over the performance of high throughput mesh networks, using results from a testbed. An improved channel access mechanism is designed in this paper on the top of VCS, utilizing the frame aggregation and BACK strategies in high throughput wireless standards. The proposed mechanism, called CSMA with Opportunistic CA (CSMA/OCA) characterizes the exposed nodes based on their collision properties, and classifies them in transmitter side exposed (T-Exposed, the nodes within the CS range of the transmitter) and receiver side exposed (R-Exposed, the nodes within the CS range of the receiver) nodes. The CSMA mechanism is augmented to allow transmission from the T-exposed nodes which are outside the CS range of the receiver, and the R-exposed nodes which are outside the CS range of the transmitter. This augmentation in CSMA mechanism allows communication for the exposed nodes those do not result in a collision during MPDU communication. However, collision is still possible between MPDUs from one node, and control frames (BACK, RTS or CTS) from another. An opportunistic collision avoidance (OCA) mechanism is proposed in this paper, where the transmit power levels of control frames are determined in an adaptive and coordinated way, such that data-control collision and control packet loss can be avoided as much as possible. The performance of the proposed scheme is analyzed through the results obtained from a practical IEEE 802.11n mesh networking testbed. The scalability of the proposed scheme has been analyzed using simulation results.

II. Effect of Hidden and Exposed Nodes in a High Speed Mesh Network: PCS vs VCS

A number of works, such as [10] and the references therein, have shown that VCS may employ negative impact on channel access overhead due to signaling overhead and exposed nodes. Tinnirello *et al* [16] have shown both analytically and by simulation results that the situation may become worse in case of high speed networks, as the assumption of short transmission time for control frames does not hold for high speed networks. In this section, we report a series of results from a practical IEEE 802.11n+s testbed to analyze the impact of PCS and VCS over high speed multi-hop and mesh wireless networks.

A. Experimental Setups

In these experiments, we use IEEE 802.11n supported Ralink (presently MediaTek) RT-3352 router-on-chip [17] as the core of the wireless routers. The RT-3352 router-on-chip combines 802.11n draft compliant $2T2R$ MAC along with BBP/PA/RF MIMO, a high performance 400MHz

[1]In IEEE 802.11n, two 20 MHz channels are combined to obtain a 40 MHz channel, whereas in IEEE 802.11ac, four 20 MHz channels are combined to use a single 80 MHz channel. It is well known, that wider channels are more susceptible to random as well as collocated channel losses from interference [15].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2480398, IEEE Transactions on Wireless Communications

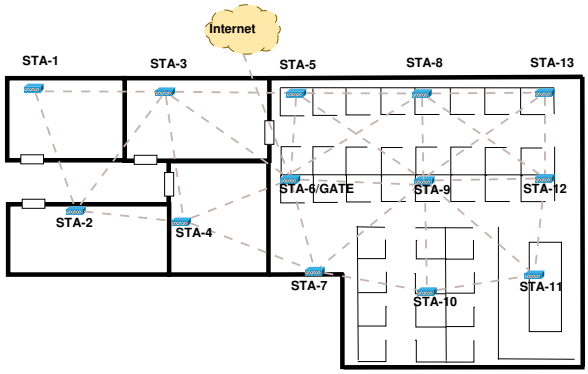


Fig. 1. High Throughput Mesh Testbed and Connectivity Layout

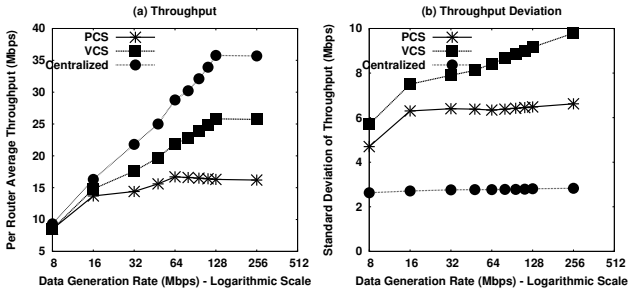


Fig. 2. Comparison among PCS, VCS and Centralized

MIPS24KEc CPU core, a Gigabit Ethernet MAC, 5-ports integrated 10/100 Ethernet Swtich/PHY, 64MB of SDRAM and 32MB of Flash. This chip can support up to 300 Mbps data rate with maximum transmit power of $16dBm$. The routers are configured with Linux kernel version 3.12 with open80211s support [18] which provides open source implementation of IEEE 802.11s mesh networking protocol stack.

B. Experimental Results

Fig. 1 shows the deployment and connectivity layout for a 13 node IEEE 802.11n+s mesh testbed, where 12 nodes act as mesh routers, and one node (STA-6) connects the mesh backbone to the Internet. All 13 nodes are able to act as an access point (AP) to the client nodes to provide backbone mesh connectivity. The dotted lines in the figure shows connectivity among the mesh routers based on the maximum transmit power and receiver sensitivity setup (maximum transmit power 16 dBm, receiver sensitivity -81 dBm). In the testbed, we have used two types of data flows generated through `iperf` tool - the upload traffic flow and the download traffic flow. The upload traffic flows are from mesh routers to the mesh gate (STA-6) and the download traffic flows are from mesh gates (STA-6) to mesh routers. Out of the total traffic flows, 60% data are from download traffic and 40% data are for upload traffic. The performance is evaluated by varying the data generation rate which in turn changes the traffic load of the network. The performance of PCS and VCS is evaluated with a comparison to an centralized scheduling scenario [19] which is generated based on a centralized formulation. The centralized formulation uses a spatial time division multiple access (STDMA) based scheduling, where exposed nodes are allowed to communicate while hidden nodes are blocked explicitly. This scheduling mechanism gives a theoretical upper bound along with protocol overhead, for IEEE 802.11 access scheduling. Therefore, we consider this scheme as the benchmark for performance comparison in this paper, and show how close our proposed distributed scheme can perform compared to the centralized solution. During the design of the centralized scheduling, we have assumed interference range equals to the CS range, as interference beyond the CS range (such as, additive interference) is difficult to design in a decentralized system [20]. In the testbed evaluation, the A-MPDU aggregation level is considered to be 64 KB. The effect of dynamic rate selection is also evaluated, and the performance data is reported later in this paper.

Fig. 2(a) depicts the channel access strategies for three mechanisms - PCS, VCS and the centralized access [19], with respect to average per router throughput. The x-axis shows the mean data generation rate, where every router generates data based on a log-normal distribution along the mean with standard deviation as 2 Mbps. The data generation rate does not include the forwarding traffic. Fig. 2(b) compares the three mechanisms with respect to the standard deviation of routers' throughput. While the average throughput shows the network performance, the standard deviation of throughput indicates effect of hidden and exposed terminals over the throughput performance. As all the nodes transmit traffic towards STA-6, the effect of hidden and exposed terminals is less for the nodes which are in one-hop away from STA-6. Fig. 2(a) shows that throughput loss becomes substantial at high traffic load, when the data generation rate is more than 10 Mbps. Though VCS improves performance at high traffic load by reducing hidden terminals, the throughput is still significantly less compared to the centralized scenario. At the same time, Fig. 2(b) indicates that the throughput deviation is very high for PCS and VCS at high traffic load. From extensive analysis of router traces, we have found that packet loss in PCS is very high for the nodes which experience hidden terminals. However, throughput variation for VCS is higher than PCS, that indicates severe network under-utilization at the presence of exposed nodes. In a high speed mesh network with high traffic load, a single exposed node at every transmission opportunity[2] may lead to network under-utilization equivalent to 64 KB data transmission. As a consequence, the throughput deviation inflates at high traffic load.

The above results indicate that IEEE 802.11 PCS and VCS fail to achieve even half of the centralized throughput in a high data rate wireless mesh network. Therefore, the standard CS mechanisms are required to be revisited for implementing high throughput mesh networks based on IEEE 802.11 standard. The target is to block hidden nodes to avoid data losses due to collision, and to allow transmissions to the exposed nodes for effective utilization of available network capacity. However, enabling communication to all the exposed nodes may create additional problems in a mesh network, as discussed in the

[2]A transmission opportunity indicates the time required to transmit an A-MPDU once a node gains access to the channel

next section.

III. Exposed Nodes: Spatial Transmission and Data-Control Collisions

Modern hardware supports with dynamic power adaptation and capture enabled devices [21] can reduce interference from hidden nodes by tuning CS range to make it equivalent to the interference range, although cannot eliminate them completely. Whereas receiver coordination similar to VCS is necessary to detect the nodes which are outside the CS range of the transmitter, however within the CS range (or interference range) of the receiver. In this design, we consider a network, where CS range is tuned to make it equal to the interference range through some existing mechanism similar to [22], and our target is to further reduce the hidden nodes which are beyond the scope of detection through tuning the CS range, while allowing communication to the exposed nodes as much as possible. The proposed CSMA/OCA protocol works on the top of VCS to improve the performance of high throughput mesh networks by reducing number of hidden nodes and opportunistically allowing communication to the exposed nodes.

As a protocol level simplification, CSMA/OCA considers only the nodes which are within the CS range, and are detectable through either PCS or VCS. The proposed protocol overlooks interference from outside the CS range (additive interference) which is not pre-detectable through PCS or VCS and difficult to capture in a real-time environment. For this purpose, this paper differentiates the term 'collision' and 'interference' as follows: collision is considered for the nodes which are within the CS range and are detectable, whereas interference is considered for the nodes which are outside the CS range, but results in data loss due to additive interference.

During PCS, the nodes which are within the CS (or interference) range of the receiver, but are outside the CS range of the transmitter can be a potential hidden node, as any transmission from it remains undetectable to the transmitter though it causes collision at the receiver. The VCS solves this problem by blocking all the nodes which are within the CS range of both the transmitter and the receiver. As a consequence exposed nodes may result network under-utilization as follows:

1) The nodes which are within the CS range of a transmitter, say T_1, but are outside the CS (or interference) range of a receiver, get blocked by overhearing the RTS message from T_1. These nodes can be a potential transmitter for some other nodes in the network, as they are not within the interference range of a receiver. These nodes are termed as *T-Exposed* nodes.
2) The nodes which are within the CS (or interference) range of the receiver, say R_1, however are outside the CS range of a transmitter, get blocked by overhearing the CTS message from R_1. Though these nodes can not be a transmitter, nevertheless they can be a potential receiver for some other nodes outside the CS range of R_1. These nodes are termed as *R-Exposed* nodes.

Fig. 3-Case 1 shows transmission and collision scenarios for T-Exposed nodes. The dark and light circles denote the transmission range and the CS range respectively. $C \rightarrow D$ communication is feasible as the data communications do not overlap at the receiver, and therefore collision does not exist. However, VCS blocks such communication resulting in node C to be an T-Exposed node. Although, allowing communication to such node may result in data-control collision, as shown in Fig. 3-Case 1(b). The BACK from node B may collide with the data from node C. Similar situation may arise for the CTS from node D. Therefore, special care has to be taken while allowing transmissions to the T-Exposed nodes. Fig. 3-Case 2 shows transmission and collision scenarios for R-Exposed nodes. The communications $A \rightarrow B$ and $C \rightarrow D$ does not result in a collision. However in VCS, node D gets blocked on overhearing the CTS frame from node B. Similar to the earlier scenario, allowing communication to R-Exposed nodes may result in a data-control collision, where one MPDU or two consecutive MPDUs may get lost in an A-MPDU. Based on these collision scenarios, an opportunistic access mechanism is proposed in this paper, as discussed in the next section.

IV. Opportunistic Access: Design and Analysis

The discussions till now have shown that the exposed nodes result in severe under-utilization of spatial reuse in high data rate mesh networks. Though VCS suffers from the signaling overheads, with a little modification in the CTS frame structure, the exposed nodes can be detected within the CS range of the transmitter and the receiver. However, allowing transmissions to all the exposed nodes may result in data-control collision, as shown in Fig. 3. Therefore, an opportunistic access mechanism is introduced in this section to deal with this problem. The opportunistic access mechanism utilizes VCS, where RTS and CTS messages are used for the detection of hidden nodes, as well as allowing transmission to the exposed nodes in an opportunistic way such that data-control collision can be minimized. The OCA mechanism uses an adaptive and coordinated transmit power calculation mechanism, where the control frames are transmitted based on a predefined power level such that data-control collisions can be avoided as much as possible. The detailed design of the opportunistic access mechanism is discussed in the following subsections.

A. Carrier Sensing: Detection of Hidden and Exposed Nodes

The legacy VCS mechanism uses a table, called the *network allocation vector* (NAV), to maintain the transmission blockage on overhearing the RTS and the CTS frames. The RTS and the CTS frames contain a duration field (DU) which indicates the time duration for the channel reservation. On overhearing the RTS and the CTS frames, every node sets its NAV for the time mentioned in the DU field. In the proposed augmentation of VCS, different NAVs are maintained for every overheard RTS and CTS frame, to detect the exposed nodes and to avoid the data-control collision. Let, RTS_{act} and CTS_{act} denote the sets of nodes from which a node has received the RTS or CTS frames, respectively, and $\mathcal{F}.DST$ denote the destination address associated with the frame $\mathcal{F}$. Further assume that $\mathcal{N}_i$ denotes the set of nodes which are in the CS range of node

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2480398, IEEE Transactions on Wireless Communications

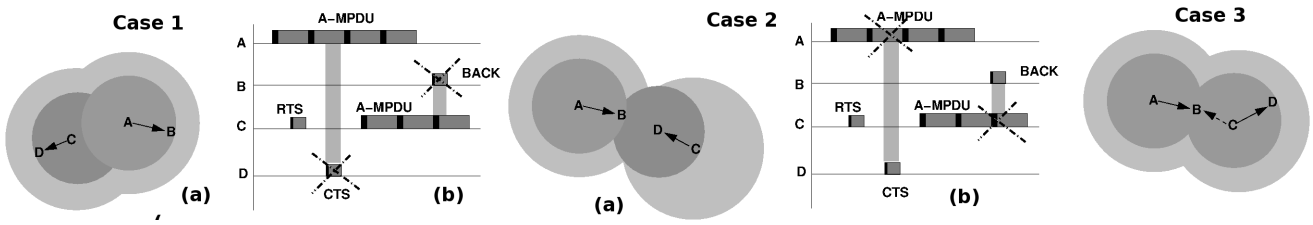


Fig. 3. **Case 1:** Spatial Transmissions and Collision Scenario for T-Exposed Nodes, **Case 2:** Spatial Transmissions and Collision Scenario for R-Exposed Nodes, **Case 3:** Hidden Node Scenario

Algorithm 1 Node S wants to transmit data to node R

1: **if** $(CTS_{act} = NULL) \wedge (\forall RTS_{act}.DST \notin \mathcal{N}_S)$ **then**
2: Calculate η_S.
3: Send <RTS,$\eta_S >$ using P_{max}; /*T-exposed nodes*/
4: **else**
5: Back-Off and retry;
6: **end if**

Algorithm 2 Node R receives RTS from node S

1: **if** $(RTS_{act} = NULL) \wedge (\forall CTS_{act}.DST \notin \mathcal{N}_R)$ **then**
2: Calculate $P_{Tx}^{(R)}, \eta_R$;
3: **if** $P_{Tx}^{(R)} \in \mathcal{P}$ **then**
4: Send $< CTS, \eta_R >$ using $P_{Tx}^{(R)}$; /*R-exposed nodes*/
5: **end if**
6: **end if**
7: $RTS_{act} \leftarrow this.RTS$ /*Append the received RTS in RTS_{act}*/

Algorithm 3 Node S receives CTS from node R

1: **if** $(CTS_{act} = NULL) \wedge (\forall RTS_{act}.DST \notin \mathcal{N}_S)$ **then**
2: Calculate $P_{Tx}^{(S)}$.
3: Send DATA using $P_{Tx}^{(S)}$;
4: **else**
5: Back-Off and retry;
6: **end if**
7: $CTS_{act} \leftarrow this.CTS$ /*Append the received CTS in CTS_{act}*/

i. This set can be populated using the standard IEEE 802.11 beaconing procedure.

We also include an additional 1 byte field, called background noise level (denoted as η_i for node i), at every control frame header. The background noise level indicates the total incident power on the receiver, before the communication starts. The background noise level is measured in terms of received signal strength, expressed in dBm, before transmitting a control packet. Assume that node B is an intended receiver. Therefore following the VCS mechanism, node B needs to transmit a CTS packet after it receives a RTS successfully. The received signal strength at node B is the indication of channel noise near the receiver. This information is propagated to the transmitter, in the form of background noise level, so that it can adjust its power level accordingly. This background noise level value is used for OCA along with the VCS mechanism, as discussed in the subsequent subsection.

The decision controls for hidden and exposed node detection are explained through Algorithm 1, Algorithm 2 and Algorithm 3. According to these algorithms, every data and control frames are transmitted using a predefined power level. The actual power level to transmit the data and control frames are calculated based on the OCA mechanism, as discussed later. In these algorithms, $P_{Tx}^{(i)}$ denotes the transmit power for the data or control packet to be transmitted, and P_{max} denotes the maximum available power level. $\mathcal{P}$ denotes the set of available power levels according to the physical layer modulation and coding technology.

The control statements in these algorithms define whether a node should initiate a communication based on the VCS mechanism. As mentioned earlier, whenever a node overhears a RTS or CTS control packet, it appends or updates the RTS_{act} and CTS_{act} sets accordingly. The lifetime of an entry in these sets is equal to the duration field mentioned in the corresponding RTS or CTS control packets, that denotes how much time a channel is going to be reserved by the corresponding node. Furthermore, it can be noted that a RTS transmission does not always indicate a data communication. It may happen that the sender fails to receive the CTS packet from the intended receiver due to a busy channel or interference. Therefore, after an entry is appended or updated in the RTS_{act} set, a node senses the channel after a timeout interval[3]. If the channel is found to be idle, the corresponding entry from RTS_{act} is deleted. These three algorithms can correctly identify the hidden nodes as well as both types of exposed nodes, as described in the following subsections.

1) Detection of Hidden Nodes: The hidden node scenario can occur for two cases - (i) a transmitter node is within the CS range of another receiver node, and (ii) a receiver node is within the CS range of another transmitter node. For the first scenario, considering Fig. 3-Case 3, let $A \rightarrow B$ communication starts first. Therefore, node C can overhear the CTS frame from node B, which is included in the CTS_{act} set. According to Algorithm 1, the condition is evaluated to be false, as $CTS_{act} \neq NULL$, and node C starts the back-off without initiating the communication.

For the second scenario, let us assume that $C \rightarrow D$ communication starts first. Node B is outside the CS range of node D, but within the CS range of node C. In this scenario node B acts as a receiver, and therefore, should not initiate a communication. Node B can overhear the RTS from node C, and includes it in the RTS_{act} set. On receiving the RTS frame from node A, node B executes Algorithm 2. However, the condition is evaluated to be false as $RTS_{act} \neq NULL$.

[3]In our implementation, this timeout is kept equal to the duration of $3 \times SIFS + T_{CTS}$, where SIFS is the short inter-frame space duration and T_{CTS} is the duration of a CTS frame in time unit (TU).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2480398, IEEE Transactions on Wireless Communications

Therefore it does not replies back with the CTS, and the communication is deferred avoiding possible collision due to hidden terminals.

2) Spatial Reuse by T-exposed Nodes: Considering Fig. 3-Case 1, let $A \rightarrow B$ communication starts first. Node C within the CS range of node A wants to initiate a transmission with node D, which is outside the CS range of node A. As node C is outside the CS range of node B, it does not receive any CTS. Further, $RTS_A.DST \neq C$. Therefore, the condition in Algorithm 1 is evaluated to be true, and node C forwards the RTS to node D. Node D is outside the CS range of both the nodes A and B. Therefore, the condition of Algorithm 2 is also evaluated to be true, and D replies back with the CTS, resulting in a communication initialization at node C following Algorithm 3.

3) Spatial Reuse by R-exposed Nodes: Considering Fig. 3-Case 2, let $A \rightarrow B$ communication starts first. As node D is outside the CS range of node A, it does not overhear the RTS. Therefore $RTS_{act} = NULL$. Assume, node D receives an RTS from node C. As node D is within the CS range of node B, it overhears the CTS from node B. However, $CTS_B.DST = A \notin \mathcal{N}_D$. Therefore following Algorithm 2, node D replies back with the CTS, resulting in the communication initialization at node C, as shown in Algorithm 3.

B. Opportunistic Collision Avoidance

As discussed earlier, allowing communications to the exposed nodes may result in data-control collision. The T-exposed nodes may result in control frame loss, whereas, the R-exposed nodes may affect data frames. To avoid such losses, we employ the dynamic power adaptation feature available with the commodity wireless routers. The modern commodity router hardwares support a set of transmit power levels for every physical modulation and coding schemes, that can be tuned by the MAC layer driver module. A higher transmit power improves the possibility of correct reception and decoding of a frame, however increases the interference range due to that communication. A frame can be received and decoded correctly if the received signal to interference and noise ratio (SINR) for that frame is beyond a certain threshold, called the *capture threshold*. For a communication $S \rightarrow R$ between two nodes S and R, this can be expressed as;

$$SINR_R = \frac{P_{tx}^{(S)} G_{SR}}{\eta_R} \geq \mathcal{S}_{thresh} \tag{1}$$

where $\mathcal{S}_{thresh}$ is the capture threshold required to correctly decode the frame, $P_{tx}^{(S)}$ is the transmit power level at node S, G_{SR} is the channel gain between S and R. As mentioned earlier, η_R is the background noise level at the receiver R, that denotes total power at the channel just before node R receives the data frame from S. This implies the total noise power contributed by all other communications except $S \rightarrow R$, near the node R. This noise power interferes with the $S \rightarrow R$ communication.

The OCA mechanism proposed in this paper dynamically adjusts the power level for the frames which may undergo a collision. Otherwise the frames are transmitted using the minimum power level such that the communication can sustain. Overall, the OCA mechanism works as follows:

- CTS and BACK control frames may get lost due to probable collision from a T-Exposed node, as shown in Fig. 3-Case 1. Therefore these control frames are transmitted using a higher power level, whenever the background noise level calculated near the sender is high enough. This power level is decided based on the sender side background noise level information (η) transmitted through the RTS and data frames. If the calculated power level is higher than the available power levels, then the communication is not initiated.
- Data frames may get lost due to probable collision from a R-exposed node, as shown in Fig. 3-Case 2. However, in this scenario, the sender side background noise level is very low, and therefore CTS and BACK control frames are transmitted using the minimum power level such that the communication can sustain. As a consequence, the possibility of data loss due to R-exposed nodes can be reduced.
- The RTS frames are transmitted using maximum available power level (P_{max}), since the maximum power level gives maximum possibility of receiving a frame correctly. The RTS frames are required to be received correctly for further coordination in the OCA mechanism.

The adjustment of the transmit power level for a CTS frame works as follows. Let, node S want to communicate to node R, and accordingly transmit the RTS frame with maximum power level P_{max}. The RTS frame also contains the parameter η_S, the background noise level at node S measured just before transmitting the RTS frame. On reception of the RTS frame, let the device driver of node R reports measured SINR as $SINR_{RTS}$. Then,

$$SINR_{RTS} = \frac{P_{max} G_{SR}}{\eta_R} \tag{2}$$

where η_R is the background noise level at node R measured before the reception of the RTS frame. It can be noted that the device driver of every node i periodically measures the background noise level and stores the value in the variable η_i. The background noise level is also used in the standard PCS and VCS mechanism to check whether the channel is free [23], [16]. For instance, the channel is assumed to be free if η_i is less than the CS threshold.

From Equation (2), node R can calculate the value of the channel gain G_{SR}. Now, let $P_{tx}^{(R)}$ denote the transmit power level of node R, for forwarding the CTS frame to node S. For correct reception and decoding of the CTS frame at node S, Equation (1) needs to be satisfied. Therefore,

$$\frac{P_{tx}^{(R)}\, G_{RS}}{\eta_S} \geq \mathcal{S}_{thresh} \tag{3}$$

Thus,

$$P_{tx}^{(R)} \geq \frac{\mathcal{S}_{thresh}\, \eta_S}{G_{RS}} \tag{4}$$

Since the communication interfaces for all the nodes are assumed to be homogeneous and the VCS mechanism has

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2480398, IEEE Transactions on Wireless Communications

already blocked the communications from the hidden nodes resulting in no hidden node interference, we can assume $G_{RS} \approx G_{SR}$. So,

$$P_{tx}^{(R)} \geq \frac{\mathcal{S}_{thresh}\ \eta_S\ P_{max}}{SINR_{RTS}\ \eta_R} \tag{5}$$

The CTS frames are transmitted only if $P_{tx}^{(R)} \leq P_{max}$. Otherwise, the communication is not initiated. As discussed earlier, a commodity wireless router supports a set of discrete power levels $\mathcal{P}$. Therefore, $P_{tx}^{(R)}$ is approximated to the next available power level from $\mathcal{P}$, higher than $P_{tx}^{(R)}$.

The transmit power levels for the BACK and data frames are calculated in a similar way. The power adaptation method opportunistically handles both the T-Exposed and R-Exposed nodes. For T-Exposed nodes, η_S becomes high. Therefore CTS and BACK frames are transmitted at a higher power level such that the control frames can be received and decoded correctly. For R-Exposed nodes, η_S is very low. Therefore, CTS and BACK frames are transmitted at lower power levels, reducing the possibility of collision with the data frames from the R-Exposed node.

1) Implementation Issue 1 (Measurement of Background Noise Level and SINR): The proposed OCA scheme relies on the measurement of background noise level and the calculated SINR value. In this work, we use an active measurement technique [24], [25] for measuring the received signal strength before the data communication, which is expressed in terms of background noise level. The MadWiFi like device drivers use a hardware abstraction layer (HAL) that measures the difference between the signal level and the noise level for each packet [26]. This measured value is used as the SINR value in our proposed scheme. Further, the noise level of the channel is measured in each interrupt, after reception of a sequence of packets. In our scheme, the latest channel noise reported by the HAL is used as the value of background noise level, expressed in terms of dBm.

However, it can be noted that both the SINR and the channel noise level fluctuates irregularly. To avoid sudden peaks of SINR and background noise level fluctuations, we use an exponentially weighted moving average (EWMA) mechanism to smooth down the reported SINR and background noise level values. Let $\mathcal{S}_{curr}$ is the reported SINR value by the HAL on receiving a packet, and $\mathcal{S}_{sm}$ is the smoothed average value. $\mathcal{D}_{sm}$ is the deviation in estimated SINR. We use the following iterative equations to estimate the smoothed value of SINR.

$$\mathcal{S}_{sm} = (1-\rho)\mathcal{S}_{curr} + \rho\mathcal{S}_{sm} \tag{6}$$

$$\mathcal{D}_{sm} = (1-\rho)|\mathcal{S}_{sm} - \mathcal{S}_{curr}| + \rho\mathcal{D}_{sm} \tag{7}$$

$$\mathcal{S}_{sm} = \mathcal{S}_{sm} - \mu\mathcal{D}_{sm} \tag{8}$$

Here ρ and μ are design parameters, and chosen to give the effect of previous measurement over the current measurement. In OCA, we use $\rho = 0.1$ and $\mu = 1$. These values are chosen based on experimental experiences that gives good smoothing by avoiding the sudden SINR peaks due irregular fluctuations. The calculated background noise level is also smoothed in a similar way with the smoothing parameters chosen as $\rho = 0.2$ and $\mu = 0.8$.

2) Implementation Issue 2 (Adaptive Modulation and Coding in IEEE 802.11): IEEE 802.11 supports adaptive modulation and coding (AMC) where every node has the flexibility to select the modulation and coding scheme (MCS) based on the channel quality and several other performance factors. The physical data rate and the transmit power depends on the selected MCS level. Therefore in a scheme where dynamic power selection is used to mitigate interference, AMC needs to collaborate with the transmit power selection mechanism to choose the appropriate MCS. It can be noted that for the control frames, the AMC always selects the MCS that provides the lowest data rate, because the lowest data rate sustain for maximum channel noise. Therefore, in the proposed scheme, the transmit power for the control frames is selected from the available power levels supported by the MCS corresponding to the lowest data rate.

The problem is non-trivial for the data frames. Equation (5) gives the minimum transmit power level required for successful decoding of the signal at the receiver. In the implementation of CSMA/OCA, once the minimum transmit power level is decided for a communication session, the AMC selects the MCS level that supports transmit power level greater than $P_{tx}^{(R)}$. The proposed CSMA/OCA and AMC works together as follows:

1) CSMA/OCA selects $P_{tx}^{(R)}$ according to equation (5).
2) AMC considers the MCS levels that support transmit power levels greater than or equals to $P_{tx}^{(R)}$. From this reduced set of supported MCS levels, the best MCS is chosen following the AMC algorithms. Let the selected MCS level be $\mathcal{M}$.
3) $\mathcal{M}$ supports a set of transmit power levels. Let it be $\mathcal{P}_{\mathcal{M}}$. CSMA/OCA selects the minimum power level from $\mathcal{P}_{\mathcal{M}}$ which is greater than or equals to $P_{tx}^{(R)}$.

Following this procedure, the proposed CSMA/OCA works together with the standard AMC procedure of IEEE 802.11.

V. Performance Evaluation of CSMA/OCA

The 13 node IEEE 802.11n+s high data rate mesh networking testbed, as shown in Fig. 1 is used to evaluated the performance of the proposed scheme and compare the results with the standard PCS, VCS as well as with the centralized solution as discussed earlier [19]. The performance is also compared with an adaptive PCS mechanism proposed by Park *et al* [27] and the AP coordination mechanism proposed by Nishide *et al* [12]. In [27], the authors have proposed a distributed carrier sense update algorithm (DCUA), that adaptively tunes the transmit power and carrier sense threshold of every node based on a pricing function calculated using the packet error rate. On the contrary, the AP coordination mechanism [12] detects hidden and exposed nodes based on the frame collision probability received through data and control packets.

The proposed CSMA/OCA is implemented as a loadable kernel module (LKM) in the IEEE 802.11s protocol stack for MAC layer channel access. In the implementation, CSMA/OCA is interfaced with the AMC (Minstrel protocol - default AMC for Linux kernel) and the HAL to handle the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2480398, IEEE Transactions on Wireless Communications

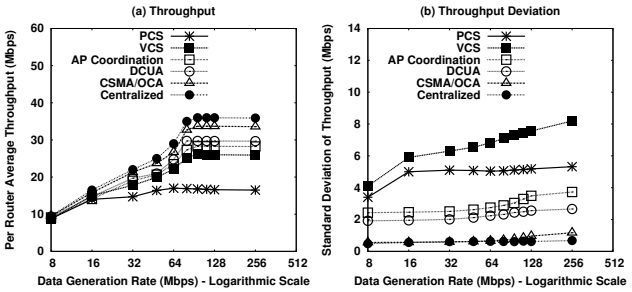


Fig. 4. For Different Channel Access Strategies (a) Throughput, (b) Throughput Deviation

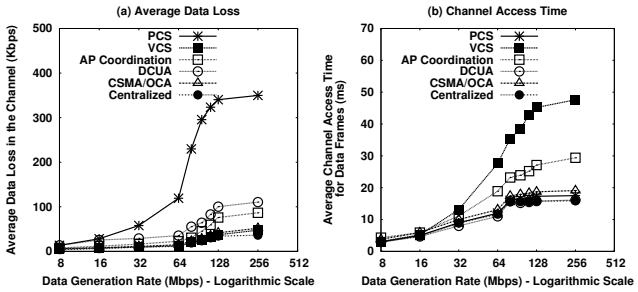


Fig. 5. For Different Channel Access Strategies (a) Channel Data Loss, (b) Average Channel Access Delay for Data Frames

issues related to dynamic MCS selection and calculation of SINR along with background noise level. The system setup is kept similar as discussed in Subsection II-A. The AMC uses the IEEE 802.11n supported MCS levels along with the supported transmit power levels and receiver sensitivity as directed by the RT-3352 hardware [17]. For instance, for MCS $0-8$ and with two different channel widths 20 MHz and 40 MHz, the available transmit powers are $\{3, 5, 8, 11, 14\}$ dBm and $\{5, 8, 11, 14, 16\}$ dBm, respectively.

Fig. 4(a) depicts different channel access protocols with respect to the average per user throughput. The average per user throughput is calculated as the average data transmitted successfully per second. Every mesh router uses A-MPDU aggregation level set to 64 Kbytes. The figure indicates that the network gets saturated (obtains maximum throughput) for PCS when the traffic load is more than 48 Mbps. After the saturation point, the throughput decreases slowly due to increased contention in the network. On the contrary, VCS and other channel access protocols get saturated near 80 Mbps traffic generation rate. The DCUA and AP coordination mechanisms improve average per router throughput compared to the PCS and VCS mechanisms, though the saturation throughput for these schemes are significantly less compared to the centralized strategy. The proposed CSMA/OCA mechanism attains maximum saturation throughput among all the schemes except the centralized strategy, and the performance is close to the centralized strategy. As indicated earlier, the centralized strategy is not implementation-feasible in a wireless mesh network. Being a decentralized scheme, the CSMA/OCA protocol can be easily implemented with marginal modifications in the existing mac80211 module, whereas the network can attain a performance benefit which is comparable with the centralized strategy.

Fig. 4(b) depicts throughput deviation among all the channel access strategies with respect to the traffic load in the network. As indicated earlier, throughput deviation is maximum for PCS and VCS, since hidden and exposed terminals increase unfairness in the network [9]. In presence of hidden and exposed terminals, performances of some nodes are affected by repeated channel access back-off which increases throughput deviation in the network. AP coordination and DCUA reduces this unfairness by eliminating a considerable number of hidden and exposed terminals. However, both of these mechanisms fail to reduce hidden and exposed terminals uniformly in the network. For instance, DCUA can eliminate only the hidden nodes which are within the maximum CS threshold. Similarly, AP coordination can detect only those hidden and exposed nodes which are within the CS range of the neighboring APs. Further AP coordination significantly elevates the control overhead in the network. The proposed CSMA/OCA can eliminate most of the hidden and exposed terminals with less control overhead.

Fig. 5(a) and Fig. 5(b) show the channel data loss and average channel access delay, respectively, for different channel access strategies. The channel data loss indicates the amount of data which are transmitted by a sender, however lost in the channel (acknowledgement is not received) and subsequently retransmitted by the sender. The channel data loss can result from two reasons - collision from the hidden terminals and data loss due to external and additive interference. As the CS range is tuned to make it equal to the interference range through the use of a high carrier sensing threshold value, data loss due to interference is almost negligible. Therefore, Fig. 5(a) indicates the effect of hidden terminals on the performance of the access strategies. On the other side, channel access delay is calculated as the time difference between the time when a MAC data frame is scheduled for transmission (it is at the head of the interface queue), and the time when it is actually transmitted. Therefore, Fig. 5(b) indicates the effect of exposed terminals over the performance. These two figures show that while channel data loss is maximum and grows exponentially for PCS, VCS results in maximum channel access time. AP coordination also has high channel access time, as the coordination requires significant amount of time. It can be noted that the time for control packet exchanges are included within the channel access time. The proposed CSMA/OCA mechanism reduces both the channel data loss as well as average channel access time, resulting in high throughput performance of the network.

Finally we evaluate the effect of A-MPDU aggregation level over the throughput attained through different channel access strategies, as shown in Fig. 6(a) and Fig. 6(b). The mean data generation rate for this experiment is considered to be 64 Mbps (that is just near the saturation level) for Fig. 6(a), and 32 Mbps (the network is unsaturated) for Fig. 6(b). In both the cases, the data generation varies along the mean data generation rate following a log-normal distribution with variance 16 Mbps. The performance of the centralized strategy

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2480398, IEEE Transactions on Wireless Communications

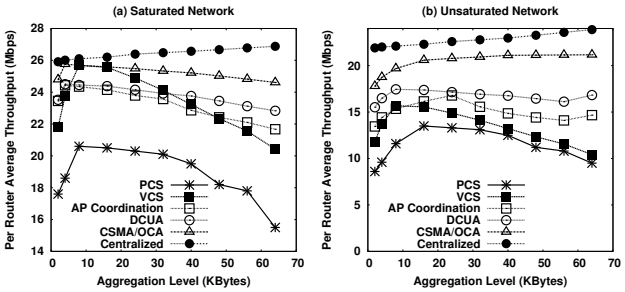


Fig. 6. Effect of A-MPDU Aggregation Level over Per Router Throughput (a) Saturated Network, (b) Unsaturated Network

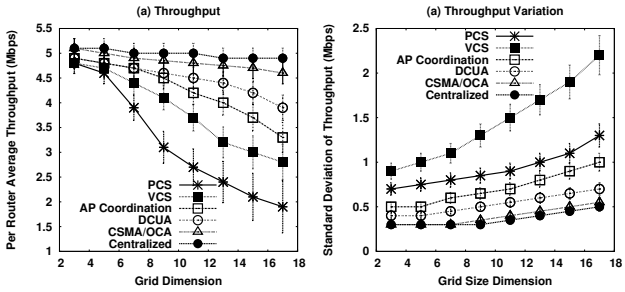


Fig. 7. Simulation Results for Different Channel Access Strategies (a) Throughput, (b) Throughput Deviation

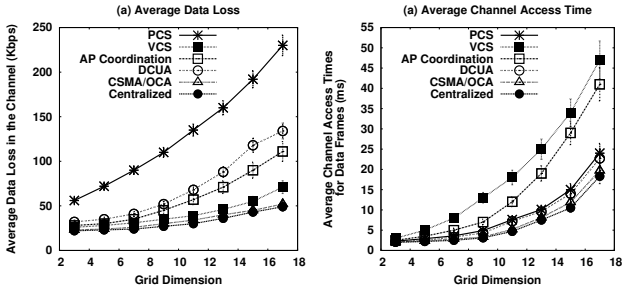


Fig. 8. Simulation Results for For Different Channel Access Strategies (a) Channel Data Loss, (b) Average Channel Access Delay for Data Frames

slowly increases with the increase in data aggregation level, as data aggregation level reduces the physical and MAC control overhead. The performance improvement with respect to the data aggregation level is more prominent in case of a unsaturated network, as shown in Fig. 6(b). With the increase in A-MPDU frame aggregation level, the performance of PCS and VCS first increases, and then drops linearly, and attain a very low throughput compared to the centralized strategy. The performance for PCS and VCS drops after a threshold aggregation level, as the data loss due to collision overshoots the effect of physical and MAC control overheads. With the increase in A-MPDU payload size, the loss due to collision also increases, as discussed earlier. Further VCS shows better performance at low aggregation level compared to AP coordination and DCUA, since AP coordination has significant control overhead, and DCUA can not eliminate hidden terminals completely. The proposed CSMA/OCA scheme performs similar to VCS when aggregation level is low, however, improves the network performance compared to VCS, as well as other schemes, as aggregation level increases. Further, the proposed scheme shows a consistent performance with the increase in the A-MPDU frame aggregation level. These experiments show that the proposed CSMA/OCA results in notable performance improvements in a high throughput wireless mesh network with minimum modifications to the standard mac80211 kernel module at the network protocol stack.

VI. Simulation Results

Although the testbed results give the performance boost for the proposed CSMA/OCA protocol, the experiments are limited with the number of nodes in the testbed. To analyze the scalability of the system, we have simulated the proposed CSMA/CA protocol in Qualnet-5.0.1 network simulator, and compared the results with other related schemes. In Qualnet-5.0.1, we have taken grid topologies of different sizes, with number of nodes in the grid varying from 9 (grid 3×3) to 289 (grid 17×17). Every intermediate node in the grid has 4 neighbors without any cross edges. The mesh gate is placed at the center of the grid. Similar to the testbed scenario, every mesh router has both upload and download traffic. The upload and download traffic are generated using Poisson distribution with the mean and variance as 3 Mbps and 2 Mbps respectively. This indicates a wide variation in traffic distribution across the network. We have executed 10 different scenarios with such random generated traffic model, and plotted the average and standard deviation (90% of the confidence interval) of the results in the graphs. The AMC and power setup for different data rates are kept similar to the testbed setup.

Fig. 7 shows the simulation results for throughput and throughput deviation comparison among different access strategies. In the grasp, grid dimension of n means a grid size of $n \times n$. Following the trend shown by the testbed results as discussed earlier, the simulation results also depict that the proposed CSMA/OCA scheme performs better than others. CSMA/OCA shows a consistent throughput with the increase in grid size.

Fig. 8 shows the average channel data loss and average channel access time for different access strategies. The figure indicates that the proposed CSMA/OCA is scalable to reduce average data loss similar to VCS and average channel access time similar to PCS. The simulation results reveal that the proposed CSMA/OCA mechanism is scalable and provides good performance benefit even in a large network.

VII. Conclusion

This paper presented the severity of the hidden and exposed terminal problem in case of a high throughput wireless mesh network using practical testbed results. The analysis revealed that the hidden terminals cause severe data loss, whereas the exposed terminals under-utilize the network capacity by reducing spatial reuse opportunities. Based on the IEEE 802.11n frame aggregation and BACK capabilities, this paper proposed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2480398, IEEE Transactions on Wireless Communications

an opportunistic access protocol over the VCS paradigm to defend the hidden and exposed terminal problems. The effectiveness of the proposed scheme is analyzed through the results from a practical high speed indoor mesh testbed as well as from simulation.

REFERENCES

[1] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Communications Magazine*, vol. 43, no. 9, pp. S23–S30, 2005.

[2] G. R. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, and B. Walke, "IEEE 802.11s: the WLAN mesh standard," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 104–111, 2010.

[3] E. Perahia and M. X. Gong, "Gigabit wireless LANs: An overview of IEEE 802.11ac and 802.11ad," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 15, no. 3, pp. 23–33, Nov. 2011.

[4] B. Brown and N. Green, Eds., *Wireless World: Social and Interactional Aspects of the Mobile Age*. New York, NY, USA: Springer-Verlag New York, Inc., 2002.

[5] A. Tsertou and D. I. Laurenson, "Insights into the hidden node problem," in *proceedings of the 2006 IWCMC*, 2006, pp. 767–772.

[6] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, "MACAW: a media access protocol for wireless LAN's," *SIGCOMM Comput. Commun. Rev.*, vol. 24, no. 4, pp. 212–225, Oct. 1994.

[7] J. Monks, V. Bharghaban, and W. M. Hwu, "A power controlled multiple access protocol for wireless packet networks," in *proceedings of IEEE INFOCOM*, May 2007, pp. 219–228.

[8] A. Muqattash and M. Krunz, "Power controlled dual channel (PCDC) medium access protocol for wireless ad hoc networks," in *proceedings of IEEE INFOCOM*, vol. 1, March 2003, pp. 470–480.

[9] L. B. Jiang and S.-C. Liew, "Improving throughput and fairness by reducing exposed and hidden nodes in 802.11 networks," *IEEE Trans. Mobile Computing*, vol. 7, no. 1, pp. 34–49, Jan 2008.

[10] P. M. van de Ven, A. J. Janssen, and J. S. van Leeuwaarden, "Optimal tradeoff between exposed and hidden nodes in large wireless networks," *SIGMETRICS Perform. Eval. Rev.*, vol. 38, no. 1, pp. 179–190, Jun. 2010.

[11] P. van de Ven, A. Janssen, and J. van Leeuwaarden, "Balancing exposed and hidden nodes in linear wireless networks," *IEEE/ACM Transactions on Networking*, vol. 22, pp. 1429 – 1443, October 2014.

[12] K. Nishide, H. Kubo, R. Shinkuma, and T. Takahashi, "Detecting hidden and exposed terminal problems in densely deployed wireless networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 11, pp. 3841–3849, 2012.

[13] S. Chakraborty, S. Chattopadhyay, S. Chakraborty, and S. Nandi, "Defending concealedness in IEEE 802.11n," in *proceedings of the 6th COMSNETS*, Jan 2014, pp. 1–8.

[14] L. Deek, E. Garcia-Villegas, E. Belding, S. Lee, and K. Almeroth, "Intelligent channel bonding in 802.11n WLANs," *IEEE Transactions on Mobile Computing*, vol. 13, pp. 1536–1233, June 2014.

[15] Texas Instruments, "WLAN channel bonding: Causing greater problems than it solves," Tech. Rep., 2003.

[16] I. Tinnirello, S. Choi, and Y. Kim, "Revisit of RTS/CTS exchange in high-speed IEEE 802.11 networks," in *proceedings of the Sixth IEEE WoWMoM*, 2005, pp. 240–248.

[17] MediaTek RT3352 802.11n 2T2R platform (2.4GHz) - single-band 802.11n with 300mbit/s data rates for Wi-Fi access points and routers. Last visited 21 December, 2014. [Online]. Available: http://www.mediatek.com/en/products/connectivity/wifi/home-network/wifi-ap/rt3352/

[18] Open80211s: Open source implementation of IEEE 802.11s for Linux kernel. Last visited 21 December, 2014. [Online]. Available: www.open80211s.org

[19] G. Brar, D. M. Blough, and P. Santi, "Computationally efficient scheduling with the physical interference model for throughput improvement in wireless mesh networks," in *proceedings of the 12th MobiCOM*, 2006, pp. 2–13.

[20] A. Iyer, C. Rosenberg, and A. Karnik, "What is the right model for wireless channel interference?" *IEEE Transactions on Wireless Communications*, vol. 8, no. 5, pp. 2662–2671, May 2009.

[21] J. Jeong, S. Choi, J. Yoo, S. Lee, and C.-K. Kim, "Physical layer capture aware MAC for WLANs," *Wirel. Netw.*, vol. 19, no. 4, pp. 533–546, May 2013.

[22] T.-S. Kim, H. Lim, and J. C. Hou, "Improving spatial reuse through tuning transmit power, carrier sense threshold, and data rate in multihop wireless networks," in *proceedings of the 12th MobiCOM*, 2006, pp. 366–377.

[23] J. Deng, B. Liang, and P. Varshney, "Tuning the carrier sensing range of IEEE 802.11 MAC," in *proceedings of the IEEE GlobeCOM*, vol. 5, 2004, pp. 2987–2991.

[24] C. Reis, R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Measurement-based models of delivery and interference in static wireless networks," in *Proceedings of the 2006 SIGCOMM*, 2006, pp. 51–62.

[25] W. L. Tan, P. Hu, and M. Portmann, "Experimental evaluation of measurement-based SINR interference models," in *Proceedings of the 2012 IEEE WoWMoM*, June 2012, pp. 1–9.

[26] RSSI in MadWiFi. Last visited 21 December, 2014. [Online]. Available: http://madwifi-project.org/wiki/UserDocs/RSSI

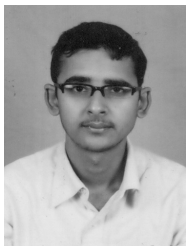
[27] K.-J. Park, L. Kim, and J. C. Hou, "Adaptive physical carrier sense in topology-controlled wireless networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 87–97, 2010.

Sandip Chakraborty Sandip Chakraborty received the PhD degree from Indian Institute of Technology Guwahati, India in 2014. At present, he is working as an Assistant Professor at Indian Institute of Technology Kharagpur, India. His research interests include wireless networks, mobile computing and distributed computing.

Dr. Chakraborty is a Member of IEEE, IEEE Communications Society and Association for Computing Machinery.

Sukumar Nandi Sukumar Nandi received the PhD degree in Computer Science and Engineering from Indian Institute of Technology Kharagpur, India. He is currently a Senior Professor of computer science and engineering with Indian Institute of Technology, Guwahati, Assam, India. He is coauthored of a book entitled *Theory and Application of Cellular Automata* (IEEE Computer Society). His research interests include traffic engineering, wireless networks, network security and distributed computing.

Dr. Nandi is a Senior Member of IEEE, a Senior Member of Association for Computing Machinery, a Fellow of The Institution of Engineers (India) and a Fellow of The Institution of Electronics and Telecommunication Engineers (India).



Subhrendu Chattopadhyay Subhrendu Chattopadhyay received his B.Tech degree from West Bengal University of Technology and M.Tech degree from Indian Institute of Technology, Guwahati, India. He is currently working towards his PhD degree with Indian Institute of Technology, Guwahati, Assam. He has received a research fellowship from TATA Consultancy Services, India. His current research interests are broadly in the area of computer networking, distributed systems and social network analysis.