

Performance analysis of Wireless MAC Protocols using a Search based Framework*

Shamim Begum
Department of Electrical Engineering
University of Southern California
Email: sbegum@usc.edu

Ahmed Helmy
Department of CISE
University of Florida, Gainesville
Email: helmy@cise.ufl.edu

Sandeep Gupta
Department of Electrical Engineering
University of Southern California
Email: sandeep@poisson.usc.edu

Abstract—Previously, we have developed a framework to perform systematic analysis of CSMA/CA based wireless MAC protocols. The framework first identifies protocol states that meet our study objective of minimizing a given performance metric. It then applies search techniques and heuristics to construct sequences of protocol events in a given topology that satisfy our objective. In this paper, we demonstrate that our framework can easily be extended to evaluate performance of new protocols by evaluating two completely different variants, namely MAC protocols for (i) quality of service (QoS), and (ii) power control. In each case, we identify previously unknown problems with the protocol. In particular, we generate scenarios where throughput of a lower priority class can be as high as 5 times compared to the throughput of a higher priority class, thus contradicting the basic notion of QoS.

Traditional performance evaluation approaches typically evaluate average performance but do not capture the worst cases, nor do they expose the protocol breaking points. Thus this paper demonstrates the usefulness of a systematic approach in evaluating the protocol breaking points.

I. INTRODUCTION

A wireless adhoc network may be used when a fixed communication infrastructure, wired or wireless, does not exist or has been destroyed. The goal of such a network is to allow a group of communicating nodes to setup and maintain connections among themselves without the support of a base station. Sharing a limited communication bandwidth efficiently among all nodes in the network is the main objective of wireless MAC protocols. MAC protocols must also exercise power control as wireless hosts have a limited amount of energy [17]. To support real time applications, e.g., voice and video, MAC protocols must provide quality of service (QoS) [16]. Minimum guarantees in terms of connectivity, throughput, or service are required by mission critical applications, e.g., military, crisis response, and security applications. Evaluating the worst case performance is very important to avoid mission failures in such applications. Providing a systematic approach for evaluating the worst case performance of a broad class of MAC protocols motivates this work.

Test generation (TG) is mainly based on search techniques that search for valid sequences of protocol events that expose weaknesses in the design of a protocol. Traditional test generation approaches target verification and are based on

forward search methods where the entire search space is exhaustively searched for test scenarios [1], [2]. Formal verification approaches use high-level system description languages to model and to analyze network protocols [3], [4], and involve determining the set of all reachable states of the models.

Previously, we developed a framework for evaluation of worst case performance of basic CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) protocols as presented in our technical report [10]. Instead of adopting the validation approach, our framework uses a *falsification approach* and directly targets the protocol conditions that adversely effect the protocol performance. The main formalism we used is that of a finite state machine (FSM) that represents state transition rules of the protocol under study. Given a performance metric of the protocol and a network topology, the framework uses search techniques to generate network scenarios leading to the worst case performance. It uses deterministic techniques and heuristics that often make it possible to generate the worst-case scenario in practical run times. Using the framework, previously we evaluated worst performance of IEEE 802.11b [5] networks by generating scenarios that lead to the reduction of throughput upto 89.7% [10].

In this work, we demonstrate that it is easy to extend the above basic framework to carry out performance analysis of variations of CSMA/CA protocols that consider QoS and power control. Using the extended framework, we perform a systematic analysis of protocols that use priority based schemes to provide QoS [12] and transmission power control (TPC) based schemes for power control [17], [18], [19], [20]. In this paper, we present case studies on IEEE 802.11e [12] and basic TPC [17]. In each case, we validate our findings by performing ns-2 [11] simulations for the scenarios generated by our extended framework. We generate scenarios where the throughput of a lower priority class can be as high as 5 times compared to the throughput of a higher priority class. This contradicts the basic notion of QoS and specifically disproves the results of the studies that report that a lower priority class *always* achieves lower throughput compared to a higher priority class [13], [14], [15], [16]. Among these studies, [16] shows that lower priority class has throughput about 1/3 compared to the throughput of a higher priority class [16]. Using the insights gained from our systematic protocol analysis, we identify potential modifications for both

*This research was supported by NSF and NASA.

the protocols. Our initial analysis shows the promise of these modifications. Complete evaluation of the modified versions of these protocols is a subject of our ongoing research.

This paper has two main objectives. First, we demonstrate that our previously developed framework is general and can easily be extended to evaluate new protocols. Second, we evaluate the worst case performance of variations of CSMA/CA protocols for QoS and power control, and identify previously unknown problems in the design of these protocols. We also illustrate how the scenarios generated by our approach provide insights into potential modifications of the protocol.

The rest of the paper is organized as follows. Section II presents related work. Section III provides a brief overview of our prior performance evaluation framework. Section IV presents the extension of that framework for performance analysis of CSMA/CA based MAC protocols as well as the results of the analysis. Section V concludes the paper with a brief outline of our future work.

II. RELATED WORK

The primary objective of this work is to demonstrate the extendibility of the basic framework presented in our technical report [10]. We extend the framework to study CSMA/CA protocols for QoS and power control. The main contributions of this work are as follows.

- (1) We propose modifications to the underlying FSM model to incorporate the study of a broader class of protocols.
- (2) We develop new heuristics to generate worst case scenarios for these protocols.
- (3) We derive insights from our performance analysis to systematically improve protocols and hence utilize the framework in the domain of protocol design and modification.

There is a large body of literature that studies IEEE 802.11x protocols [6], [7], [13], [16]. These works provide keen insights for the average case analysis. However, to our knowledge, no approach has identified protocol breaking points using systematic analysis as we do in this paper. We perform analysis on the case studies of CSMA/CA protocols for quality of service and power control. IEEE 802.11e [12] is an industry standard that is an extension of the legacy 802.11b to provide quality of service. [13], [14], [15] show that the protocol provides quality of service by assuring that the higher priority class achieves more throughput compared to a lower priority class. [16] shows analytically and via simulations that the throughput of a higher priority class is 3 times compared to the throughput of a lower priority class. We extend our framework and use it to generate scenarios in which a lower priority class achieves more throughput compared to a higher priority class in IEEE 802.11e networks. Thus our results contradict the basic notion of QoS by exposing, for the first time, the breaking points of the IEEE 802.11e protocol. We also extend the framework to analyze protocols for transmission power control (TPC). A significant amount of previous work [12], [17], [18], [19], [20] has identified various issues with the basic TPC protocols. However, to the best of our knowledge, the results and issues regarding throughput and fairness that

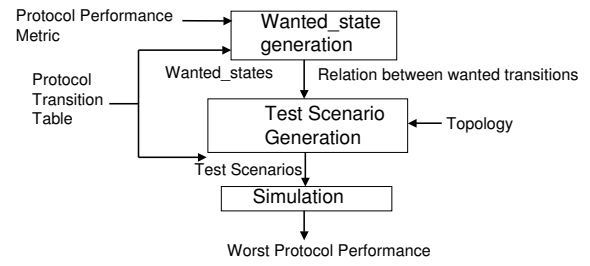


Fig. 1. An overview of our framework.

we have identified have not been identified by any previous work.

III. FRAMEWORK OVERVIEW

Given a wireless MAC protocol, our goal is to evaluate the worst case performance of the protocol with respect to a given set of protocol performance metrics. Figure 1 presents the block diagram of our proposed framework. Inputs to the framework are: (1) the protocol model, (2) a network topology, and (3) a protocol performance metric. The framework uses two main algorithms: (1) wanted_states generation, and (2) test scenario generation, to generate the worst case scenario with respect to the given performance metric for the given topology. It then simulates the test scenarios using a simulation framework and outputs the worst case performance for the given metric.

Given a protocol performance metric, it first transforms the performance metric in a form that reflects our study objective. For example, given throughput, it transforms it into a set of **wanted_states** that it minimizes or maximizes in later steps in order to generate scenarios that lead to minimum throughput in a given topology. The wanted_states generation algorithm transforms the protocol performance objective into wanted_states. Second, given a set of wanted_states and a topology, the test generation algorithm generates scenarios that maximize or minimize the study objective, which in turn, minimizes (or maximizes) the given protocol performance metric. The test scenarios are then simulated in a simulation environment to estimate the actual performance provided by the test scenarios. Using an example, Sections III-A and III-B respectively present a brief overview of models and algorithms of the basic framework. For details, see our technical report [10].

A. Basic models

Let us consider a toy protocol \mathbf{P} and a 4-node chain topology in which our objective is to generate scenarios that lead to the worst case throughput at a node. Throughput is defined as the fraction of time the channel is used to successfully transmit payload bits [6]. Let ρ be the amount of payload (data) successfully transmitted in time γ , then **throughput** is defined as:

$$0 \text{ --- } 1 \text{ --- } 2 \text{ --- } 3$$

$$G = \{ G_0 = \{1\}, G_1 = \{0, 2\}, G_2 = \{1, 3\}, G_3 = \{2\} \}$$

Fig. 2. Model of network topology.

Necessary transitions (Increase throughput)				
	Start state	Input event	End state	Output event
1	Idle	Packet	Transmit	RTS Transmit, RTS Receive
2	Transmit	End of RTS	WCTS	Start WCTS timer
3	Idle	RTS Recv start	Receive	
4	Receive	RTS Recv end	Transmit	CTS Transmit, CTS Receive
5	WCTS	CTS Recv start	WCTS & Receive	
6	WCTS & Receive	CTS Recv end	Transmit	Data Transmit, Data Receive
7	Idle	RTS overhear start	Receive	
8	Receive	RTS overhear end	Defer	Start Defer timer
9	WCTS	WCTS timer expire	Backoff	Start Backoff timer
10	Receive	RTS Recv start	Collision	Start Backoff time
11	Backoff	Backoff timer expire	Transmit	RTS Transmit, RTS Receive

Fig. 3. Transition table of protocol P.

$$throughput = \rho/\gamma. \quad (1)$$

Topology is modeled in terms of transmission range of each node in the network. Transmission range of node i is a set G_i containing the nodes who hear its transmission. Figure 2 represents a wireless network of 4 nodes where $G_0 = \{1\}$, $G_1 = \{0, 2\}$, $G_2 = \{1, 3\}$, and $G_3 = \{2\}$. Figure 3 presents a finite state machine model or the transition table of **protocol P**. Each row of the transition table represents a state transition of a node running the protocol. The protocol works as follows: upon receiving a packet from higher layer for node j , node i transmits an *RTS* destined for node j , schedules a *WCTS* (Wait-for-CTS) timer to wait for the *CTS* from j . Upon receiving the *RTS* destined for it, node j transmits a *CTS* (Clear-To-Send)

Wanted transition (Reduce throughput)	Wanted states	
	Transmitter	Receiver
Unsuccessful RTS	Backoff (BO)	Collision (COL)
Unsuccessful CTS	COL	BO
Unsuccessful Data	BO	COL
Silent drop of RTS	BO	Defer

Fig. 4. Generation of wanted_states.

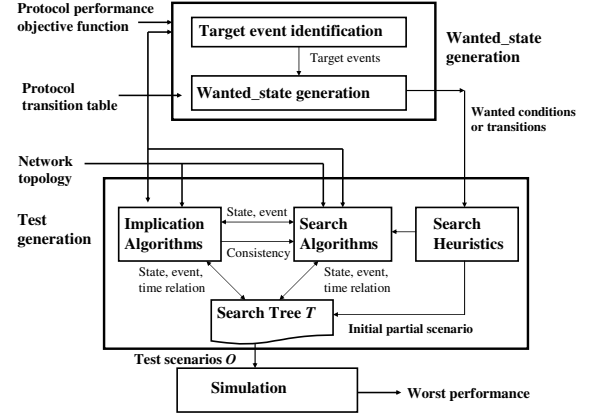


Fig. 5. Detail components of our framework.

to node i . On overhearing the *RTS*, a node k defers access to the channel by scheduling a timer. If node i receives the *CTS* from j before its *WCTS* timer expires, it goes to *Transmit* state to transmit the data, otherwise, it goes to *Backoff* state after which it retransmits the *RTS*. Row 1 of the table presented in Figure 3 states the following transition. When a node in *Idle* state receives a *Packet* from higher layer, it changes to *Transmit* state and triggers *RTS Transmit* and *RTS Receive* events.

B. Main algorithms

Given a metric, such as throughput, our objective is to generate scenarios that lead to the worst case value for the metric. We achieve this objective using the following steps. Given throughput, we first transform it into a protocol condition that we maximize in later steps in order to generate scenarios that lead to minimum throughput in a given topology. We refer the conditions that meet our study objective as **wanted_states**. **Wanted_states generation** procedure used in our framework is presented in Figure 5. This procedure transforms the protocol performance objective into wanted_states. Given a set of wanted_states and a topology, the **test generation algorithm** in Figure 5 generates scenarios that maximize our study objective, which in turn, minimize throughput in the given topology.

Wanted_states generation: The wanted_states generation algorithm first identifies *Data Receive* as the **target event** based on ρ and γ in Equation 1. Note that the target event *Data Receive* is output in row 6 of the transition table presented in Figure 3. The algorithm then uses a backward search technique to generate the transitions necessary (rows 6, 4, and 1 in the figure) to trigger the target event. Note that the transitions necessary to trigger the *Data Receive* event nullifies our study objective (instead of meeting the objective). Starting from these transitions, the algorithm then applies a forward search technique to generate **wanted_transitions**.

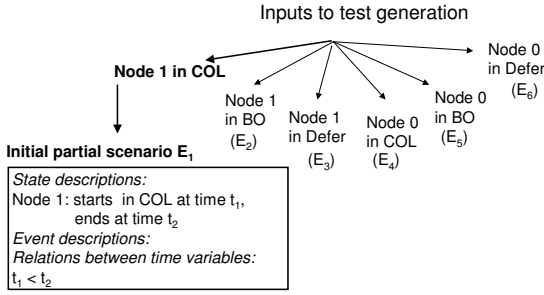


Fig. 6. Constructing initial partial scenario without heuristics.

Any of these wanted transitions is sufficient to generate a condition that meet our study objective. Figure 4 presents the wanted_states, e.g., *BO*, *COL* of the transmitter and/or the receiver in order to penalize throughput.

Test generation without heuristics: Now with the knowledge of wanted_states that penalize throughput, our goal is to generate the details of a network scenario that lead to worst case throughput at link 0-1 in the topology presented in Figure 2 using the test generation algorithm presented in Figure 5. The inputs to the test generation algorithm are the topology, the transition table and the wanted_states. We first construct an initial partial scenario that we input as the root node of the search tree. A **scenario** is defined in terms of network node states, protocol events and time relations between the events and state transitions and represents a global picture of the network. In constructing the initial scenario, we use heuristics to choose the initial scenario that is deemed likely to lead to the worst case. Let us consider the case without the heuristics first.

Given the inputs, the test generation algorithm first constructs all possible initial partial scenarios using the wanted_states and the topology. Figure 6 presents the set of initial partial scenarios from which the algorithm selects the first choice. For example, there are six alternative choices of receivers to be in one of the three wanted_states when the study objective is to minimize throughput at link 0-1 of the topology. Among these choices, the algorithm proceeds with the first choice (partial scenario E_1) which is the case when node 1 is in COL state. We use search and implications to generate all valid scenarios leading from **all** initial scenarios (E_1, E_2, E_3, \dots). Finally, we compare **all** valid scenarios and select the scenario that leads to worst case throughput at link 0-1.

Test generation using heuristics: Given the inputs, the test generation algorithm first constructs all possible initial partial scenarios by using heuristics. Figure 7 presents the first choice that the algorithm selects to generate a valid scenario. If the algorithm finds a valid scenario by exploring this choice, it reports it as the scenario leading to worst throughput at link 0-1. Otherwise, it continues with the second choice, and so

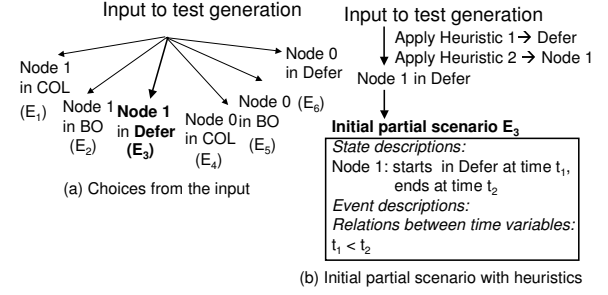


Fig. 7. Constructing initial partial scenario with heuristics.

on. Figure 7.(a) presents the choices from the inputs to test generation algorithm. It uses a heuristic to choose the Defer state as the wanted_state, as this is the state with the highest weight among the three wanted_states. It also uses another heuristic to choose node 1 as the receiving node, as this is the node with highest node degree among the choices of node 0 and node 1. Figure 7.(b) presents E_3 , the input partial scenario which is input to the test generation algorithm. The test generation algorithm uses search and implications to generate the first valid scenario which is reported as the worst case throughput scenario.

IV. PERFORMANCE ANALYSIS OF CSMA/CA MAC PROTOCOLS

We now extend our framework to identify the worst case performance of CSMA/CA based MAC protocols. Previously, we have applied our method to several well-known protocols, e.g., IEEE 802.11 [5], MACA [8] and MACAW [9]. See our technical report [10] for analysis and results. Here we present the results of analysis of CSMA/CA protocols for QoS and TPC using extended versions of our framework.

A. CSMA/CA with Priority based QoS

Based on the analysis presented in [13], we formally define QoS as follows. Let P_1, P_2, \dots, P_n be n priority traffic classes in wireless nodes of a network, where P_1 denotes the highest priority traffic class and P_n denotes the lowest priority traffic class. Let Th_1, Th_2, \dots, Th_n denote the throughputs achieved for the respective priority classes. A protocol is said to be guaranteeing QoS if $Th_1 \geq Th_2 \geq \dots \geq Th_n$. In other words, for two priority classes P_i and P_j such that P_i is a higher class compared to P_j , the QoS guarantees that $Th_i \geq Th_j$.

Figure 8 presents the model of a wireless node in the context of QoS support when we assume that a CSMA/CA protocol is used for medium access. Figure 8.(a) presents the model of a node when no QoS is supported. In this model, a single queue is attached to *each wireless node* in which traffic of all priority classes are serviced without any differentiation. Figure 8.(b) presents the model of a wireless nodes that supports a maximum of four priority classes. One queue is attached to *each priority class* via which traffic of the corresponding class is serviced. When traffic from more than one priority class arrive at a node, to assure QoS, the

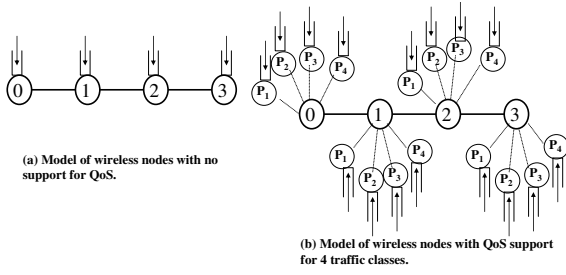


Fig. 8. Models of wireless nodes without and with QoS support.

higher priority class is granted access to the channel before the lower priority class.

The main difference between the models of wireless nodes presented in Figure 8 are as follows. (1) There are *predefined* number of queues depending on the number of priority classes the wireless network supports to provide QoS. (2) A new mechanism is introduced to select the priority class which will access the channel when traffic from multiple classes arrive at the queues. (3) The values of contention windows and other MAC parameters are different for different priority classes. Next we show that despite these differences, we only need to add new heuristics to our previously developed framework to capture the new metric.

The values of contention windows and other MAC parameters, such as, interframe spaces, are modeled using various timers in our framework. Our current model supports all three types of timers, namely periodic, suppressive and non-suppressive. In our extended framework to study QoS, we model timer values specific to a class. For example, we specify BO_i to model backoff values of priority class P_i and the relation of backoff values between various classes.

As the number of priority classes are predefined and there is a predefined priority class selection mechanism within a node, we must incorporate new heuristics to capture the priority class selection mechanism and our study objective. Here we present heuristic H_{qos} for a protocol with **deterministic** selection mechanism.

Our study objective: Our objective is to generate a scenario which provide the worst QoS for a given topology. Note that given two priority classes P_i and P_j such that P_i is the higher class compared to P_j , the QoS guarantees that $Th_i \geq Th_j$. Thus our study objective is to generate scenario that violates the above relation. In other words, our objective is to generate the scenarios that satisfy the relation $Th_i < Th_j$.

Active priority class: Let us define the priority class that is selected at a particular time for channel access as the active priority class at that time. When traffic from multiple classes arrive at a node, the protocol *deterministically* selects the highest priority class as the active priority class and allows it to access the channel.

A transmitting node is defined as a **victim** if the transmitter

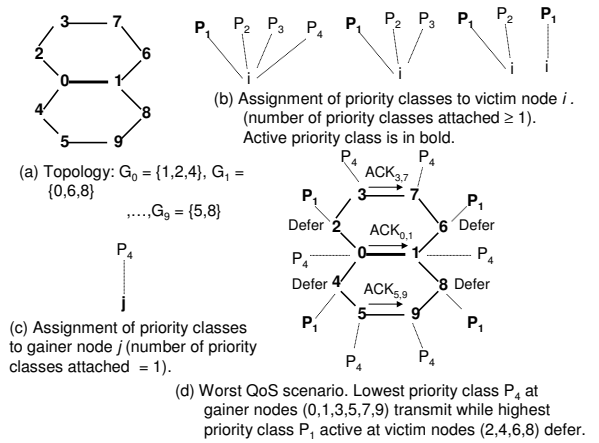


Fig. 9. A worst case QoS scenario in IEEE 802.11e.

is in backoff state because of a failed transmission, and as a **gainer** if it is successful in gaining access to the channel. A receiver is defined as a victim if the receiver is in backoff state because of a collision and as a gainer if it successfully receives the transmission. Since the assignment of priority class within a node is deterministic, we can choose the active priority class of a gainer and a victim node.

Heuristic H_{qos} : Choose a gainer node from nodes with only lowest priority class traffic and a victim node from those with highest priority.

1) Evaluation of IEEE 802.11e: IEEE 802.11e is an enhancement of the IEEE 802.11 standard MAC to support the quality of service [13]. [12] specifies the protocol. The contention based channel access is referred to as *enhanced distributed channel access* (EDCA). In this study, we only consider the QoS support mechanisms provided in EDCA. Contention based medium access is performed in backoff entity by using different parameter values for the EDCA parameter set. The backoff entity in a particular priority class in every node uses the same EDCA parameter [13]. During contention, when the contention window of two or more backoff entities in the same node allow the backoff entities to access channel at the same time, a virtual collision occurs. At this point, the backoff entity with the higher priority class transmits, whereas all other backoff entities act as if a collision has occurred on the channel. The channel access between different nodes of the network is the same as in IEEE 802.11b.

Test results: We use the extended framework to perform analysis of IEEE 802.11e to evaluate the worst case QoS. Figure 9 presents the results of our analysis. Figure 9.(a) presents the topology. We use heuristic H_{qos} to assign priority classes to victim and gainer nodes in the network. Figure 9.(b) presents the assignment of priority classes to victim nodes according to the heuristic. Note that the number of priority

TABLE I
SIMULATION RESULTS FOR SCENARIOS GENERATED BY OUR FRAMEWORK FOR IEEE 802.11E.

Scenario	Topo I			Topo II			Topo III			Topo IV		
	Th_{high}	Th_{low}	Ratio	Th_{high}	Th_{low}	Ratio	Th_{high}	Th_{low}	Ratio	Th_{high}	Th_{low}	Ratio
Test	0.01	0.02	0.5	0.32	0.53	0.6	0.04	0.21	0.19	0.06	0.16	0.37
Random	0.4	0.2	2	0.41	0.1	4	0.31	0.11	3	0.31	0.11	3

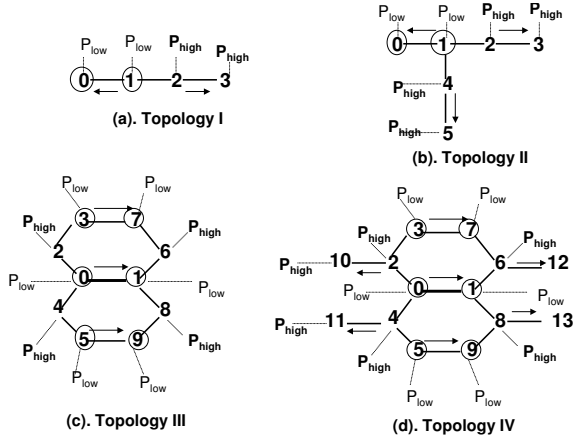


Fig. 10. Topologies used in our simulations.

classes attached to victim nodes are ≥ 1 which must contain the highest priority class P_1 . In this case, the priority class P_1 always gets access to the channel when the contention of channel occurs with other priority classes and is represented by the active priority class in **bold**. Figure 9(c) presents the assignment of only lowest priority class P_4 to gainer nodes according to the heuristic. The number of priority classes attached to gainer nodes is 1 with only P_4 , which always gets access to the channel. Figure 9(d) presents the scenario in which the gainer nodes (lowest priority classes) 0, 1, 3, 5, 7, and 9 transmit while the victim nodes (highest priority classes) defer because of the transmission between the gainers. Thus the aggregate throughput for the lowest priority class is higher than the aggregate throughput for the highest priority class resulting in worst QoS scenario.

Simulation results: We simulate the test scenarios we generated for topologies presented in Figure 10 using ns-2 network simulator [11]. We use two priority classes P_{high} and P_{low} . The circled nodes in the topologies represent the gainer nodes which have only the P_{low} priority class attached. The nodes which are not circled represent the victims which have both priority classes attached, however, the P_{high} are the active priority class in these nodes. The arrows in the figure represent the directions of flows in the **test scenarios** generated by our framework. We use CBR sources at a rate of 0.6 Mbps. Total simulation time is 50 seconds for all scenarios. We use random scenarios in which the sources and sequences are assigned randomly. Table I presents the average

throughput of the nodes of these two priority classes for test scenarios (i.e., generated by our framework) and random scenarios. The columns denoted by **Topo I**, **Topo II**, **Topo III**, and **Topo IV** indicate the simulation results obtained for topologies I, II, III, and IV, respectively in Figure 10. The columns denoted by Th_{high} , Th_{low} , **Ratio** present the average throughput of nodes with priority classes P_{high} and P_{low} , and the ratio between them, respectively. Note that the average throughput of low priority class is higher than that of high priority class in the test scenarios. On average, the lower priority class achieves a throughput 2.5 times more than the throughput achieved by the higher priority class. Note that in topology III, the lower priority class achieves a throughput which is 5 times compared to the throughput of the higher priority class. In the random scenarios, on average, the lower priority class achieves a throughput which is one third of the throughput achieved by the higher priority class on average.

The test scenarios generated by our framework are simple and intuitive given our underlying topology model and heuristic that achieve our study objective. Nevertheless, the results generated by our test scenarios contradict with the results generated by average performance evaluation approaches. For example, the analytical and simulation results of IEEE 802.11e presented in literature [13], [14], [15], [16] show that the lower priority class *always* achieves lower throughput compared to a higher priority class. [16] shows that the lower priority class achieves a throughput approximately a third compared to the high class throughput. These results demonstrate that we cannot rely on random scenarios to properly evaluate QoS guarantees. Furthermore, our framework can be easily extended to generate worst case QoS scenarios that violate the QoS guarantee provided by the protocol and thus contradict the basic notion of QoS.

Protocol analysis: Note that in the worst case (test) QoS scenarios, the lower priority class achieves higher throughput because the priority class selection mechanism only considers the access within a node. The access between nodes remains the same as legacy 802.11b [12]. Thus, the analysis of the test scenarios suggests potential modifications of the protocol to avoid such worst case behaviors with respect to QoS. For example, if the channel access between nodes is modified such that when two nodes attempt to access the channel at the same time, then the nodes with higher active priority class wins. Such a priority based access mechanism between nodes can be achieved by forcing the BO values to be zero for highest priority class (e.g., for P_{high}), to be half of the previous BO values for the second highest priority class (e.g.,

for P_{low}) and so on, when more than one nodes access the channel at the same time. The access mechanism can include priority as well as the BO values to provide QoS while not compromising fairness across the network. Our initial analysis of a version of the protocol with such a modification shows initial promise. We are in the process of thoroughly investigating the modified version of the protocol.

B. CSMA/CA with TPC

The largest source of power consumption at a wireless node is transmission power. Therefore controlling the power to appropriate level increases the energy efficiency of the MAC protocol [17]. Moreover, controlling the transmission power increases the spatial utilization of the wireless channel [17], [21]. Transmission power control schemes have been proposed where wireless nodes dynamically vary the transmission power levels for control as well as data packets to achieve energy efficiency, to improve spatial utilization and to reduce collisions. We extend and apply our framework to study TPC based schemes and identify problems in the protocols.

1) Evaluation of TPC based Schemes: The basic TPC scheme in conjunction with CSMA/CA operates as follows. RTS and CTS are transmitted using the highest power level, while Data and ACK are transmitted using the minimum power level necessary for the nodes to communicate [17]. The main objective of such a power control scheme is to improve energy efficiency and spatial utilization of the wireless network. The protocols proposed in [8], [18], [19], [20] use such a TPC based scheme to control power at the MAC level. In this section, we refer to the power control scheme used by these protocols as the *basic TPC* scheme. Let P_{max} denote the maximum power at which RTS and CTS are sent. Let $P_{desired}$ denote the desired power at which the Data and ACK are sent.

Protocol model: In TPC schemes, a wireless node varies its transmission power depending on the message it transmits. Such a variation of transmission power changes the neighborhood depending on the message. For example, we model the set of nodes that is affected by the transmission of message m by node i as G_i^m . Consider the network shown in Figure 11. Let node 2 initiate a data transmission to node 3 by sending an RTS. The $RTS_{2,3}$ (RTS from node 2 to node 3) is sent at P_{max} which is heard by all nodes in the transmission range of node 2 per RTS. Transmission ranges of node 2 for RTS and Data messages are modeled as G_2^{RTS} and G_2^{Data} , and transmission ranges of node 3 for CTS and ACK messages are modeled as G_3^{CTS} and G_3^{ACK} , respectively. In Figure 11, $G_2^{RTS} = \{0,1,3,4\}$, $G_3^{CTS} = \{1,2,4,5\}$, $G_2^{Data} = \{1,3\}$, and $G_3^{ACK} = \{2,4\}$.

Test results: Using our framework we generate scenarios which show that although the basic TPC schemes improve energy efficiency, they degrade throughput and fairness for

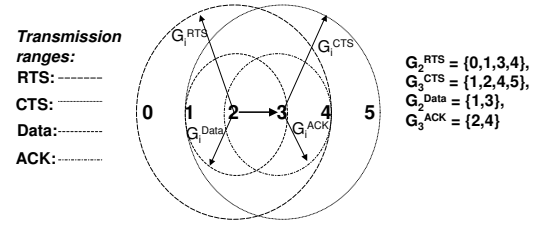


Fig. 11. Topology model in basic TPC schemes.

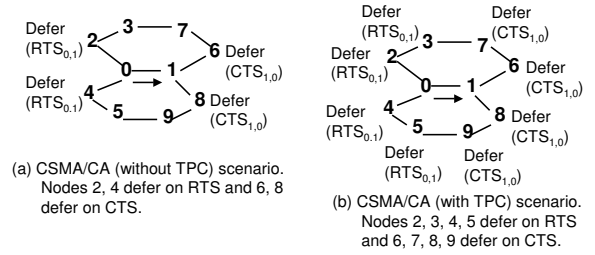


Fig. 12. Worst case scenario in schemes without and with TPC.

the worst case scenarios. Figure 12 presents an overview of the worst scenario we have generated. Figure 12.(a) presents a scenario when no power control scheme is used, while Figure 12.(b) presents a scenario where the basic TPC scheme is used. Let node 0 initiate a transmission to node 1 in Figure 12.(a) and Figure 12.(b). In schemes without power control, all messages are sent at the same power level. The nodes 2 and 4 and nodes 6 and 8 defer on hearing the $RTS_{0,1}$ and $CTS_{1,0}$, respectively, as shown in Figure 12.(a). When TPC is used by transmitting the RTS and CTS at maximum power level, nodes 2, 3, 4, and 5 defer on the RTS and the nodes 6, 7, 8, and 9 defer on the CTS, as shown in Figure 12.(b). This essentially reduces the chances of collision. However, in a highly connected network as in this example, it decreases fairness as well as the throughput of the whole network. If the data transmission between nodes 0 and 1 continues for a long time, all other nodes in the network defer for the entire period of transmission when TPC is used. In case of transmission without power control, the simultaneous transmission between nodes 0 and 1, nodes 3 and 7, and nodes 5 and 9 are possible which increases the fairness as well as the throughput of the network.

Significant amount of prior research has identified various shortcomings of the basic TPC protocols. Extensions of the basic TPC schemes have been proposed to resolve these issues. However, to the best of our knowledge, the results and issues regarding the fairness of the TPC protocols that we have identified have not been identified by any previous work. Regarding the throughput issues, [17] has identified that the throughput of the basic TPC protocols degrades compared to the CSMA/CA scheme without power control. However, the model of wireless channel assumed in [17] is

different. The channel model in [17] considers the *carrier sensing zone* outside of the transmission range. The nodes in carrier sensing zone can sense the signal but cannot decode them correctly while the nodes in transmission range sense as well as decode the signal correctly. Therefore, on sensing the channel busy on RTS/CTS packets, the nodes in carrier sensing zone defer for a period of EIFS which is much smaller compared to the time length of entire data and ACK transmission. Thus the nodes in this zone exit the defer state earlier than the nodes in the transmission range and can collide with the ongoing transmission as their RTSs are also sent at P_{max} . Following this observation, [17] concludes the degradation of throughput in the basic TPC scheme which is different from our results. We also conclude that the throughput degrades in the basic TPC schemes compared to the schemes without TPC. However, our conclusion is based on the simplest channel model consisting only of transmission range.

Protocol analysis: Our analysis provides us with insights for protocol modifications. We have performed an initial analysis of one such modification which shows performance improvements for some scenarios. We are currently further investigating the modified version of the protocol.

V. CONCLUSION AND FUTURE WORK

We have previously developed a framework to analyze MAC protocols. Given a protocol performance objective, the framework first generates the protocol conditions that meet our study objective of generating worst case scenarios. It then applies our test generation algorithm which is a mix of forward and backward searches. The sole purpose of this paper is to demonstrate the generality of this framework by analyzing two very different variations of MAC protocols for wireless adhoc networks, namely IEEE 802.11e for QoS and CSMA/CA with power control. Using the extended framework, we evaluate these protocols. In one case, our results contradict with results claimed by traditional performance evaluation approaches. In other case, our results identify previously unknown problems in the protocol design.

Our scenarios provide insights suggesting potential enhancements for the protocols studied. Evaluation of modified versions of these protocols is a subject of our ongoing research. Finally, identification of protocol design problems, protocol modifications, and re-evaluation of modified protocols using our systematic approach demonstrate the necessity as well as benefits of our systematic approach for protocol evaluation.

REFERENCES

- [1] G. Holzmann, "Design and validation of computer protocols", Prentice Hall, ISBN 0135399254.
- [2] F. Lin, P. Chu, M. Liu, "Protocol verification using reachability analysis", Computer Communication Review, vol. 17, no. 5, pp. 126-135, October 1987.
- [3] M. Kwiatkowska, G. Norman and J. Sproston, "Probabilistic model checking of the IEEE 802.11 wireless local area network protocol", PAPM/PROBMIV 2002, vol. 2399 of LNCS, pp. 169-187, July 2002.
- [4] M. Duflo, M. Kwiatkowska, G. Norman and D. Parker, "A formal analysis of Bluetooth device discovery", 1st International Symposium on Leveraging Applications of Formal Methods (ISOLA) 2004, November 2004.
- [5] IEEE Std 802.11-1997 Information Technology - telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications, pp. i -445.
- [6] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function", IEEE Journal on Selected Areas of Communication (JSAC), vol. 18, no. 3, pp. 535-547, March 2000.
- [7] C. Koksai, H. Kassab, H. Balakrishnan, "An Analysis of Short-Term Fairness in Wireless Media Access Protocols", ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems, pp. 118-119, June 2000.
- [8] P. Karn, "MACA - a new channel access method for packet radio", ARRL/CRRL Amateur Radio 9th Computer Networking Conference, pp. 134-140, 1990.
- [9] V. Bharghavan, A. Demers, S. Shenker, L. Zhang, "MACAW: a media access protocol for wireless LANs", ACM Special Interest Groups on Data Communication (SIGCOMM) 1994, pp. 212-225, September 1994.
- [10] S. Begum, "Test generation framework for evaluation of wireless adhoc MAC protocols", Dissertation Proposal submitted to department of Electrical Engineering, University of Southern California, 2006, <http://www-scf.usc.edu/~sbegum/diss-proposal-shamim.pdf>.
- [11] L. Breslau, D. Estrin, K. Fall, S. Floyd, J. Heidemann, A. Helmy, P. Huang, S. McCanne, K. Varadhan, Y. Xu, and H. Yu, "Advances in Network Simulation", IEEE Computer, vol. 33, no. 5, pp. 59-67, May 2000.
- [12] IEEE 802.11 WG, IEEE 802.11eD5.0, "IEEE Standard for Information Technology - Telecommunications And Information exchange Between Systems - Local And Metropolitan Area Networks-specific Requirements - Part 11: Wireless Medium Access Control (MAC) And Physical Layer (PHY) Specifications Amendment 8: Medium Access Control (MAC) Enhancements for Quality of Service Enhancement", IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003)), 2005 pp. 0_1 - 189.
- [13] S. Mangold, C. Sunghyun, G.R. Hiertz, O. Klein, B. Walke, "Analysis of IEEE 802.11e for QoS Support in Wireless LANs", IEEE Wireless Communications, vol. 10, no. 6, Dec 2003, pp. 40-50.
- [14] Z. Tao and S. Panwar, "Throughput and Delay Analysis for the IEEE 802.11e Enhanced Distributed Channel Access" IEEE Communications, vol. 54, no. 4, April 2006, pp. 593-603.
- [15] H. Zhu and I. Chlamtac, "Performance Analysis for IEEE 802.11e EDCF Service Differentiation" IEEE Wireless Communications, vol. 4, no. 4, July 2005, pp. 1779-1788.
- [16] Y. Xiao, "Performance Analysis of IEEE 802.11 and IEEE 802.11e Wireless LANs", IEEE Wireless Communications, vol. 4, no. 4, July 2005, pp. 1506-1514.
- [17] E. Jung and N. Vaidya, "A Power Control MAC Protocol for Ad Hoc Networks", 8th ACM SIGMOBILE International Conference on Mobile Computing and Networking (MOBICOM) 2002, September 2002.
- [18] S. Agarwal, S. Krishnamurthy, R. H. Katz, and S. K. Dao, "Distributed Power Control in Ad-Hoc Wireless Networks", IEEE Symposium on Personal Indoor and Mobile Radio Communications (PIMRC) 2001, September 2001.
- [19] J. Gomej, A. T. Campbell, M. Naghshineh, and C. Bisdikian, "Conserving Transmission Power in Wireless AdHoc Networks", International Conference on Network Protocols (ICNP) 2001, November 2001.
- [20] M. B. Pursley, H. B. Russel, and J. S. Wyszocarski, "Energy-Efficient Transmission and Routing Protocols for Wireless Multi-hop Networks and Spread-Spectrum Radios", EUROCOMM 2000, pp. 1-5, May 2000.
- [21] R. Choudhury, X. Yang, R. Ramanathan and N. Vaidya, "Using Directional Antennas for Medium Access Control in Ad Hoc Networks", 8th ACM SIGMOBILE International Conference on Mobile Computing and Networking (MOBICOM) 2002, September 2002.