Research Article

Modelling link failure in the presence of extended hidden terminals over multi-hop wireless ad hoc networks

Radha Ranganathan[1] · Vinuthna Kambalapally[2] · Kathiravan Kannan[3]

Abstract

IEEE 802.11 uses RTS/CTS (request to send/clear to send) reservation mechanism in multi-hop ad hoc networks to prevent collision drops caused by the hidden terminals. Extended hidden nodes impose great challenges to RTS/CTS mechanism by creating additional interferences and route failures. We introduce a Markov model to compute the probability of collision due to hidden and extended hidden nodes present in multi-hop ad hoc network under saturated traffic loads. This model is derived from the well-known Bianchi Markov chain model of IEEE 802.11 Distributed coordination function by introducing additional states in every back-off stage. Our model differentiates the collisions that could happen to RTS/CTS and data packets. We also compute the probability of link failure that occurs when the maximum retry limit is exceeded. The model is tested for varying network sizes with number of nodes 10, 50, 100, 150 and 200. The model validates the throughput, collision probability and link failure probability against the Bianchi model and ns-2.35 simulation result.

Keywords IEEE 802.11 · RTS · CTS · Extended hidden terminal · Link failure · Collision probability · Throughput · Markov model

1 Introduction

Shared nature of wireless transmission results in severe collisions or interferences over multi-hop ad hoc network. The wireless node equipped with omni antenna propagates the signal in all directions. Signal strength in the wireless medium fades in proportion to the square of the distance from the transmitter. In Fig. 1, when NODE-0 propagates signal in the form of data packet, the nodes in the transmission range (NODE-1) will be able to receive the data packet successfully.

The nodes in the interference range (NODE-2) will get interfered by NODE-0's transmission and receive the signal as a background noise. NODE-3 does not fall in the signal propagation range of NODE-0, implying that NODE-3 will not be interfered by NODE-0 but by NODE-1. In order to

schedule the wireless medium among multiple nodes, IEEE 802.11 is widely accepted as a medium access control (MAC) protocol for MANET. It uses binary exponential back-off algorithm (BEB) for collision avoidance.

Hidden terminals pose greater challenges to the MAC protocol design over multi-hop ad hoc networks. Hidden terminals are the nodes that are in the transmission range of the receiver but not in the transmission range of the sender of data transmission. They could cause potential interference in data transmission. To avoid such collisions, IEEE 802.11 protocol was enhanced with RTS/CTS mechanism that reserves as a medium for data transmission over the region of transmission range of both sender and receiver. This region is named as the covered region of IEEE 802.11 RTS/CTS mechanism. The remaining nodes that are lying in the detection/interference range of the sender

✉ Radha Ranganathan, radhupriya@yahoo.co.in; Vinuthna Kambalapally, vinuthna.dwh@gmail.com | [1]Department of CSE, Faculty of Science and Technology, ICFAI Foundation for Higher Education, Hyderabad, India. [2]Department of CSE, Koneru Lakshmaiah Education Foundation, Hyderabad, India. [3]Department of CSE, Easwari Engineering College, Chennai, India.
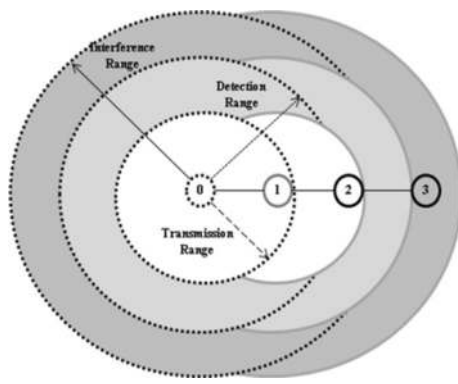
Fig. 1 Signal propagation range

and receiver are called extended hidden terminals. RTS/CTS messages cannot be decoded by extended hidden terminals, thus leading to failure in reserving the medium over the region of extended hidden terminals. This region is named as uncovered region. Physical carrier sense at transmitters does not help unless a very large carrier sensing range is adopted [1]. Extended hidden terminals lying in the uncovered region causes potential interference or collisions, which leads to data packet drops as well as RTS/CTS drops.

Packet drops could be recovered using local retransmissions at the MAC layer. But the increased collisions among hidden terminals lead to the event of exceeding the retry limits of the retransmissions. This scenario makes the transmitter drop the data packet and report link failure notification to the network layer, which unnecessarily initiates the route discovery. In this model, we take into account the collisions caused by covered and uncovered regions while transmitting RTS/CTS and data packets and derive the collision probability along with link failure probability.

Analytical models play an essential role in performance computation and protocol optimization. Bianchi was the first to describe the binary exponential back-off mechanism of distributed coordination function (DCF) protocol in a single node. The author [2] assumed that the collision probability of each transmitted packet is constant and independent of the number of retransmissions. The drawback of Bianchi's model is that it does not consider the freezing probabilities and assumes that the back-off counter is never frozen. Bianchi also calculated the packet delay of both access mechanisms separately.

Even though a myriad of Markov chain models exist to evaluate collision probability and throughput end-to-end delay, such models are generally limited to single-hop ad hoc networks. They do not consider the presence of extended hidden terminals in multi-hop ad hoc networks while deriving the performance measures. The proposed analysis is studied for RTS/CTS method of IEEE 802.11 DCF.

Our model considers the interferences caused by both hidden and extended hidden terminals. Freezing probability of the nodes during back-off stage is also considered under the assumption of saturated traffic condition with finite number of stations. This model evaluates the throughput and link failure probability extensively.

The rest of the paper is organized such that Sect. 2 covers the related work and Sect. 3 introduces the proposed Markov model and presents the derivation of collision and link failure probabilities in detail. Performance evaluation of the proposed model is explained in Sect. 4. Conclusion is briefed in Sect. 5

2 Related work

Multiple models were proposed based on Bianchi's Markov chain to describe the 802.11 protocol more accurately [3]. Chatzimisios et al. [4] considered the retransmission limit in which a packet drop happens while reaching a maximum retry limit. Zhang et al. [5] and Xiao [6] improved the analysis by taking the back-off counter freezing probability in their models. In [7], authors analysed the throughput for non-saturated traffic over heterogeneous networks and predicted that optimized throughput can be achieved prior to saturation. In [8], the author provides a quantitative analysis to estimate the optimized load for maximum throughput in a multi-hop scenario and also to find the impact of hidden nodes and capture effect. Per-flow throughput in a multi-hop network is found through an analytical model by identifying the dominating and starving flows [9]. In [10], authors found out the pattern of throughput distributions among the links of the multi-hop network by using a new back-off-the-envelope computation.

Many theoretical models have been developed for IEEE 802.11 random access scheme over single-hop wireless ad hoc networks without considering hidden terminals [4, 11–15]. They extended the Bianchi Markov model with the calculation of performance metrics like average packet delay, throughput, packet loss probability, frame error rate, frame delay, packet errors on the capacity and service time. Many authors have developed analytical models to realize IEEE 802.11 over multi-hop ad hoc networks [16–25]. However, authors [16–20] did not consider the effect of hidden terminals while calculating the throughput or delay. In [21–25], the authors derived the saturation throughput of CSMA/CA with RTS/CTS handshake in multi-hop networks. But they do consider the collisions happened during the transmission of RTS packet.

In [26], authors analysed that the interference happens on a link by considering the mutual interference from nearby multi-hop paths. They evaluated end-to-end throughput against number of nodes, connections and retransmissions. In [27], the probability of received power

at a node is studied while considering a set of nodes transmitting in the previous hop to characterize the coverage performance of the network. Salah [28] analysed the throughput and delay performance of IEEE 802.11 DCF over multi-hop ad hoc networks in the presence of hidden terminals. They analysed the effect of three parameters, namely hidden nodes, network size and maximum back-off stage in throughput and delay. They also did not take into account the extended hidden terminals in analysing the performance.

Murad et al. [29] studied collision probability of IEEE 802.11 DCF over full-duplex communication using Bianchi model and proved that collision reduces in full-duplex mode. They did not consider the effect of extended hidden terminals in duplex communication. Laura [30] handled hidden terminals and analysed the performance of IEEE 802.11 by changing packet arrival model of access point to be multiple packet reception capable. We have considered extended hidden terminals and their effect on collision, which is different from the above works to the best of our knowledge.

3 System model

We consider a horizontal chain topology of multiple nodes as shown in Fig. 2. We assume that the nodes communicate with each other using half-duplex radio transceivers with IEEE 802.11 DCF mode in saturated traffic conditions. It means that every node has at least one packet to transmit at any time.

Transmission range of a node represents the region where the packets can be successfully received and decoded. Interference range of a node represents the region where the nodes lying in this region may affect the reception of data packets. We assume that carrier sense range is almost equal to interference range.

When a node wants to transmit, it senses the medium using physical carrier sense. If the node finds that the

Fig. 2 Network model

medium is free for DIFS plus random back-off period, the node transmits RTS control packet to the receiver. RTS includes the time duration needed for the data transmission. All neighbours of the sender overhear the RTS and set their network allocation vector (NAV) timer. The receiver node responds with CTS control packet if it senses the medium to be free.

The receiver node also specifies the time duration for data reception in CTS packet. The neighbours of the receiver overhear CTS and set their own NAV accordingly. Usage of NAV enables virtual carrier sensing and limits physical carrier sensing by making the node to sleep for specified duration, thus saving power. In this way, RTS/CTS exchange is helpful in avoiding unnecessary collisions in the covered region which is shown in Fig. 2. The RTS/CTS handshake cannot completely eliminate the problem of hidden terminals. Large portion of interference range is left uncovered by RTS/CTS method. The area labelled as region 2 in Fig. 2 shows the uncovered region of RTS/CTS handshake. Covered region includes the set of nodes that are neighbours to sender and/or receiver and shaded as region 1 in Fig. 2. The remaining nodes lying in region 2 will not be able to decode the RTS/CTS messages, thereby missing out the opportunity of virtual carrier sensing.

This uncovered region is the root cause of the collisions happening over multi-hop ad hoc networks. In this work, we derive the probability of collisions caused by region 1 and region 2 separately, which is then used in the Markov chain. We assume that NODE-1 is the transmitter and NODE-2 is the receiver. While NODE-1 wants to communicate with NODE-2, NODE-1 has to send RTS to the NODE-2. In this scenario, when some other node lying in the covered (region 1) or uncovered region (region 2) also transmits at the same time, collision might happen to RTS or CTS packets. This probability is labelled as P_{C1}.

Data transmission follows the successful RTS/CTS exchange. In this scenario, collision might happen to the data packet due to the simultaneous transmission from any other node in the uncovered region. This probability is labelled as P_{c2}. Virtual carrier sensing prevents the nodes lying in the covered terminal from transmission. In the next section, we derive the collision probability occurring in region 1 and region 2. We derive the collision probability P_{c1} and P_{c2}, in the following section, and we utilize these probabilities in the Markov chain model.

We build a two-dimensional Markov chain as shown in Fig. 3, based on Bianchi model [2] for simulating IEEE 802.11 DCF with RTS/CTS extension over multi-hop ad hoc network. We have added two new states $(i, -1)$ and $(i, -2)$ at every stage to reflect RTS/CTS transmission. Every state in the model is represented using two dimensions (i, j), where i represents the stage at which the transmission is done. It ranges from 0 to n. Stage 0
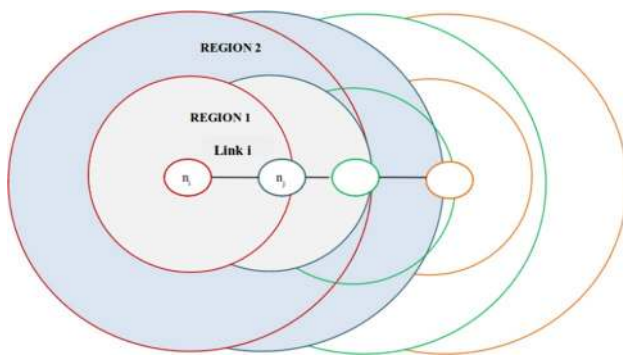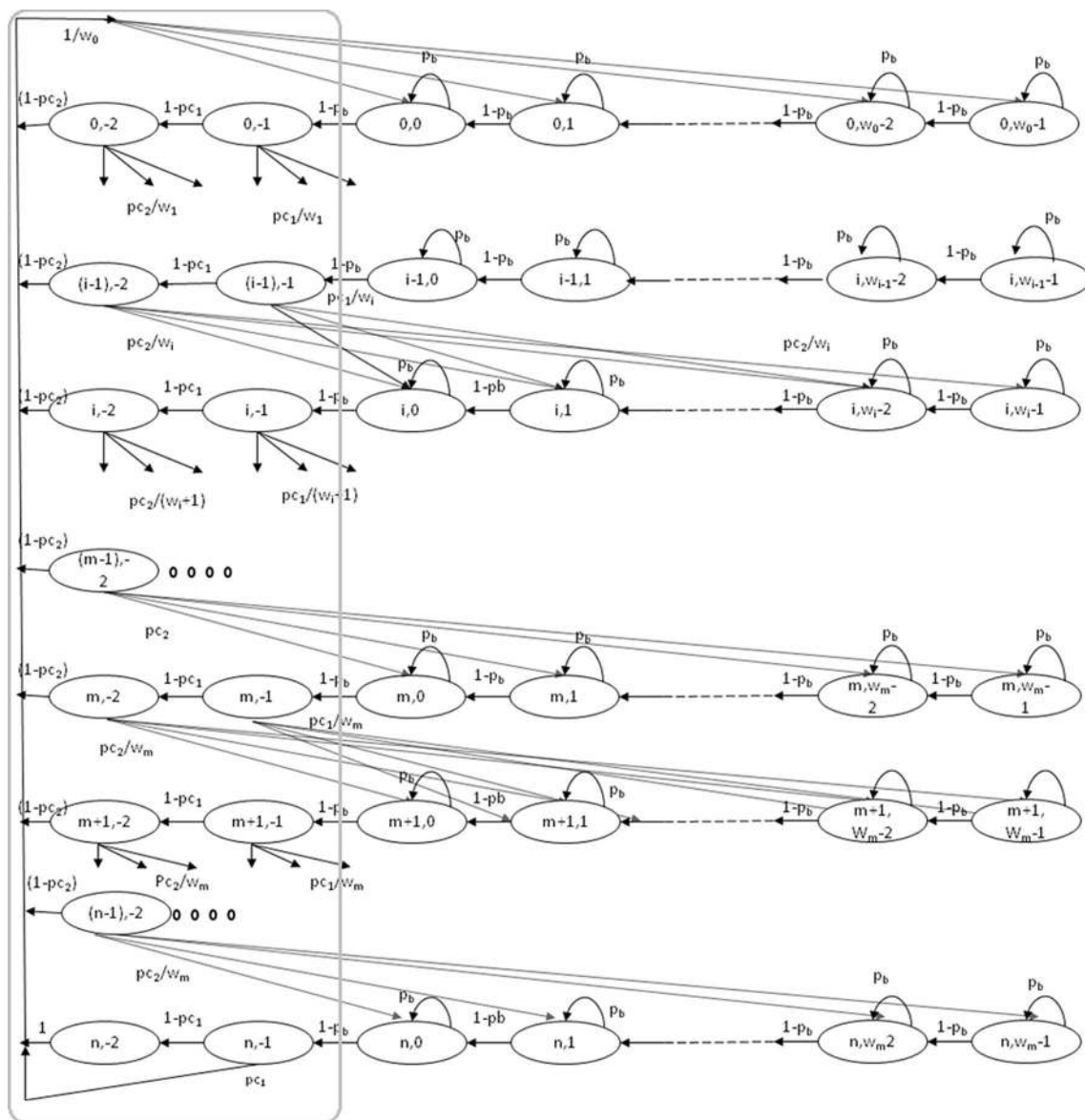
Fig. 3 Markov chain model

represents the first attempt of the transmission; stage 1 represents the first retransmission on collision. The transition from ith to $(i+1)$th stage occurs due to collision. On successful transmission, node moves from ith stage to 0th stage for transmitting the next packet. j represents the back-off counter value, and it ranges from 0 to W_i, where W_i denotes the maximum contention window size at the ith stage. Initially, when the node is at 0th stage, its back-off counter is chosen randomly and mapped to anyone of $(0, W_0 - 1)$ node and keeps switching to the next state for every idle slot time. P_b represents the busy-state probability.

When the node reaches $(0, 0)$th state, it senses the medium for the idle state and transmits RTS and then enters − 1th state. On receiving the RTS without any collision and finding the channel status to be idle, the receiver of the current node responds with CTS; on the receipt of CTS, the node transmits data and enters − 2nd state. P_{c1} represents the collision probability for RTS packet. If the RTS packet encounters collision, then the sender node will not be able to receive the CTS packet. Hence, eventually, it times out and enters the next stage in the Markov chain.

When the data packet encounters collision, the sender times out and enters the next stage. The value of W_i is exponentially incremented for every next stage till it reaches the maximum $W_{max}(W_m)$. Value of W_0 is initially set to the minimum value W_{min}. According to the specification of IEEE 802.11, W_{min} and W_{max} are set to the values 32 and

1024, respectively. Once W_i reaches the value of W_{max}, it does not change in the subsequent stages. Retransmission limit for RTS collisions (short retry count) is set to 7, and retransmission limit for data packets (long retry count) is 3. Whenever the retransmission exceeds the maximum limit, the node drops the corresponding data packet. The successful data transmission could occur at any $(i, -2)$ state where i lies between 0 and n. Transition probabilities of the individual states are given in Eq. (1).

$$
\begin{aligned}
P\{i,k|i,k+1\} &= 1 - P_b & k &\in (-1, W_i - 2) & i &\in (0, n) \\
P\{i,k|i,k+1\} &= 1 - P_{c1} & k &= -2 & i &\in (0, n) \\
P\{i,k|i,k\} &= P_b & k &\in (-1, W_i - 1) & i &\in (0, n) \\
P\{0,k|i,-2\} &= \tfrac{1-P_{c2}}{W_0} & k &\in (0, W_0 - 1) & i &\in (0, n-1) \\
P\{i,k|i-1,-2\} &= \tfrac{P_{c2}}{W_i} & k &\in (0, W_i - 1) & i &\in (1, m) \\
P\{i,k|i-1,-1\} &= \tfrac{P_{c1}}{W_i} & k &\in (0, W_i - 1) & i &\in (1, m) \\
P\{i,k|i-1,-2\} &= \tfrac{P_{c2}}{W_m} & k &\in (0, W_m - 1) & i &= (m+1, n) \\
P\{i,k|i-1,-1\} &= \tfrac{P_{c1}}{W_m} & k &\in (0, W_m - 1) & i &= (m+1, n) \\
P\{0,k|i,-2\} &= \tfrac{1}{W_0} & k &\in (0, W_i - 1) & i &= n \\
P\{0,k|i,-1\} &= \tfrac{P_{c1}}{W_0} & k &\in (0, W_0 - 1) & i &= n
\end{aligned}
\tag{1}
$$

From the transition probabilities and the Markov chain, we could derive the probability of reaching $b_{i,k}$. It is given in Eq. (2).

$$
b_{i,k} = \frac{1-(1-P_b)^{W_i-k}}{P_b}
\begin{cases}
\frac{1-P_{c2}}{W_0}\sum\limits_{i=0}^{i=n-1} b_{i,-2} + \frac{P_{c1}}{W_0}b_{n,-1} + \frac{1}{W_0}b_{n,-2} & k \in (0, W_0 - 1)\ i = 0 \\
\frac{P_{c2}}{W_i}(b_{i-1,-2}) + \frac{P_{c1}}{W_i}(b_{i-1,-1}) & k \in (0, W_i - 1)\ i = (1, m) \\
\frac{P_{c2}}{W_m}(b_{i-1,-2}) + \frac{P_{c1}}{W_m}(b_{i-1,-1}) & k \in (0, W_m - 1)\ i = (m+1, n)
\end{cases}
\tag{2}
$$

We could simplify Eq. (2) and derive each $b_{i,k}$ in terms of $b_{i,0}$ as shown in Eq. (3).

$$
b_{i,k} = \frac{1-(1-P_b)^{W_i-k}}{P_b}
\begin{cases}
\frac{(1-P_b)(1-P_{c1})}{W_0}\left((1-P_{c2})\sum\limits_{i=0}^{i=n-1} b_{i,0} + b_{n,0}\right) + \frac{(1-P_b)P_{c1}}{W_0}b_{n,0} & k \in (0, W_0 - 1)\ i = 0 \\
\frac{(1-P_b)(P_{c1}+(1-P_{c1})P_{c2})}{W_i}(b_{i-1,0}) & k \in (0, W_i - 1)\ i = (1, m) \\
\frac{(1-P_b)(P_{c1}+(1-P_{c1})P_{c2})}{W_m}(b_{i-1,0}) & k \in (0, W_m - 1)\ i = (m+1, n)
\end{cases}
\tag{3}
$$

Any state in the Markov chain could be reached from $b_{0,0}$. So, we further simplify each $b_{i,0}$ from Eq. (3) in terms of $b_{0,0}$. At the beginning, when a node wants to transmit a packet, the probability of reaching $b_{0,k}$ will be only $1/W_0$. From this view, we find the initial value of $b_{0,0}$ as shown in Eq. (4). For the subsequent iterations, $b_{0,0}$ is found by using Eqs. (5) and (6) in (3).

$$
b_{0,0} = \left(\frac{(1-(1-p_b)^{W_0})}{P_b W_o}\right)
\tag{4}
$$

The probability of reaching $b_{i,0}$ state for the stages from 1 to m is derived as shown in Eq. (5). From $m+1$th stage, the maximum value of back-off counter is fixed as 2^m probability of reaching $b_{i,0}$ for $m+1$th to nth stages as given in Eq. (6).

$$
b_{i,0} = \left(\prod_{j=1}^{j=i} \frac{(1-(1-p_b)^{2^j W_0})}{2^j W_o}\right) * \left(\frac{(1-P_b)(P_{c1}+(1-P_{c1})P_{c2})}{P_b}\right)^i * b_{0,0}\ \forall i = (1, m)
\tag{5}
$$

$$
b_{i,0} = \left(\prod_{j=1}^{j=m} \frac{(1-(1-P_b)^{2^j W_0})}{2^j W_o}\right) * \left(\frac{(1-(1-P_b)^{2^m W_0})}{2^m W_o}\right)^{i-m} \\
* \left(\frac{(1-P_b)(P_{c1}+(1-P_{c1})P_{c2})}{P_b}\right)^i * b_{0,0}\ \forall i = (m+1, n)
\tag{6}
$$

$b_{i,-1}$ and $b_{i,-2}$ can be derived in terms of $b_{0,0}$ using Eq. (7). $b_{i,-1}$ represents the state at which the node transmits the RTS packet. When the node reaches $b_{i,-2}$, it is ready to transmit the data packet. On successful transmission (without any collision), the node reaches the end and goes to the initial stage for transmission again. The generic form of $b_{i,-2}$ is shown in Eq. (8).

$$
b_{i,-1} = (1 - p_b)b_{i,0},\ i = (0, n)
\tag{7}
$$

$$
b_{i,-2} = (1 - p_b)(1 + (1 - p_{c1})b_{i,0},\ i = (0, n)
\tag{8}
$$

Successful transmission implies that the node has transmitted the data packet and received acknowledgement. The success probability of transmitting a packet is defined as the sum of success probability at each stage from 0 to n. It can be derived using Eq. (9).

$$
P_s = (1 - P_{c2}) * \sum_{i=0}^{i=n} b_{i,-2}
\tag{9}
$$

Collision drop could happen at $b_{i,-2}$. This type of data collision occurs due to the extended hidden terminals, which could not receive RTS/CTS packets. P_{c2} represents the collision due to such nodes. Collision probability of data packets can be derived using Eq. (10).

$$P_{CD} = P_{c2} * \sum_{i=0}^{i=n} b_{i,-2} \qquad (10)$$

Transmitter could overcome the collision by retransmitting the RTS or data packets. However, packet drop event occurs when the back-off stage reaches the maximum retransmission or retry count (short or long).

According to IEEE 802.11, the maximum limit for long and short retry count is 7 and 3, respectively. The packet drop could occur whenever the retransmission limit reaches either the long retry limit or the short retry limit. The maximum number of stages that the node goes through might be 10 (7 RTS and 3 data packet drops), and the minimum number of stages at which the packet drop could occur is 3 (continuous data packet drops—short retry limit). Packet drop probability due to long retry limit exceeding is given in Eq. (11) and packet drop probability due to short retry limit exceeding is given in Eq. (12).

$$P_{long} = P_{c1} * \sum_{i=7}^{i=10} b_{i,-1} \qquad (11)$$

$$P_{short} = P_{c2} * \sum_{i=3}^{i=10} b_{i,-2} \qquad (12)$$

Total packet drops due to retry limit exceeding are shown in Eq. (13).

$$P_{retrydrop} = P_{long} + P_{short} \qquad (13)$$

When NODE-n_i transmits, collision could happen to the RTS or CTS packet due to the nodes lying in either region 1 or region 2. Hence, the collision probability of RTS/CTS packets for NODE-n_i can be written as in Eq. (14).

$$P_{c1} = P_1 + P_2 \qquad (14)$$

P_1 represents the collision probability due to the terminals in region 1, which denotes the covered region, and hence, collision could happen only for RTS/CTS packets. While transmitting the data packets, nodes in covered region are prevented from transmission using virtual carrier sensing. P_1 can be calculated using Eq. (15).

$$P_1 = \sum_{j \in N(i)} x_i * x_j \qquad (15)$$

where x_i is the self-busy probability of NODE-n_i. Self-busy probability of NODE-n_i is the ratio of time interval for which NODE-n_i gets involved in transmission out of the total time interval. $N(i)$ represents the set of nodes in the covered region or the nodes that are reachable to either the sender or receiver of the transmission. $H(i)$ represents the set of nodes in the uncovered region which contend with i to occupy the medium.

P_2 represents the collision probability that occurs due to interfering nodes which may be in region 2 named uncovered region. Nodes in this region cannot receive the RTS/CTS packets and hence lack virtual carrier sensing. Collisions due to uncovered region have been the major reason behind the performance anomalies happening over multi-hop ad hoc networks. P_2 can be found using Eq. (16):

$$P_2 = \sum_{\substack{j \in H(i) \\ j \in H(R(i)) \\ j \notin H(i,R(i))}} x_i * x_j \qquad (16)$$

where $H(i)$ represents the set of hidden terminals of NODE-n_i. $R(i)$ represents the receiver of NODE-n_i, i.e., NODE-n_{i+1}. P_2 is defined as the collisions happening among NODE-n_i and its hidden terminals and collisions caused by the hidden terminals of receiver node of n_i.

Data transmission follows RTS/CTS transmission. Data transmission means that RTS and CTS have been successfully transmitted. It means that nodes in the covered region are well informed about the data transmission through NAV. Now, data collision could happen only due to the nodes lying in the uncovered region. We assume that collision occurs to the data only due to uncovered terminals. So, data collision probability P_{c2} is calculated only using P_2 as shown in Eq. (17).

$$P_{c2} = P_2 \qquad (17)$$

Busy probability P_b of the medium for a node is defined as the probability that at least one of the contending node is involved in transmission. Xi is transmission probability of NODE-n_i

$$P_b = \sum_{j \in N(i), H(i)} x_i \qquad (18)$$

4 Performance evaluation

We evaluate the performance of IEEE 802.11 DCF over multi-hop ad hoc networks for a varying number of nodes against Bianch model and ns-2.35 simulation. IEEE 802.11 FHSS has been taken for validation as shown in Table 1. Per-hop throughput is shown in Fig. 4 for varying number of nodes. Throughput in Bianchi model is

Table 1 System parameters

|	
Packet payload	1023 bytes
MAC header	34 bytes
PHY header	16 bytes
ACK length	30 bytes
RTS length	36 bytes
CTS length	30 bytes
Channel bit rate	1 Mbps
Propagation delay	1 μs
SIFS	28 μs
Slot time	50 μs
DIFS	128 μs
CWmin (slots)	32
CWmax (slots)	1024
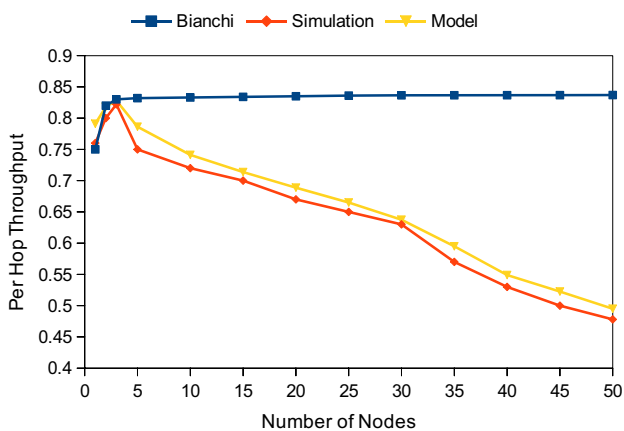
Fig. 4 Per-hop throughput

uniform due to the absence of hidden terminal. Moreover, Bianchi model assumes that the medium is always ideal, which is impossible. In reality, throughput rapidly

decreases when the number of nodes increases. Simulation result resembles with that of our model. The larger number of nodes leads to increase in hidden and extended hidden terminals, thereby reducing the throughput that is depicted in Fig. 4.

Per-hop throughput at each back-off stage is shown in Fig. 5. An increase in the number of nodes reduces the per-hop throughput due to the share with other nodes. The throughput smoothly decreases with an increase in the number of nodes. We can note the throughput is almost the same for smaller network and also the throughput for later back-off stage is high comparing earlier back-off stage. Overall collision probability for different back-off stages is shown in Fig. 6. Because of the larger contention window size, the collision probability for later back-off stages is less in comparison to the earlier back-off stages ($m = 1, 2, 3$). The number of nodes in uncovered region plays a major role in the performance of static multi-hop ad hoc networks, which is clearly depicted in Fig. 6.

Increase in collision drops creates frequent link failure even though there is no mobility. Link failure increases the control overhead drastically by route re-discovery. When the number of retransmission exceeds the limit, the event is interpreted as link failure. The link failure also leads to data packet drops and end-to-end retransmission. The probability of link failure increases with respect to the number of nodes. Bianchi model results in reduced link failure probability due to the absence of hidden terminals. Our model validates the simulation results closely as shown in Fig. 7. The average packet transmission probability of the node is shown in Fig. 8. It shows that transmission probability smoothly decreases when the number of hidden nodes increases, and during the initial back-off stage, transmission probability is more compared to later stages.
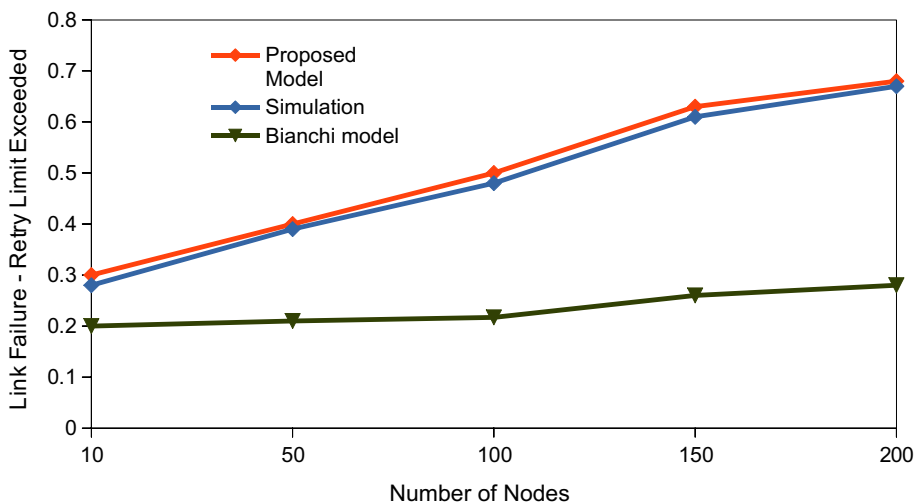
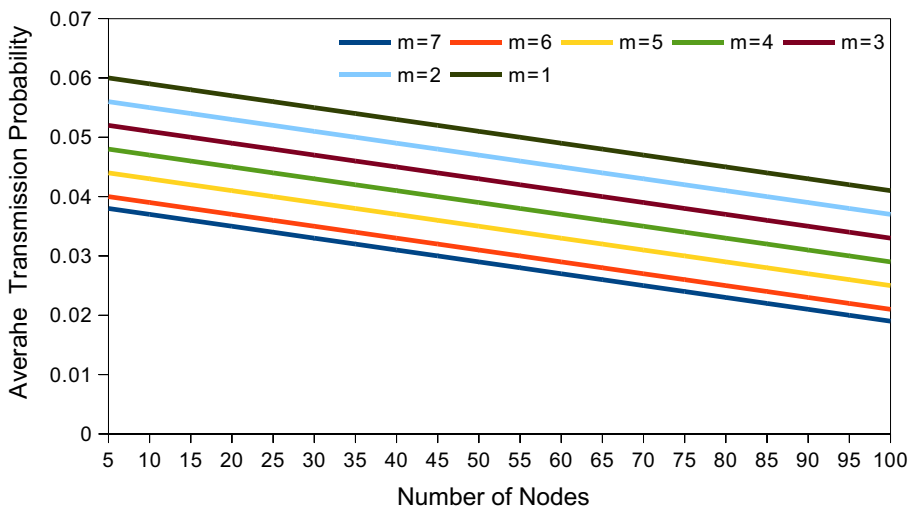**Fig. 5** Per-hop throughput for varying back-off stages
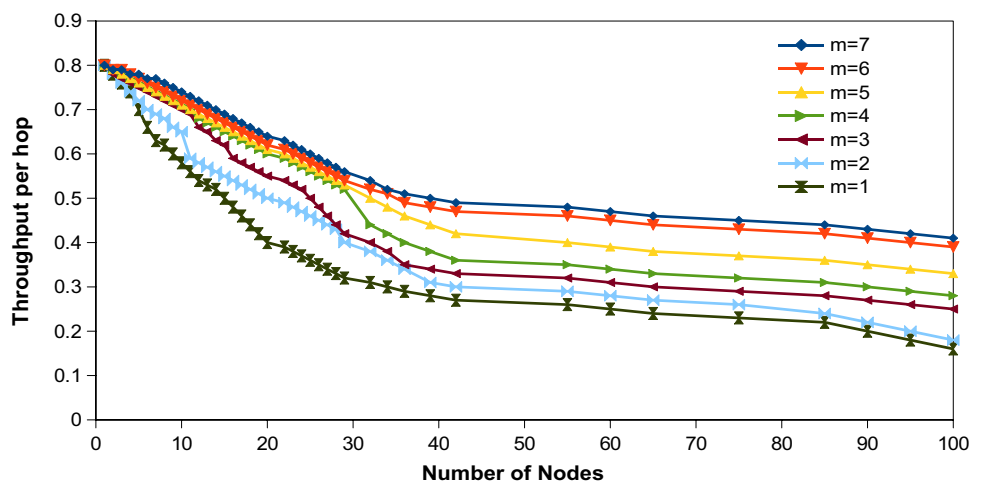
Fig. 6 Collision probability for varying back-off stages
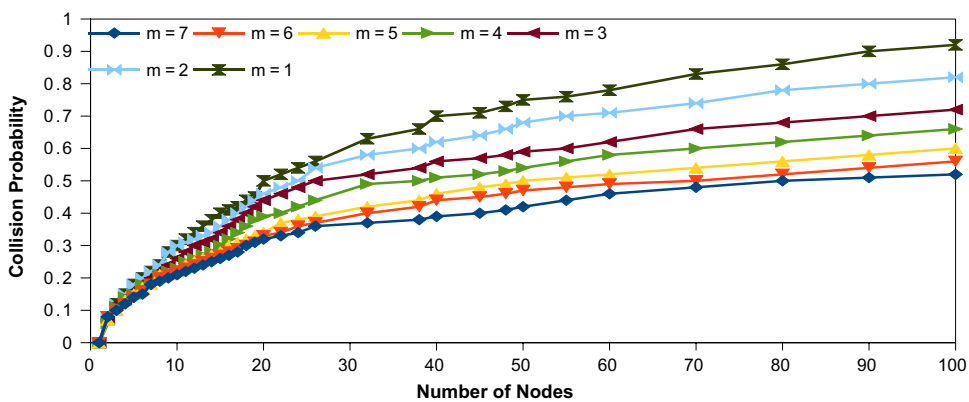
Fig. 7 Packet drop probability

Fig. 8 Average packet transmission probability

5 Conclusion

Analytical models play an essential role in performance computation and protocol optimization. Many models exist to evaluate collision probability, throughput and end-to-end delay. Those models are generally limited to single-hop ad hoc networks. They do not consider the presence of extended hidden terminals in multi-hop ad hoc networks.

This paper presents an analytical model to find throughput, collision probability and link failure probability for IEEE 802.11 RTS/CTS in the presence of extended hidden terminals. We analysed the per-hop throughput and collision probability at various back-off stages. We validated the link failure probability against ns-2.35 simulation for varying number of network sizes with number of nodes 10, 50, 100, 150 and 200 and thus proved that the results match closely with simulation. This model can be used to find out the route failure by using short and long retry limit probability. End-to-end delay could be derived by incorporating appropriate delay along with the corresponding probability values. End-to-end route failure can be derived by using the link failures happening in the end-to-end path. Our future work will be done based on these factors.

Compliance with Ethical Standards

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Xu K, Gerla M, Bae S, (2002), How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks. In: Global telecommunications conference, GLOBECOM. IEEE, vol 1, no. 1, pp72–76 doi: 10.1109/GLOCOM.2002.118804
2. Bianchi G (2000) Performance analysis of the IEEE 802.11 distributed coordination unction. IEEE J Sel Areas Commun 18(3):535–547
3. Wu H, Peng Y, Long K, Cheng, S Ma J (2002), Performance of reliable transports protocol over IEEE 802.11 wireless LAN: analysis and enhancement. In: Proc. IEEE INFOCOM, vol 2, pp 599–607
4. Chatzimisios P, Boucouvalas A, Vitsas V (2003) IEEE 802.11 packet delay—a finite retry limit analysis. In: Proc. IEEE GLOBECOM, vol 2, pp 950–954
5. Zhang L, Shu Y, Yang O, Wang G (2006) Study of medium access delay in IEEE 802.11 wireless networks. Commun IEICE Trans 89:1284–1293
6. Xiao Y (2005) Performance analysis of priority schemes for IEEE 802.11 and IEEE 802.11e wireless LANs. IEEE Trans Wireless Commun 4:1506–1515
7. Malone D, Duffy K, Leith D (2007) Modeling the 802.11 distributed coordination function in nonsaturated heterogeneous conditions. IEEE/ACM Trans Netw 15(1):159–17
8. Ng PC, Liew SC (2007) Throughput analysis of IEEE802.11 multi-hop ad hoc networks. IEEE/ACM Trans Netw (ToN) 15(2):309–322
9. Garetto M, Salonidis T, Knightly EW, (2006) Modeling per-flow throughput and capturing starvation in CSMA multi-hop wireless networks. In: INFOCOM
10. Liew SC, Kai CH, Leung HC, Wong P (2010) Back-of-the- envelope computation of throughput distributions in CSMA wireless networks. IEEE Trans Mob Comput 9(9):1319–1331
11. Chatzimisios P, Boucouvalas AC, Vitsas V (2003) Packet delay analysis of IEEE 802.11 MACprotocol. Electron Lett 39(18):1358–1359
12. Chatzimisios P, Vitsas V, Boucouvalas AC (2002) Throughput and delay analysis of IEEE 802.11 protocol. In: Proceedings of 2002 IEEE 5th international workshop on networked appliances, IEEE, Liverpool, pp 168–174
13. Hadzi-Velkov Z, Spasenovski B (2003) Saturation throughput-delay analysis of IEEE 802.11 DCF in fading channel. In: IEEE international conference on communications ICC'03, vol 1, pp 121–126
14. Yeo J, Agrawala A (2003) Packet error model for the IEEE 802.11 MAC protocol. In: 14th IEEE proceedings on personal, indoor and mobile radio communications PIMRC 2003, vol 2, IEEE, pp 1722–1726
15. Carvalho MM, Garcia-Luna-Aceves JJ (2003) Delay analysis of IEEE 802.11 in single-hop networks. In: Proceedings on 11th IEEE international conference on network protocols, IEEE, pp146–155
16. Khalaf R, Rubin I (2006) Throughput and delay analysis in single hop and multihop IEEE 802.11 networks. In: 3rd international conference on broadband communications, networks and systems, BROADNETS 2006, IEEE, pp 1–9
17. Alizadeh-Shabdiz F, Subramaniam S (2006) Analytical models for single-hop and multi-hop ad hoc networks. Mobile Netw Appl 11(1):75–90
18. Khalaf R, Rubin I, Hsu J (2007) Throughput and delay analysis of multihop IEEE 802.11 networks with capture. In: IEEE international conference on communications, ICC'07, IEEE, pp 3787–3792
19. Siripongwutikorn P (2006) Throughput analysis of an IEEE 802.1 lb multihop ad hoc network. In: IEEE region 10 conference on TENCON 2006, IEEE, pp 1–4.
20. Siris VA, Stamatakis G, Tragos E (2011) A simple end-to-end throughput model for 802.11 multi-radio multi-rate wireless mesh networks. IEEE Commun Lett 15(6):635–637
21. Wang Y, Garcia-Luna-Aceves JJ (2002) Collision avoidance in multi-hop ad hoc networks. In: Proceedings of 10th IEEE international symposium on modeling, analysis and simulation of computer and telecommunications systems, MASCOTS 2002, IEEE, pp 145–154
22. Wang Y, Garcia-Luna-Aceves JJ (2004) Modeling of collision avoidance protocols in single-channel multihop wireless networks. Wireless Netw 10(5):495–506
23. Fu J, Zhou Z, Zheng L, Wang J, Li X (2011) Throughput analysis of IEEE 802.11 DCF in presence of hidden nodes. In: 2011 International conference on multimedia technology (ICMT), IEEE, pp 920–922
24. Jeong J, Kim H, Lee T, Shin J (2010) An analysis of hidden node problem in IEEE 802.11 multihop networks. In: 2010 Sixth international conference on networked computing and advanced information management (NCM), IEEE, pp 282–285

25. Lee J, Yeom I (2009) Avoiding collision with hidden nodes in IEEE 802.11 wireless networks. IEEE Commun Lett 13(10), 743–745.

26. Buratti C, Verdone R (2017) End-to-end throughput of Ad Hoc multi-hop networks in a poisson field of interferers. IEEE/ACM Trans Netw 25(5):3189–3202. https://doi.org/10.1109/TNET.2017.2729165

27. Ahsen M, Hassan SA, Jayakody DNK (2016) Propagation modeling in large-scale cooperative multi-hop ad hoc networks. In: IEEE Access.

28. Abdulhadi S, Jaseemuddin M, Anpalagan A (2014) On the throughput capacity of cooperative multi-hop wireless Ad hoc networks with multi-flow. Wireless Pers Commun 79(1):629–646. https://doi.org/10.1007/s11277-014-1877-x

29. Murad M, Eltawil AM (2018) Collision tolerance and throughput gain in full-duplex IEEE 802.11 DCF. In: 2018 IEEE international conference on communications (ICC), Kansas City, MO, pp 1–6, https://doi.org/10.1109/ICC.2018.8422695

30. Medina-Marin L, Parra-Michel R, Orozco-Lugo AG, Lara M (2018) Analysis of packet arrival model for 802.11 protocol under hidden terminals and asynchronous MPR detection. In: 2018 IEEE 9th Latin American symposium on circuits and systems, pp 1–4.