Performance Evaluation of IEEE 802.11 DCF in Wireless Multi-hop Ad-hoc Networks

Keyur N Upadhyay  
Computer Engineering Department  
B.V.M Engineering College  
V.V.Nagar, India  
mailtokeyur@gmail.com

Mayur M Vegad  
Computer Engineering Department  
B.V.M Engineering College  
V.V.Nagar, India  
mayurmvegad@yahoo.com

Tejas M Vasavada  
Information Technology Department  
A.D.Patel Institute of Technology  
V.V.Nagar, India  
tejas_m_vasavada@yahoo.co.in

Abstract—IEEE 802.11 is widely adopted protocol for wireless network currently. Despite its several drawbacks the distributed coordination function of IEEE 802.11 has been a primary choice for many wireless ad hoc networks. In this paper we studied the performance of this protocol under various scenarios including a couple of regular and random topologies. We have chosen per flow throughput, packet corruption ratio, and end-to-end delay as our performance metrics. We use ns-2 as the simulation tool. In regular scenario we had chosen inter node distance and number of hops and for random scenario we had chosen number of flows as the running parameters.

Keywords—IEEE 802.11, medium access control, distributed coordination function.

I. INTRODUCTION

The IEEE 802.11 [1] is the most popular standard for Wireless Local-Area Networks (WLANs) and wireless ad-hoc networks. In the first CSMA/CA based standard [1] which is known as 802.11, IEEE defines a MAC layer and three physical (PHY) layers at the 2.4 GHz band: Infrared, FHSS (frequency hopping spread spectrum) and DSSS (direct-sequence spread spectrum). At the medium access layer, two MAC access methods are specified: a mandatory distributed coordination function (DCF) and an optional point coordination function (PCF). DCF is a contention based protocol and PCF is contention free protocol needing a central access point for the medium access control. In our current work the focus is on wireless ad hoc networks we focus our evaluation only on DCF.

In the DCF, a station wishing to transmit first listens to the channel. If the channel is sensed “idle” for a time DIFS (distributed inter-frame space) then the station begins a random backoff [1]. If the channel is sensed “busy” at any time during the backoff, the backoff is paused until the channel is sensed idle for DIFS period and the backoff is again resumed. The station transmits its pending frame when its backoff timer expires.

On transmitting a data frame, if this frame is received correctly, the receiver sends back an ACK frame after a short inter-frame space (SIFS) period. There are two requirements on the duration of SIFS. First, the duration should be long enough to ensure that the physical (PHY) layer of the receiver can turn itself from receiving to transmitting state. Second, SIFS should be shorter than DIFS so that an ACK frame can be sent before other stations resume their backoff. In the DCF scheme, DIFS is equal to SIFS plus two idle slots.

Contention based protocols are the mainstream MAC protocols for distributed and self-organized wireless networks since in such networks the infrastructure is usually not present and there is no clear separation between the roles of access points and client stations. The support of contention based DCF also made IEEE 802.11 based equipments popular choices for various wireless ad hoc networks.

Most of the contention based MAC protocols, including the IEEE 802.11 DCF, are based on Carrier Sense Multiple Access (CSMA). In CSMA, a station may transmit if and only if the medium is sensed to be idle. The reason is to avoid this station causing interference to the current ongoing transmission sensed on the medium. In addition to basic CSMA, the DCF also incorporates acknowledgement signals and a back-off mechanism.

Besides the two-way (Data-ACK) basic access scheme described above, DCF also includes an optional RTS/CTS access scheme also known as virtual carrier sensing scheme. In this, each Data frame transmission is preceded by an exchange of small RTS/CTS frames between the sender and the receiver. This not only helps reduce the duration of collision but also helps in reserving the medium for the subsequent Data-ACK transfer. Further, it also mitigates the hidden terminals problem substantially.

The IEEE 802.11 DCF is known to be non-efficient in shared channel use due to its over-cautious approach towards assessing the possibility of causing interference. In particular, a station simply blocks its own transmission when it senses the medium is busy, or it receives a channel reservation message sent by any other station. However in many cases this channel assessing station’s own transmission may not introduce enough signal energy to disturb the on-going transmission at its receiver. This problem is also known as exposed terminals problem. In this paper we study DCF by evaluating its performance in wireless ad-hoc networks under different scenarios including some regular and random topologies.

The rest of the paper is organized as follows. In Section II we discuss different scenarios that we have considered for the evaluation. Section III elaborates the simulation set ups and
describes the obtained results. Finally, Section IV concludes the paper.

II. TOPOLOGY DESCRIPTION

In this section we describe the different scenarios we undertook for the evaluation purpose. The topologies we studied consist of followings:

1. Non-random scenario
2. Random scenario

A. Non random scenario

Under non random scenario we evaluated two kinds of topologies: a regular chain topology and a parallel chain topology.

In regular chain topology we had only one flow between two extreme nodes as shown in Fig. 1, where as in parallel chain topology we set up two flows as shown in Fig. 2.

Fig. 1. Regular chain topology with 130m < ds < 250 m. Here, ds is the inter node distance.

Regular chain topology: In regular chain topology (Fig.1.) we kept 6 to 16 nodes placed at uniform distance ds in a chain manner. We varied ds from 130m to 250m. We performed our study based on mainly two running parameters: inter node distance and no. of hops involved in the flow. The flow had an FTP connection using TCP as the transport layer protocol between the two extreme nodes.

![Regular Chain Topology Diagram](image)

Fig. 2. Parallel chain topology with 130m < ds < 250 m. Here, ds is the inter node distance and ifdst is the inter flow distance. ifdst = 200 meters

Parallel chain topology: as shown in Fig. 2, for parallel chain topology we kept total number of 12 nodes making two parallel flows having 5 hops each. The distance between the two flows was kept 200 meters. In each flow we set up an FTP connection over TCP between two extreme nodes of the respective chain. Number of seeds (used for the backoff initialization) for both the non-random cases are 30 and the simulation was run for 100 seconds.

B. Random scenario

Topological area chosen for random topology was 600 × 600 and total 50 nodes were deployed with uniform distribution. Unlike other two topologies in non-random scenarios, in random scenario we set number of flows as the running parameter. For each flow, the source and the destination was chosen randomly. Hence, the number of hops in each flow for each simulation run was also random. To have a reliable average result we run simulation for 50 seeds for each point. The simulation time for this random scenario is 50 Seconds.

III. SIMULATION RESULTS

We chose ns-2 (ver. 2.33) [5] for our simulation. We considered two regular topologies and one random topology for our experiments. In regular two variants chain and parallel chain were simulated. Our evaluation focused throughput at transport layer, end-to-end delay and corruption ratio of packets at transport layer. Average of all these are considered in most of results. We also measured per flow throughput in chain and parallel chain. An Average delay is considered for in both regular topologies.

All simulations were done at 1Mbps data rate. Two ray propagation model was used. We kept TCP packet size to 1000 bytes. The transmission range and carrier sensing range are 250 meters and 550 meters, respectively. AODV is chosen as underlying routing protocol. In all experiments, the errors were assumed to be caused due to MAC collisions only.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS-2</td>
<td>Version 2.33</td>
</tr>
<tr>
<td>Data rate</td>
<td>1 Mbps</td>
</tr>
<tr>
<td>Propagation model</td>
<td>Two ray ground</td>
</tr>
<tr>
<td>Transmission range</td>
<td>250 meters</td>
</tr>
<tr>
<td>Carrier sensing range</td>
<td>550 meters</td>
</tr>
<tr>
<td>Routing protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Transport protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Packet size</td>
<td>1000 bytes</td>
</tr>
<tr>
<td>Simulation time</td>
<td>100 seconds (non-random scenario) 50 seconds (random scenario)</td>
</tr>
<tr>
<td>Number of seeds</td>
<td>30 seeds (non-random scenario) 50 seeds (random scenario)</td>
</tr>
</tbody>
</table>

A. Regular chain topology (single-TCP flow)

The simulation time for regular topology was 100 seconds and the experiments of regular topologies were repeated 30 times, each with seed value 30 used to vary the selection of backoff initializations at each node. A single TCP flow was set between the two extreme nodes of chain. In regular chain topology we evaluated two kind of analysis, one is based on inter nodal distance between the nodes participating in the chain and other is for different number of hops along the flow.
The plots in Fig. 3 shows throughput and packet corruption ratio at different inter nodal distances. Similarly plots in Fig. 4 shows average delay at different inter nodal distances.

Fig.3: Per flow throughput & PCR Vs inter node distance for regular chain topology

Fig.4: Average delays Vs inter node distance for regular chain topology

Now as such inter node distance wise analysis, we also studied the number of hop wise analysis and measured the impact of throughput and average delay based on that observation.

The plot in Fig. 5 depicts impact of number of hops on throughput, i.e. throughput decreases as number of hops increases. As observed, the evaluation was carried out at three representative values of ds: 130m, 170m, and 230m. Fig. 6 shows the plots of end-to-end delay with number of hops for different values of ds.

Fig.5: Per flow throughput Vs number of hops for regular chain topology

Fig.6: Average delay Vs number of hops for regular chain topology

These above plots shown in Fig.5 and Fig.6 clearly indicate the effect of number of hops on throughput and average delay.

B. Regular parallel chain topology (two-TCP flows)

In parallel chain topology, the simulation time, number of seeds and other simulation parameters were similar as in single chain topology. However, here numbers of TCP flows are two as shown in Fig. 2. In this experiment we kept number of hops fixed to 5 (6 nodes in each flow). Again, we varied the inter nodal distance and we lead our observation by vary the inter nodal distances between nodes and measure the end-to-end throughput and delay for each flow. We also calculate the Jain's Fairness Index (JFI) and plot it.

The plots in Fig. 7 shows throughput and Jain fair index for different inter nodal distances. Similarly plots in Fig. 8 show average delay at different inter nodal distances. We see that at higher inter nodal distance has slightly degraded the fairness. Comparing the per-flow throughput of parallel chain (~8Kbps) with that of the single chain (~17Kbps), it is clear that the presence of other flow has decreased the MAC performance severely.

Fig.7: Average throughput & JFI Vs inter node distance for parallel chain topology
C. Random Scenario

The simulation time for random topology is 50 seconds and each point is an average of total 50 runs, each with a different seed for the random deployment of nodes and the random selection of sender-receiver pairs for the flows involved. We varied number of flows from 1 to 11 and measured the end-to-end throughput, delay and packet corruption ratio.

The plots in Fig.9 show the impact of number of flows on per flow throughput and packet corruption ratio for random scenario.

The plots shown in Fig.10 depict average delay Vs number of flows.

IV. FUTURE WORK

The term “capture effect” refers to phenomenon by which receiver is able to recover one of such overlapping frame successfully, as long as signal-to-interference ratio is above a minimal acceptable threshold. Applicability of “capture effect” in IEEE 802.11 based wireless network has also been experimentally studied [2], [3] and it is found that the capture behavior is differential based on the arrival of the frame of interest which we referred as differential capture capability (DCC) of receiver [4].

In our future work we aim to compare the performance of different MAC protocols (including the standard 802.11 DCF) assuming DCC at PHY.

REFERENCES

5. www.isi.edu.edu/nsnam/ns/