Defending Concealedness in IEEE 802.11n

Sandip Chakraborty, Subhrendu Chattopadhyay, Suchetana Chakraborty, Sukumar Nandi
Department of Computer Science and Engineering, IIT Guwahati, Assam, India 781039
Email: {c.sandip, subhrendu, suchetana, sukumar}@iitg.ernet.in

***Abstract*—IEEE 802.11 distributed coordination function supports two access mechanisms - the basic access and the four-way access, both of which are vulnerable to the hidden and the exposed node problem (collectively called the concealed node problem). Though most of the works in literature suggest to overlook this problem due to the associated overhead to solve them, this paper shows that the problem becomes severe for high speed wireless mesh networks. An opportunistic four-way access mechanism is designed to defend this problem in IEEE 802.11n mesh networks that supports high data rates. The performance of the proposed scheme is evaluated in a practical 802.11n indoor mesh testbed, that shows a significant performance improvement compared to the standard access mechanisms.**

***Keywords*-IEEE 802.11n; exposed; opportunistic access**

I. Introduction

IEEE 802.11 *'Carrier Sense Multiple Access with Collision Avoidance'* (CSMA/CA) supports two different access technologies - the *basic access*, where every data frame is followed by a corresponding acknowledgement (ACK) frame, and the *four-way access*, where two control frames are used to reserve channel before the actual data communication, namely the 'Request to Send' (RTS) and the 'Clear to Send' (CTS) frames. The basic access mechanism results in the well known *hidden node* problem [1]. Considering Fig. 1, both the nodes A and C want to transmit to the node B simultaneously. The basic access mechanism uses the concept of physical carrier sensing (PCS) before the data communication, where the nodes sense the channel for being idle. As node C is outside the carrier sense (CS) range of node A, it can not sense the ongoing data transmissions $A \rightarrow B$. As a result, node C may initiate another communication with node B, resulting interference near the receiver. The four-way access mechanism [2] solves the hidden node problem by communicating with RTS and CTS handshaking control frames before the actual data transmission. On overhearing these control frames, every node in the CS region of the transmitter and the receiver defer its transmissions to avoid interference. This procedure is called virtual carrier sensing (VCS). However, the four way access mechanism introduces another problem, called the *exposed node problem* [3]. Considering Fig. 1, a node G, outside the CS range of the receiver node B, can initiate communication from node F. However, on overhearing the CTS frame from node B, node F defers all the communication through it. Therefore, on receiving an RTS frame from node G, node F does not reply back with a CTS frame to initiate the communication. Here, F is a receiver-side exposed node, termed as *R-exposed* node in this paper, that can act as a potential receiver, but is blocked due to the VCS. Similarly, from Fig. 1, exposed node problem can also occur at the transmitter side because of the communication blockage due to RTS overhearing. These nodes are termed as *T-exposed* in this paper. In the figure, D is a T-exposed node that can also act as a potential transmitter for another receiver E, outside the CS range of the node B.

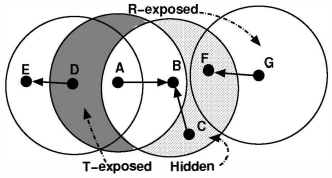

Fig. 1. Hidden, T-exposed and R-exposed nodes

The effects of the concealed nodes for IEEE 802.11 basic and four-way access mechanisms have been well studied in literature, such as [4] and the references therein. Recent researches have shown that RTS/CTS access mechanism does not perform well always, because of the signaling overhead [5] due to control message transmission. Nevertheless, the basic access mechanism suffers from both the hidden and the T-exposed nodes. On the contrary, the four-way access can solve the hidden node problem, but undergoes for both the T-exposed and R-exposed nodes. Though the exposed nodes reduce the spatial reuse, allowing communications to these nodes may result in data-ACK interference, if not properly synchronized. However, as shown in this paper, the exposed node problem becomes severe in the case of high data rate mesh networks built upon the 802.11n technology. In [6], the authors have shown that RTS/CTS exchange can results in performance drop for high data rate mesh networks by increasing number of exposed nodes. However, they have not considered the complete features of 802.11n high speed networks, such as frame aggregation and block ACK (BACK). A number of works exist for mitigating the exposed terminal problem, such as [3] and the references therein, however, they require even additional messages over RTS/CTS, and do not consider the advanced technologies supported by 802.11n. This paper theoretically models the performance of the high data rate mesh networks for three different scenarios with concealed nodes to show their effect over the high speed network

The works of Sandip Chakraborty and Suchetana Chakraborty are supported by the TATA Consultancy Services (TCS), India through the TCS Research Fellowship Program. The authors would like to thank Mr. Rajendra Singh, Skiva Technologies for providing necessary hardware and technical supports to implement the testbed.

978-1-4799-3635-9/14/$31.00 ©2014 IEEE

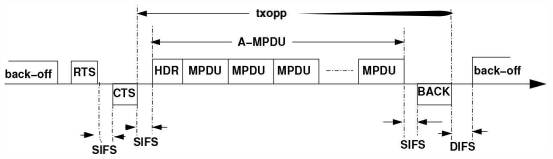

Fig. 2. 802.11n frame aggregation

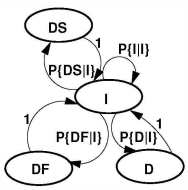

Fig. 3. Basic Access

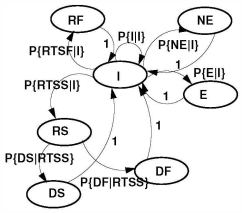

Fig. 4. Four-way Access

performance. An opportunistic RTS/CTS access mechanism is designed to mitigate the problem with the hidden nodes and T-exposed nodes completely, and to partially solve the problem with R-exposed nodes. The frame aggregation and BACK techniques for 802.11n network are used for avoiding data-ACK interference at the exposed nodes. The performance of the proposed scheme is analyzed through the experimental results from a practical 802.11n indoor mesh testbed.

II. Modeling Concealedness in 802.11n

802.11n [7] can support data rates upto 600 Mbps by employing full-duplex dual band multiple input multiple output (MIMO) technologies. It uses the optional four-way handshake mechanism along with the *'frame aggregation'* and BACKs. In the frame aggregation scheme, several MAC protocol data units (MPDUs) are aggregated in a common data unit, called the A-MPDU, associated with a common header. Once the A-MPDU is received, a BACK is forwarded, that contains the MPDU sequence numbers, which are not received correctly due to interference, and need to be retransmitted. If the BACK is not received, the entire A-MPDU is assumed to be lost. The four-way access mechanism for 802.11n frame aggregation and BCAK is shown in Fig. 2. SIFS and DIFS denote the short inter-frame space and data inter-frame space durations, respectively.

A. System Model

This paper considers a network with n nodes uniformly deployed in a plane based on a homogeneous spatial Poisson distribution with node density λ. Every node follows contention based channel access through IEEE 802.11 distributed coordination function (DCF) employing a binary exponential back-off procedure. Let R_{CS} denote the CS range, and R_{IF} denote the interference range. In general, $R_{CS} \leq R_{IF}$ Every node supports 802.11n frame aggregation with BACK capabilities. Let β denote the aggregation level of every node, that means, an A-MPDU can contain β number of MPDUs. For the purpose of theoretical modeling, a discrete time model is considered where the time is divided into fixed length slots of length σ μs, and every event occurs at the beginning of a time slot. The data frames are generated at every node based on a Pareto-normal distribution with a minimum data generation duration as ω μs. Let α denote the probability that a node has data to transmit at time duration $\mathcal{T}$. Then, $\alpha = (\omega/\mathcal{T})^c$, where c is a constant. It can be noted that, if otherwise mentioned, the terms 'transmitter' and 'receiver' denote a data transmitter and a data receiver, respectively.

B. Basic Access with Hidden and T-exposed Nodes

The 802.11n basic access is represented as a 4-state discrete time Markov model, as shown in Fig 3. In a time slot, a node in the system can be in one of the four states;

(i) *Idle State (I):* A node remains in the idle state, if it does not have data to transmit. The average time duration of this state (T_I) is, $T_I = (1-\alpha)\sigma$.

(ii) *Data Success State (DS):* This state represents the successful transmission of data. Let H, D_M and T_a denote the A-MPDU header size, the MPDU size, and the expected A-MPDU transmission time, respectively. Therefore $T_a = H + \alpha\beta D_M$. Assume ρ be the propagation delay, $SIFS$ and $DIFS$ be the two inter-frame space times, and T_b be the BACK transmission time. Therefore, the duration of this state (T_{DS}) is calculated as;

$$T_{DS} = T_a + SIFS + \rho + T_b + SIFS + \rho$$

(iii) *Data Failure State (DF):* This state represents the failure of data transmission due to the interference. As the data and the BACK communications are in reverse directions, the interference is of two types - the data-data interference, and the data-BACK interference. For the data-data interference, the average number of corrupted MPDUs is equal to $\beta\alpha^2$. The data-BACK interference can corrupt either one or two MPDUs, making an average loss of 1.5 MPDUs. Further, if the BACK is lost due to the data-BACK interference, the complete A-MPDU is considered to be lost. Let $T_{ab} = T_a + T_b$. Assuming T_{DF} is the average time a node remains in the DS state,

$$T_{DF} = \frac{T_a}{T_{ab}}(0.5\alpha^2\beta D_M + 0.5 \times 1.5 D_M) + \frac{T_b}{T_{ab}} T_{DS}$$

(iv) *Deferred State (D):* A node goes to the deferred state due to the PCS. The duration of this state is $T_D \approx T_{DS}$.

1) Calculation of Steady State Probabilities: Let $\mathcal{P}_I$, $\mathcal{P}_{DS}$, $\mathcal{P}_{DF}$ and $\mathcal{P}_D$ denote the steady state probabilities for the states I, DS, DF and D, respectively. Then considering the time-homogeneity, the steady state probabilities for the Markov model, shown in Fig. 3, are expressed as follows.

$$\mathcal{P}_{\mathbb{S}_b} = \mathcal{P}_I \times \mathrm{P}\{\mathbb{S}_b | I\}; \qquad \mathbb{S}_b \in \{DS, DF, D\} \tag{1a}$$

$$\mathcal{P}_I = \mathcal{P}_I \times \mathrm{P}\{I|I\} + \mathcal{P}_{DS} + \mathcal{P}_{DF} + \mathcal{P}_D \tag{1b}$$

Let τ denote the probability that a node attempts for a data transmission. The steady state value of τ is calculated according to [8] as; $\tau = 2/(CW+1)$ where CW is the

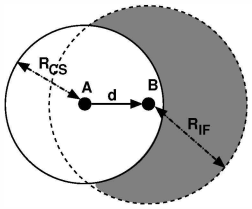

Fig. 5. Basic access

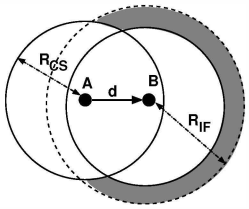

Fig. 6. Four-way access

average contention window size used in IEEE 802.11 DCF back-off procedure. Therefore;

$$\tau = \mathrm{P}\{DS|I\} + \mathrm{P}\{DF|I\} \tag{2}$$

Substituting the values and simplifying, $\mathcal{P}_I$ is represented as;

$$\mathcal{P}_I = 1/(1 + \tau + \mathrm{P}\{D|I\}) \tag{3}$$

The average duration of a transmission opportunity, denoted as $\mathcal{T}$, is calculated as;

$$\mathcal{T} = \mathcal{P}_I T_I + \mathcal{P}_{DS} T_{DS} + \mathcal{P}_{DF} T_{DF} + \mathcal{P}_D T_D \tag{4}$$

2) Analysis of Data Transmission: Let $\mathcal{E}_1$ denote the event that no node in an area Ψ transmits in a given time slot. Based on the Poisson distribution of the nodes, the probability of the event $\mathcal{E}_1$ is calculated as,

$$\wp(\mathcal{E}_1) = \sum_{\nu=0}^{\infty} (1-\tau)^{\nu} \frac{(\lambda\Psi)^{\nu}}{\nu!} e^{-\lambda\Psi} = e^{-\tau\lambda\Psi} \tag{5}$$

Considering Fig. 5, the shaded region indicates the area where hidden nodes can exist for the transmission$A \rightarrow B$. The area of the shaded region, denoted as $\Psi_h(d)$, is given by,

$$\Psi_h(d) = \pi R_{IF}^2 - \Psi_l(R_{CS}, R_{IF}, d) \tag{6}$$

where the value of $\Psi_l(R_{CS}, R_{IF}, d)$ is calculated using simple geometrical analysis. Assuming a spatial Poisson distribution of the nodes, let $f_{CS}(d)$ denote the probability density function (PDF) of the distance between nodes A and B. $f_{CS}(d)$ is calculated as;

$$f_{CS}(d) = \frac{2\pi d}{\pi R_{CS}^2} = \frac{2d}{R_{CS}^2} \tag{7}$$

$\mathrm{P}\{DS|I\}$ and $\mathrm{P}\{DF|I\}$ are calculated as;

$$\mathrm{P}\{DS|I\} = \int_0^{R_{CS}} e^{-\tau\lambda\Psi_h(x)} f_{CS}(x) dx \tag{8}$$

$$\mathrm{P}\{DF|I\} = 1 - \mathrm{P}\{DS|I\} \tag{9}$$

3) Analysis of Deferred State: A node goes to the deferred state if any other node within its CS region starts transmission. In case of the basic access, the nodes in the deferred state include the T-exposed nodes. Henceforth, $\mathrm{P}\{D|I\}$ is calculated as;

$$\mathrm{P}\{D|I\} = \int_0^{R_{CS}} \left(1 - e^{-\tau\lambda\pi R_{CS}^2}\right) f_{CS}(x) dx \tag{10}$$

C. Four-way Access with Exposed Nodes

Fig. 4 presents a 7-state Markov model to analyze the four-way access mechanism. This mode introduces two new states - *RTS success (RS)* and *RTS failure (RF)*, and divides the deferred state into two states - *exposed (E)*, and *non-exposed (NE)*, that is the deferred nodes that are not exposed. The data success (DS) and the data failure (DF) states are initiated after the RS state. Let T_{RTS} and T_{CTS} denote the RTS and the CTS transmission times, respectively, and $T_{\mathcal{S}}$ denote the duration of state $\mathcal{S}$. Then, the duration of these states are calculated as follows,

$$T_{RS} = T_{RTS} + SIFS + \rho + T_{CTS} + DIFS + \rho$$
$$T_{RF} \approx T_{RS};\ T_{NE} \approx T_{DS} + T_{RTS};\ T_E \approx T_{NE}$$

The duration of the DS and DF states are similar to the basic access scenario.

1) Calculation of Steady State Probabilities: Let $\mathcal{P}_I$, $\mathcal{P}_{RS}$, $\mathcal{P}_{RF}$, $\mathcal{P}_{DS}$, $\mathcal{P}_{DF}$, $\mathcal{P}_{NE}$ and $\mathcal{P}_E$ denote the steady state probabilities for the states I, RS, RF, DS, DF, NE and E, respectively. Then considering the time-homogeneity, the steady state probabilities for the Markov model, shown in Fig. 4, are expressed as follows.

$$\mathcal{P}_{\mathbb{S}_f} = \mathcal{P}_I \times \mathrm{P}\{\mathbb{S}_f|I\};\ \mathbb{S}_f \in \{RF, RS, NE, E\} \tag{11a}$$

$$\mathcal{P}_{\mathbb{S}_{f'}} = \mathcal{P}_{RS} \times \mathrm{P}\{\mathbb{S}_{f'}|RS\};\ \mathbb{S}_{f'} \in \{DS, DF\} \tag{11b}$$

$$\mathcal{P}_I = \mathcal{P}_I \times \mathrm{P}\{I|I\} + \mathcal{P}_{RF} + \mathcal{P}_{DS} + \mathcal{P}_{DF} + \mathcal{P}_{NE} + \mathcal{P}_E \tag{11c}$$

Similar to the basic access mechanism, the average duration of a transmission opportunity for the four-way access, denoted as $\mathcal{T}_f$, is represented as;

$$\mathcal{T}_f = \mathcal{P}_I T_I + \mathcal{P}_{RS} T_{RS} + \mathcal{P}_{RF} T_{RF} + \mathcal{P}_{DS} T_{DS} + \mathcal{P}_{DF} T_{DF} + \mathcal{P}_{NE} T_{NE} + \mathcal{P}_E T_E \tag{12}$$

2) Analysis of RTS/CTS Communication: The analysis of the RTS/CTS communication is similar to the analysis of the data transmission for basic access, except that the communication is successful if both the RTS and the CTS are transmitted successfully. Therefore, during RTS (or CTS) transmission, no other node in the interference range of the RTS (or CTS) transmitter should initiate another transmission. Let $\mathcal{E}_3$ denotes the event that no other node in the interference range of the transmitter and the receiver initiates a transmission. The probability of this event, denoted as $\wp(\mathcal{E}_3)$, is derived as;

$$\wp(\mathcal{E}_3) = e^{-2\tau\lambda\Psi_{RC}(R_{IF}, d)} \tag{13}$$

where $\Psi_{RC}(R_{IF}, d)$ denote the area bounded by the interference range of the RTS/CTS transmitter where the nodes are in d distance apart, and can be calculated using a similar procedure. As a result,

$$\mathrm{P}\{RS|I\} = \int_0^{R_{CS}} e^{-2\tau\lambda\Psi_{RC}(R_{IF}, x) f_{IF}(x) dx} \tag{14}$$

$$\mathrm{P}\{RF|I\} = 1 - \mathrm{P}\{RS|I\} \tag{15}$$

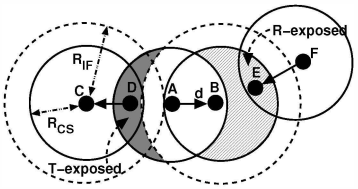

Fig. 7. Exposed nodes for four-way access

where $f_{IF}(x)$ is obtained as, $f_{IF}(x) = \frac{2x}{R_{IF}^2}$.

3) Analysis of Data Communication: In case of the four way handshaking, data failure can occur if a node within the interference range, but outside the CS range of the receiver, initiates a transmission. This can happen because of $R_{IF} > R_{CS}$. Assuming Fig. 6, data is transmitted successfully, if no node in the shaded region initiates a transmission. Let $\Psi_{data}(d)$ denotes the area of the shaded region, when the nodes are in d distance apart. The value of $\Psi_{data}(d)$ can be calculated using s similar procedure.

$$\mathrm{P}\{DS|RS\} = \int_0^{R_{CS}} e^{-2\tau\lambda\Psi_{data}(x)f_{CS}(x)dx} \tag{16}$$

$$\mathrm{P}\{DF|RS\} = 1 - \mathrm{P}\{DS|RS\} \tag{17}$$

4) Analysis of the Deferred Scenarios: During RTS/CTS communication, all the nodes in the CS ranges of both the transmitter and the receiver will defer their communications. As discussed earlier, these nodes are grouped into two classes - the non-exposed nodes, and the exposed nodes, including both the T-exposed and the R-exposed. The shaded regions in Fig. 7 show the position of the exposed nodes when the communicating nodes are in d distance apart. The area of this region, denoted by $\Psi_E(d)$, is calculated as;

$$\Psi_E(d) = 2\pi R_{CS}^2 - \Psi_l(R_{CS}, R_{IF}, d) - \Psi_{RC}(R_{CS}, d) \tag{18}$$

Similarly, The area of the region where non-exposed nodes are placed, denoted by $\Psi_{NE}(d)$, is calculated as;

$$\Psi_{NE}(d) = \pi R_{IF}^2 - \Psi_l(R_{CS}, R_{IF}, d) \tag{19}$$

Therefore,

$$\mathrm{P}\{E|I\} = \int_0^{R_{CS}} e^{-2\tau\lambda\Psi_E(x)f_{CS}(x)dx} \tag{20}$$

$$\mathrm{P}\{NE|I\} = \int_0^{R_{CS}} e^{-2\tau\lambda\Psi_{NE}(x)f_{CS}(x)dx} \tag{21}$$

D. Calculation of the Per-Node Throughput

The per-node throughput, represented as $\mathcal{G}$, is calculated as,

$$\mathcal{G} = \frac{\mathcal{P}_{DS}T_{DS}}{\mathcal{T}} \tag{22}$$

TABLE I
NUMERICAL VALUES OF THE MODELING PARAMETERS

Parameter	value	Parameter	value
MPDU size	1024 bytes	CTS size	14 bytes
β	20	Data rate	300 Mbps
BACK size	20 bytes	Slot time	$10\mu s$
A-MPDU header	28 bytes	SIFS	$10\mu s$
RTS size	20 bytes	DIFS	$50\mu s$

E. Model Verification and Analysis

This subsection verifies the proposed theoretical model, and analyzes the performance of the 802.11n mesh network for the different scenarios based on the numerical data obtained from the proposed theoretical model. The parameters used for the calculation of the theoretical model is summarized in table I. The data sets are generated using Maxima toolbox for the three different access models based on the theoretical analysis - the basic access, the four-access and the optimal access. The model for the optimal access scenario is derived from the four-way access model, shown in Fig. 4, by assuming $\mathcal{P}_E = 0$. This indicates that the exposed nodes are allowed to transmit with the assumption that interference does not occur.

1) Verification of the Theoretical Model: To verify the theoretical model proposed in this section, the numerical data obtained from the model is compared with the simulation results. The simulation is performed in NS-2.35 network simulator framework for both the basic access and the four-way access mechanism for 802.11n with frame aggregation and BACK support. Similar parameters, as given in table I, are used for the simulation purpose. The results are plotted with respect to the data generation probability (α) at every node. Every simulation setup is executed for 10 times with different seed values, and the average is taken to plot the graphs. The confidence interval, expressed in terms of the difference between the maximum and the minimum results, are also shown in the graphs. For both the theoretical and the simulation results, node density is considered as 16 nodes per $100m$, where the mean carrier sensing range is $50m$ with $5m$ variance. In the simulation setup, the capture threshold is taken as $20dB$ with transmit power $16dBm$ and receiver sensitivity $-85dBm$, according to RT-3352 802.11n wireless routers [9] (used for the testbed setup, as discussed in subsequent section). With this setup, the mean interference range becomes $65m$ with $5m$ variance.

Fig. 8 and Fig. 9 show the comparisons between the theoretical and the simulation results for the basic access and the four-way access, respectively. The vertical lines in the simulation results show the confidence interval. Both the figures show that the theoretical results and the simulation results are similar.

2) Effect of Hidden and Exposed Nodes: Fig. 10 compares the normalized throughput with respect to α for three scenarios, as discussed earlier. The figure reveals that when the data generation rate is very low, basic access performs marginally better than the four-way access. This is because of

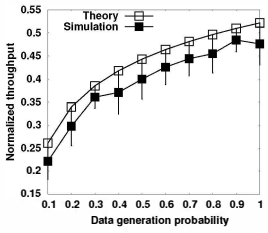

Fig. 8. Basic access

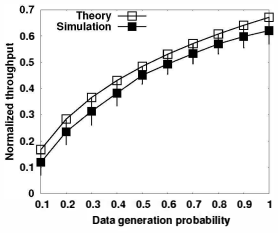

Fig. 9. Four-way access

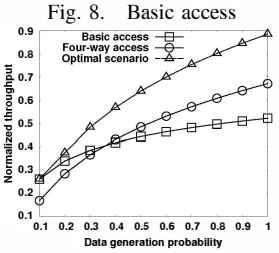

Fig. 10. Effect of α

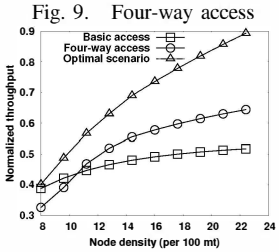

Fig. 11. Effect of λ

the signaling overhead associated with RTS/CTS handshaking. However, with higher data generation rates, the four-way handshake performs better than the basic access. The network throughput can be considerably improved with the optimal channel access, where the concealed nodes are completely avoided. Similar result is obtained from Fig. 11, that shows the normalized throughput with respect to the node density λ. As λ value increases, more exposed and hidden nodes are generated in the system, resulting in performance degradation for the basic access and the four-way access. Further, the signaling overhead associated with the optimal scenario is considerably lower than the benefits even in case of the low load scenario. Both the figures reveal that the optimal scenario provides better performance compared to the basic access and the four-way access, for both the low-load and the high-load scenario. Therefore, it is desirable to eliminate the concealed nodes as much as possible to improve the network performance by extensive spatial reuse.

III. Opportunistic Access: Design and Analysis

In the proposed opportunistic access mechanism built over four way access, the RTS and CTS messages are used for the detection of hidden nodes, as well as transmission is allowed to the exposed nodes. The data-BACK interference at T-exposed nodes are solved using a mechanism called 'null framing'. However, the interference at R-exposed nodes are not avoidable, and therefore the proposed opportunistic access mechanism allows transmission for the R-exposed nodes only if the data loss due to interference is comparatively less than the performance gain. The detailed design of the opportunistic access mechanism is discussed in following sections.

A. Opportunistic RTS/CTS Access

The legacy RTS/CTS protocol uses a table, called the *network allocation vector* (NAV), to maintain the transmission blockage on overhearing the RTS/CTS frames. The RTS/CTS frames contain a duration field (DU) that indicates the time duration for the channel reservation. On overhearing the RTS/CTS frames, every node sets its NAV for the time

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: Send RTS; /*T-exposed nodes*/
3: **else**
4: Back-Off and retry;
5: **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: Send CTS; /*R-exposed nodes*/
3: **end if**
4: $RTS_{act} \leftarrow this.RTS$ /*Append the received RTS in RTS_{act}*/

mentioned in the DU field. In the proposed augmentation of four-way access, different NAVs are maintained for every overheard RTS/CTS frame to detect the exposed nodes, and to avoid the data-BACK and data-control interferences. 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 frame $\mathcal{F}$. Further assume that $\mathcal{N}_i$ denote the set of nodes that are in the CS range of node i. This set can be populated using standard beaconing.

The decision controls for exposed node detection are explained through Algorithm 1 and Algorithm 2, 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. 1, 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 node C is outside the CS range of node B, but within the CS range of node A. In this scenario node C acts as a receiver, and therefore, should not initiate a communication. Node C can overhear the RTS from node A, and includes it in the RTS_{act} set. On receiving the RTS frame from any other node, say H, node C executes Algorithm 2. However, the condition is evaluated to be false as $RTS_{act} \neq NULL$. Therefore it does not replies back with the CTS, and the communication is deferred.

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

3) Spatial Reuse by R-exposed Nodes: Considering Fig. 1, let $A \rightarrow B$ communication starts first. As node F is outside the CS range of node A, it does not overhear the RTS. Therefore $RTS_{act} = NULL$. Assume, node F receives an RTS from node G. As node F is within the CS range of node B, it overhears the CTS from node B. However, $CTS_B.DST = A \notin \mathcal{N}_F$. Therefore following Algorithm 2, it replies back with the CTS, resulting in the communication initialization.

B. Interference resolution

As discussed earlier, allowing the communication to the exposed nodes may result in data-BACK or data-control interferences. Two main properties of 802.11n access mechanism is explored to solve this problem, the frame aggregation along with BACK, and multiple simultaneous data streaming using MIMO technology. The MIMO with dual streaming in 802.11n allows a node to transmit and receive simultaneously using two different channels (20/40 MHz).

Interference can not be avoided completely for the nodes that are outside the CS range of the receiver. A node can avoid interference by overhearing the existing communications within its CS range. Further, the interference can occur either at the transmitter side (when there is an ongoing communication within the transmitter's CS range) or at receiver side (when there is an ongoing communication within the receiver's CS range). Based on this observation, either transmitter or receiver takes the responsibility to avoid interference, as described in the following subsections.

1) Sender Side Interference Avoidance: Considering Fig. 1, allowing $D \rightarrow E$ communication simultaneously with $A \rightarrow B$ communication may result in data-control and data-BACK interference at D, when E sends the CTS and the BACK frames, respectively. Similarly data-BACK interference can occur at A, when B sends the BACK frame. The control frames are lost in this scenario. To avoid this situation, this paper introduces the concept of NULL framing within an A-MPDU frame, as shown in Fig. 12. The NULL framing is a transmission gap within the A-MPDU frames, that indicates a possible interference duration. As shown in Fig. 12, on overhearing the RTS frame from node D, node A forwards a NULL frame after the current MPDU. This information is also appended in the MPDU sub-header to inform the receiver B about the upcoming NULL frame. To avoid interference, the size of the NULL frame is made equal to $SIFS + T_{CTS} + DIFS$. Further, node D initiates the RTS transmission at the end of a $DIFS$ interval, after it senses the beginning of an MPDU transmission from A. Similarly, from the DU field of the overheard RTS from node A, node D knows the end of the reservation period for node A. Therefore, node D forwards another NULL frame to avoid the data-BACK interference.

2) Receiver Side Interference Mitigation: Considering Fig. 1, let $A \rightarrow B$ starts earlier than $G \rightarrow F$, resulting in data-CTS and data-BACK interference at nodes B and F. The data frames will be lost in this scenario. However, as the size of the control and BACK frames are less than the MPDU, either one or two MPDUs will be lost. Further, the transmission of data frames are controlled by the transmitter, and in this scenario, the coordination between the transmitters is costly as they are more than two hops away. Therefore, interference can not be avoided completely. In the proposed opportunistic access, the receiver initiates the communication if the losses of MPDUs due to the interference is less. Based on the CTS overhearing, node F can determine the number of receivers within its CS range. Let the number of such receivers be $\Re_F$. Due to the data-CTS and data-BACK interference, maximum number of MPDU losses can be calculated as $4 \times \Re_F$. Let $G \rightarrow F$ communication wants to reserve the channel for $P_{G \rightarrow F}$ numbers of MPDUs. Then, node F initiates the communication by replying back with a CTS frame, if $(4 \times \Re_F / P_{G \rightarrow F}) < \Upsilon$, where Υ is a constant threshold. The value of Υ is determined based on the cost-benefit trade-off, as analyzed in the next section.

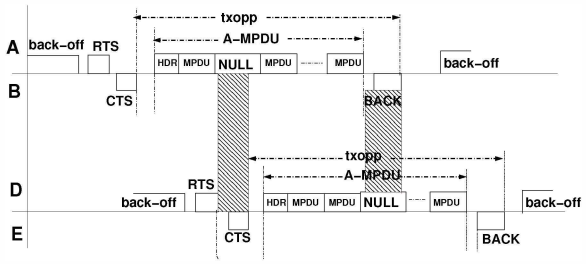

Fig. 12. Interference scenario and NULL framing

To find out the expected value of $\Re_i$ for a node i, let us assume that ϑ be the probability that a node acts as a receiver. From Fig. 1, the nodes that are inside the CS range of both the transmitter and the receiver, can not act as a receiver due to the hidden node problem. Therefore, only the nodes that are in the CS range of the receiver, but not in the CS range of the transmitter, can act as a receiver. Let Ψ_R denote the area where a receiver node can exist. Ψ_R can be calculated as,

$$\Psi_R = R_{CS}^2 (\frac{2\pi}{3} + \frac{\sqrt{3}}{2})$$

From the assumption of the spatial Poisson distribution of the nodes, the expected number of receiver within the CS region of a node i, denoted as $E[\Re_i]$, is calculated as,

$$E[\Re_i] = \vartheta \sum_{\nu=0}^{\infty} \nu \frac{(\lambda \Psi_R)^\nu}{\nu!} e^{-\lambda \Psi_R} = \vartheta \lambda \Psi_R \qquad (23)$$

From the steady state distribution, $\vartheta = \alpha$, where α is the frame generation probability as mentioned earlier. Henceforth;

$$E[\Re_i] = \alpha \lambda R_{CS}^2 (\frac{2\pi}{3} + \frac{\sqrt{3}}{2}) = 2.96 \alpha \lambda R_{CS}^2 \qquad (24)$$

Let there are ε number of nodes in the area πR_{CS}^2 (the area bounded by the CS range of a node). Therefore,

$$E_{MAX}[\Re_i] = 2.96 \alpha \frac{\varepsilon}{\pi R_{CS}^2} R_{CS}^2 = 0.94 \alpha \varepsilon \qquad (25)$$

As $\alpha \leq 1$, the expected number of interfering frames is considerably lower than the number of frames to be transmitted by a R-exposed node. Therefore, in spite of some frame losses,

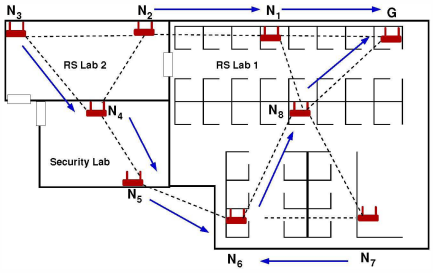

Fig. 13. 802.11 Indoor mesh testbed and connectivity layout

the overall performance of the network can be improved by allowing the transmission to the R-exposed nodes.

IV. Experimental Results

This section analyzes the performance of the proposed opportunistic access through the results from a indoor mesh testbed.

A. Testbed Analysis

The proposed scheme is implemented and evaluated using a 9-node 802.11n indoor mesh testbed deployed over the IIT Guwahati computer science department research labs, as shown in Fig. 13. The connectivity among the nodes is shown using dotted lines. The node G works as the mesh gateway. Each node is a Skiva Easyconnect RT001 N300 WiFi router with RaLink RT-3352 chipset [9]. This chip can support up to 300 Mbps data rate with maximum transmission power of 200 mW, that corresponds to average $10m$ CS range and $15m$ interference range, with a deviation of $\pm 5m$ based on the external noise factor.

1) Testbed Setup: Every node communicates with the gateway through multi-hop communication. On average 10 number of clients are attached with every mesh node. Trivial File Transfer Protocol (TFTP) is used as the application layer traffic, that uses UDP at the network layer. Two scenarios have been evaluated - a scenario when the network is loaded, and in the second scenario, the network load is low. In the fully loaded scenario, every client generates traffic at an average rate of 10 Mbps. The average traffic generation rate for the lightly loaded scenario is 1 Mbps. The proposed opportunistic access mechanism is implemented as a loadable kernel module (LKM) at every router. The MAC layer calls the LKM to decide the access policy. The blue arrows in Fig. 13 indicate an example data flow communication architecture in the mesh network that is used for evaluation purpose. It can be noted that the MAC layer forwarding decision is based on a link quality metric, called the expected transmission count [10], that periodically measures the link quality in terms of signal strength and frame loss. Therefore, the best path is not necessarily the minimum-hop path. The performance of the proposed opportunistic access scheme is compared with the basic access and the four-way access mechanisms. For 802.11n, dual streaming is used with frame aggregation level set to 20. The MPDU size is kept fixed at 256 Kb.

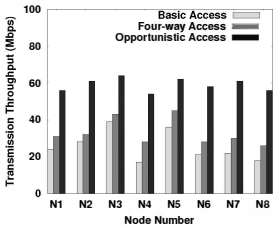

Fig. 14. Throughput: High Load

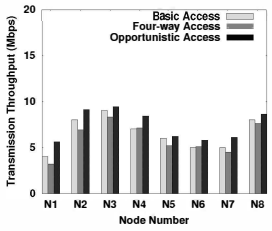

Fig. 15. Throughput: Low Load

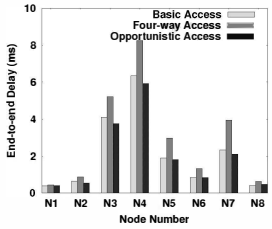

Fig. 16. Delay: High Load

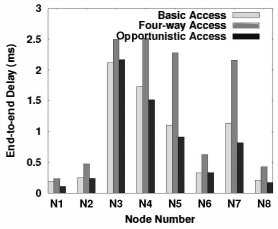

Fig. 17. Delay: Low Load

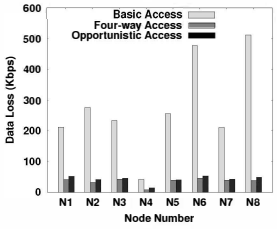

Fig. 18. Loss: High Load

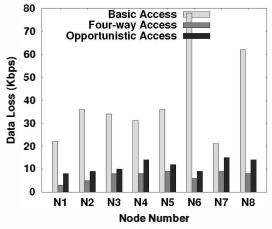

Fig. 19. Loss: Low Load

2) Per Node Performance: Fig. 14 and Fig. 15 compare the performance of the opportunistic scheme with other naive approaches in terms of average transmission throughput per mesh node. The average transmission throughput is calculated as the amount of data transmitted successfully per unit time. For the fully loaded network, the transmission throughput for the four-way access is more than the transmission throughput for the basic access, as the four way access reduces data loss due to hidden nodes. On the contrary, Fig. 15 reveals that for the lightly loaded network, basic access performs better than four-way access, which is because of extra control overhead. However, both the figures show that the proposed opportunistic access mechanism performs better than other two approaches, for both the fully loaded network and the lightly loaded network.

Fig. 16 and Fig. 17 show the forwarding delay for the above two scenarios. The figure reveals that for both the fully loaded and the lightly loaded scenario, the forwarding delay for the four-way access is more than the basic access. The analysis of the individual packet traces have revealed that this increment forwarding delay is partially because of RTS/CTS handshaking, and more because of the transmission deferring due to the VCS. It can be noted that due to the frame aggregation and BACK schemes, the RTS/CTS handshaking overhead is considerably reduced in case of 802.11n. Further, the transmission deferring is avoided in the case of the proposed opportunistic forwarding by allowing exposed node to participate in communications, which decreases the forwarding delay substantially by reducing the waiting time.

Fig. 18 and Fig. 19 analyze the packet loss for the three

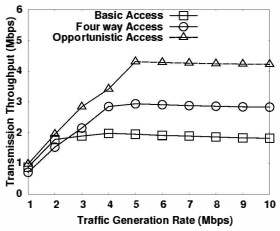

Fig. 20. Throughput

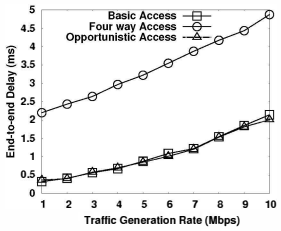

Fig. 21. Forwarding Delay

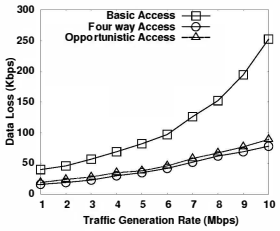

Fig. 22. Data Loss

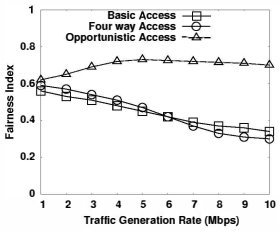

Fig. 23. Fairness

access protocols in the two different scenarios. These figures divulge that the data loss is considerably more in the case of basic access mechanism. The reason behind the data loss for the basic access is mainly due to the hidden nodes. For the testbed scenario, number of hidden nodes is more for nodes $N6$ and $N8$, which results in high data loss for these two nodes, as seen from Fig. 18. For the fully loaded network, the amount of data loss is significant, compared to the four-way access and the opportunistic access. The four way access and the opportunistic access avoids the data loss by reserving the channel through the RTS/CTS handshaking and the VCS. The small data loss for the four way access and the opportunistic access is due to the interference from the nodes which are outside the CS range.

3) Effect of the Network Traffic Load: For this set of experiments, the performance of the individual clients are evaluated by varying traffic generation rates. Fig. 20 shows the average per client transmission throughput with respect to the traffic generation rate. As usual, the performance of the opportunistic access is more than the basic access and the four-way access. One interesting observation can be made from the figure that the saturation point of the network is different for different channel access mechanism. While the basic access makes the network saturated at per client 2 Mbps data generation rate, the four-way access saturates the network as 4 Mbps, and the opportunistic access makes the network saturated at 5 Mbps. Because of the hidden nodes, lots of data frames are dropped, which reduces the network capacity for the basic access. The T-exposed nodes further reduces the capacity by blocking the nodes through the PCS. Though the hidden node problem is being solved for the four-way access, the exposed node problem causes the reduction in network capacity for the four-way access mechanism. The proposed opportunistic access mechanism unleash the network capacity by solving both the concealed node problem. Fig. 21 and Fig. 22 show the average end-to-end forwarding delay and the average data loss for the three access mechanisms. As earlier, the opportunistic access mechanism reduces both the forwarding delay and the data loss.

Another network performance parameter, fairness, is used to evaluate the performance of the proposed access mechanism, as shown in Fig. 23. Fairness is calculated in terms of Jain's fairness index [11]. The fairness index value 1 indicates maximum fairness. The figure shows that the fairness index value for the basic access and the four-way access is considerably less compared to the proposed opportunistic access. The packet drops due to hidden nodes result in severe unfairness in the basic access scenario. In the four way access, the R-exposed nodes does not reply back with the CTS packets, which results in high back-off value for the RTS transmitters. This causes unfairness in the network. The problem of unfairness becomes severe as network load increases. The opportunistic access solves both the hidden nodes and exposed nodes, resulting in fairness improvement.

V. Conclusion

This paper shows the severity of the concealed nodes problem in case of the high speed wireless mesh network using theoretical modeling. The analysis shows that the hidden nodes cause severe data losses, and the exposed nodes under-utilize the network capacity by reducing the spatial reuse opportunities. Based on the 802.11n frame aggregation and BACK capabilities, this paper proposes an opportunistic access protocol over the four-way access paradigm to defend the concealed node problems. The effectiveness of the proposed opportunistic scheme is analyzed by results from a practical high speed indoor mesh testbed analysis.

References

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

[2] 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.

[3] J. Yao, T. Xiong, and W. Lou, "Elimination of exposed terminal problem using signature detection," in *Proceedings of the 9th Annual IEEE SECON*, 2012, pp. 398–406.

[4] J. Alonso-Zarate, L. Alonso, G. Kormentzas, R. Tafazolli, and C. Verikoukis, "Throughput analysis of a cooperative ARQ scheme in the presence of hidden and exposed terminals," *Mob. Netw. Appl.*, vol. 17, no. 2, pp. 258–266, Apr. 2012.

[5] R. Bruno, M. Conti, and E. Gregori, "IEEE 802.11 optimal performances: RTS/CTS mechanism vs. basic access," in *Proceedings of the 13th IEEE PIMRC*, vol. 4, 2002, pp. 1747–1751.

[6] 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.

[7] N. Hajlaoui, I. Jabri, and M. Benjemaa, "Experimental study of IEEE 802.11n protocol," in *Proceedings of the seventh ACM WiNTECH*, 2012, pp. 93–94.

[8] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. on S. Areas in Comm.*, vol. 18, no. 3, pp. 535–547, 2000.

[9] RaLink RT3352 series ieee 802.11n routers-on-chip. [Online]. Available: http://www.mediatek.com/_en/01_products/04_pro.php?sn=1006

[10] M. E. M. Campista, P. M. Esposito, I. M. Moraes, L. Costa, O. Duarte, D. G. Passos, C. V. N. de Albuquerque, D. C. M. Saade, and M. G. Rubinstein, "Routing metrics and protocols for wireless mesh networks," *IEEE Network*, vol. 22, no. 1, pp. 6–12, 2008.

[11] R. Jain, A. Durresi, and G. Babic, "Throughput fairness index: An explanation," Tech. rep., Department of CIS, The Ohio State University, Tech. Rep., 1999.