# Enhancing IEEE 802.11 Random Backoff in Selfish Environments

Lei Guang, *Student Member, IEEE,* Chadi Assi, *Member, IEEE,* and Abderrahim Benslimane, *Member, IEEE,*

***Abstract*— Wireless access protocols currently deployed in MANET use distributed contention resolution mechanisms for sharing the wireless channel. In such an environment, selfish hosts that fail to adhere to the MAC protocol may obtain an unfair share of the channel bandwidth at the expense of performance degradation of well-behaved hosts. We present a novel access method, Predictable Random Backoff (PRB), that is capable of mitigating the misbehavior of selfish hosts; particularly, hosts that deliberately do not respect the random deferment of the transmission of their packets [6]. PRB is based on minor modifications of the IEEE 802.11 Binary Exponential Backoff (BEB) and forces each node to generate a *predictable backoff interval*; the key idea is to adjust, in a predictable manner, the lower bound of the contention window in order to enhance the per-station fairness in selfish environments. Hosts that do not follow the operation of PRB are therefore easily detected and isolated. We present an accurate analytical model to compute the system throughput using a three-dimensional Markov chain. We evaluate the performance of PRB under normal case and in the presence of selfish hosts. Our results show that PRB and BEB perform similarly in the former case. Selfish hosts, however, achieve substantially higher throughput than well behaved hosts under BEB. PRB, on the other hand, can effectively enhance IEEE 802.11 BEB by mitigating the impacts of these MAC selfish misbehaviors and guarantee a fair share of the wireless channel for well behaved hosts.**

***Index Terms*— ad hoc networks, medium access control, 802.11, performance evaluation, selfish misbehavior.**

## I. Introduction

Reliable communication in ad hoc networks depends on the inherent trust among nodes. Trust means that nodes need to fully cooperate with each other to ensure correct routes establishment mechanisms, protection of routing information and security of packet forwarding [5], [12], [16]–[18], [21], [22], [24]. However, this trust might be abused by adversaries to carry out security breaches through compromised nodes. The traditional approach to provide network security is built on cryptography-based authentication. However, this is not sufficient to solve the problems arising from new node misbehaviors in mobile ad hoc networks (MANET). Hence, securing MANET against MAC layer misbehavior has become a major challenge in the research community.

Host misbehaviors in MANET can be classified into two categories; namely, selfish misbehavior [7], [20] and malicious misbehavior [2], [14]. A selfish host can deliberately misuse the MAC protocol to gain more network resources than well-behaved hosts. The node can benefit from this behavior by: (1) obtaining a large portion of channel capacity (hence improved throughput); (2) reduced power consumption; (3) improved quality of service, e.g. low network latency. For example, IEEE 802.11 requires hosts competing for the channel to wait for backoff interval [20] before any transmissions. A selfish host may choose to wait for a smaller backoff interval, thereby increasing its chance of accessing the channel and hence reducing the throughput share received by well-behaved stations. The authors of [20] showed that such selfish misbehavior can seriously degrade the performance of the network and accordingly they proposed some modifications for the protocol (e.g., by allowing the receiver to assign backoff values rather than the sender) to detect and penalize misbehaving nodes. Similarly, the authors of [23] addressed the same problem and proposed a system, DOMINO, to detect greedy misbehavior such as backoff manipulations in IEEE 802.11.

Alternatively, malicious misbehavior aims primarily at disrupting the normal operation of the network. This includes colluding adversaries that continuously send data to each other in order to deplete the channel capacity in their vicinity (i.e., causing a denial of service attack, DoS) and hence prevent other legitimate users from communicating [25]. A new class of vulnerabilities was presented in [10] where a host could maliciously modify the protocol timeout mechanism (e.g. by changing SIFS parameter in IEEE 802.11 [1]) and force MAC frames to be dropped at well-behaved nodes. A host exploiting this vulnerability will completely cooperate in forwarding data packets but maliciously forces the forwarding operation to fail. Moreover, the attack also targets crossing flows (flows that traverse through a malicious node) by disrupting their communication and forcing the routing protocol to reroute packets around the misbehaved node.

In order to mitigate the impact of selfish nodes on the network performance, particularly those smart nodes [11], we proposed a new adaptive and predictable algorithm PRB (Predictable Random Backoff) that is based on minor modifications of the IEEE 802.11 BEB (Binary Exponential Backoff), as explained in the subsequent sections. The motivation of PRB is to enhance BEB performance for well-behaved stations in a selfish environment and facilitate the detection procedures against potential selfish stations. Another major contribution of this paper is to develop an accurate analytical model in order to evaluate the performance of PRB by employing a three dimensional Markov chain analysis. We consider in our study the performance of PRB under two cases; namely, the normal behavior and the selfish behavior. **Further, we focus throughout the paper on single hop wireless networks where all nodes are within a transmission range of each**

Manuscript received xxxxx; revised xxxxx.

Lei Guang and Chadi Assi are with Concordia Institute for Information System Engineering, Concordia University. Abderrahim Benslimane is with Laboratoire Informatique d'Avignon, Université d'Avignon.

**other. Note however that the PRB access method, as a misbehavior prevention scheme, can also be applied to multihop ad hoc networks[1]. Additionally, in this work we do not consider the case of colluding hosts and we assume for our model a saturated network where each host always has traffic to send.** In the rest of this paper, we overview the MAC layer selfish misbehavior in wireless networks in Section II. Then in Section III, we describe the IEEE 802.11 BEB algorithm and propose our PRB algorithm. Section III-B.3 illustrates the method to facilitate the detection of selfish behavior with incoperation of PRB. In Section IV, we present our PRB analytical model based on three dimensional Markov chains. We consider both normal case and attack case for BEB and PRB models. Moreover, we validate our analytical model by implementing PRB using NS-2 in Section V. Section VI presents the simulation results using NS-2. Finally, Section VII concludes the paper.

## II. Selfish Behavior in MAC Layer

The IEEE 802.11 (the most popular access protocol for wireless networks) Distributed Coordination Function (DCF) mode [1] combines Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) with a Request to Send/Clear to Send (RTS/CTS) handshake to avoid collisions. It works as follows: when a node has a packet to transmit, if the node senses the medium idle for a period of time longer than or equal to a Distributed Inter Frame Space (DIFS), the packet transmission may start at the beginning of the immediately following slot. Otherwise, the node should backoff for a certain period based on a value randomly selected from $[0, CW]$, where $CW$ is the contention window size. DCF is designed under the assumption that all participating nodes are well behaved. While well-behaved nodes strictly obey the protocol operation, the misbehaving nodes may deviate from the standard to either cause unfairness problems or disrupt the network services. This misbehavior may be hard to differentiate from some normal cases. For example, when a node selects a smaller contention window, it is hard to distinguish whether this selection is due to selfish behavior or a random normal selection.

With the implementation of MAC protocol in software rather than hardware or firmware in network access cards, it is easy to modify the protocol by a selfish or greedy node [7], [11], [23] in order to increase their own share of the common transmission resource. A selfish node may adjust or manipulate its backoff mechanism in different ways to access the channel with higher probability. One way is to choose a small backoff value rather than a valid generated random number by the backoff algorithm, e.g. using range $[0, \frac{CW}{2}]$ rather than $[0, CW]$ or always generating small random value regardless of the range. In the presence of a collision or busy medium or retry, the selfish node will have more chance to win the channel than other nodes. A selfish node may also set longer time duration than the actual transmission time in its RTS/CTS. Those nodes that overhear the exchange will have to adjust their Network Allocation Vector (NAV) accordingly and consequently defer longer time before transmission. Further, they can even adjust the DIFS or SIFS time to further exacerbate the unfairness.

**Algorithm 1** Binary Exponential Backoff

```
$cw_0 \leftarrow [0, 2^{i_{min}} - 1]$
for $each\ sending\ packet\ P_i$ do
    if $P_i\ fails\ to\ transmit$ then
        $CW_{i+1} = 2 \times CW_i$
    else
        $CW_{i+1} = CW_{min}$
    end if
    if $CW_{i+1} > CW_{max}$ then
        $CW_{i+1} = CW_{max}$
    end if
    $cw_{i+1} \leftarrow [0, CW_{i+1}]$
end for
```

The authors of [20] showed that such selfish misbehavior can seriously degrade the performance of the network and accordingly they proposed some modifications for the protocol (e.g., by allowing the *trusted* receiver to assign backoff values rather than the sender) to detect and penalize misbehaving nodes. Similarly, the authors of [23] addressed the same problem and proposed a system, DOMINO, to *detect* greedy misbehavior in IEEE 802.11. However, these systems can be easily exploited by new and smart selfish nodes as presented in [11]; furthermore, most of these systems do not apply for MAC misbehavior in MANET (mobile ad hoc networks).

## III. Proposed Scheme

Our proposed algorithm is designed to require minimal modifications to IEEE 802.11 DCF mode, and mitigate the negative impacts in the presence of misbehaved nodes that manipulate the selection of $cw$ to achieve selfish goals. In this section, we first overview the mechanism of IEEE 802.11 BEB. Second, we present our scheme (*Predictable Random Backoff*, PRB) that is based on modifications of BEB. Finally, we explain how to incorporate PRB into IEEE 802.11 and the existing detection systems to mitigate and detect selfish MAC layer misbehavior.

### A. Binary Exponential Backoff (BEB)

The IEEE 802.11 random access protocol works as follows. A station with data packets to transmit chooses a random backoff value and counts down this value when the channel is sensed idle. When the channel is sensed busy, the counter remains frozen. The algorithm used for backoff is called *Binary Exponential Backoff (BEB)*. As illustrated in **Algorithm 1**, the backoff value $cw_0$ is initially randomly selected from the range $[0, CW = CW_{ub}]$, where $CW_{ub} = CW_{min} = 2^{i_{min}} - 1$; $CW_{ub}$ is doubled if the transmitted packet fails (indicated by the pre-set timeout timer expires [1]), e.g., due to collisions or experiencing CRC errors. $CW_{ub}$ keeps on increasing until reaching the upper bound $CW_{max}$, where $CW_{max} = 2^{i_{max}} - 1$. Each time a packet transmission is successful, $CW_{ub}$ is reset to $CW_{min}$.

**[1] In multihop Ad Hoc networks, there are serious problems arising from exposed and hidden terminals which require the design of a more robust misbehavior detection system; this is outside the scope of this paper.**

**Algorithm 2** Predictable Random Backoff

```
$CW_{lb}^{0} = CW_{lb}^{def} = 1$
$cw_0 \leftarrow [0, 2^{i_{min}} - 1]$
for $each\ sending\ packet\ P_i$ do
    if $\alpha_l \times cw_i < W_t$ then
        if $cw_i == 0$ then
            $CW_{lb}^{i+1} = CW_{lb}^{spec}$
        else
            $CW_{lb}^{i+1} = \alpha_l \times CW_{lb}^{i}$
        end if
    else
        $CW_{lb}^{i+1} = CW_{lb}^{def} = 1$
    end if
    $cw_{i+1} \leftarrow [CW_{lb}^{i+1} - 1, min(2^{i_{min}+n_f}, 2^{i_{max}}) - 1]$
end for
```

### *B. Predictable Random Backoff (PRB)*

*1) Preliminary:* **The key idea of PRB is to adjust in a predictable manner the lower bound of the contention window (denoted as $CW_{lb}$; initially $CW_{lb} = 0$)** in order to enhance the per-station fairness in selfish environments. That is, in order to ensure that well behaved stations receive a fair share of the channel bandwidth. Moreover, the proposed protocol will ensure that selfish nodes will (and unlike BEB) easily be detected and punished if they deliberately do not follow the operation of PRB. We found that the predictable change of the lower bound can result in a significant performance improvement of well-behaved stations (in terms of throughput, delays, fairness) in the presence of selfish stations. Moreover, the method can also improve the overall network throughput in congested, non-selfish environments while maintaining good fairness index.

Other predictable backoff schemes (e.g., IdleSense [15], LMILD [8], etc.) have been also proposed. **LMILD (Linear/Multiplicative Increase and Linear Decrease) is only designed to improve the network throughput (i.e., does not deal with fairness) in a congested environment. Its contention range can be predicted as follows: in case of a failed transmission, $CW_{ub}$ is either linearly increased or multiplicatively increased with a factor of $1.5$ instead of $2$. Upon a successful transmission, instead of directly resetting $CW_{ub}$, $CW_{ub}$ will be linearly reduced while $CW_{lb}$ is always set to $0$.** IdleSense [15] on the other hand is a novel access method derived from 802.11 DCF in which all stations use similar value for the contention window to benefit from good short term fairness. The analysis of Idle Sense showed a high throughput, a low collision overhead, a low delay and a better channel access fairness. However, unlike IdleSense, our PRB protocol focuses on changing the contention window lower bound in order to achieve higher throughput and better channel access fairness for well behaved nodes in the presence of selfish hosts. Further, PRB will prevent selfish hosts from achieving a higher advantage of the channel over well behaved hosts by manipulating access protocol parameters.

*2) Principle of PRB: PRB* algorithm is random and "predictable". It is random because (similar to BEB) the backoff value is selected randomly from the contention window. Unlike BEB, it is predictable since the lower bound of the contention window ($CW_{lb}$) for the next transmission is predictable based on the current selected $cw$. Accordingly, and regardless of the attack strategies a selfish node may apply to manipulate the selection of $cw$ (as mentioned in [11]), that will only lead to two consequences:

- if the selfish node follows PRB, the negative impacts it has on the network performance will be mitigated regardless of the attack strategies;
- if the selfish node does not follow PRB, since the backoff selection is predictable, the receiver can easily detect the misbehavior of the transmitter and perform immediate punishment (as discussed in Section III-B.3).

PRB operates as follows: initially, a node with a data packet to transmit randomly chooses a $cw_i$ from $[0, CW_{min}]$. Upon a successful data transmission, if both $cw_i$ and $\alpha_l \times cw_i$ are less than $W_t$[2], a lower bound of the contention window for the next $cw_{i+1}$ selection will be assigned as $CW_{lb}^{i+1} = \alpha_l \times CW_{lb}^{i}$. In case $cw_i$ is selected as 0, $CW_{lb}$ is set to a pre-specified value $CW_{lb}^{spec}$. Otherwise, $CW_{lb}$ will be set to a default value[3]. Therefore, the node needs to select $cw_{i+1}$ from $[CW_{lb}^{i+1} - 1, CW_{min}]$ for the next transmission. In the presence of a failed transmission due to collision or packet errors, the upper bound $CW_{ub}$ is doubled and $cw$ is selected from $[CW_{lb}^{i+1} - 1, min(2^{i_{min}+n_f} - 1, 2^{i_{max}} - 1)]$, where $n_f$ is the number of failed transmissions. Finally, $CW_{ub}$ continues to increase until it reaches $CW_{max}$.

*3) Detection and Reaction based on PRB:* Contrary to previous work [20], the role of a receiver is to *only* detect a selfish sender in order to eliminate the exploits introduced by untrusted partners [11].

First, we consider a selfish node that *only* aims at obtaining higher throughput by choosing smaller $cw$. A Rx[4] can compute $B_{act}^{i}$, the actual backoff time duration, for each received frame by using the methods described in [20], [23]. **The condition $CW_{act}^{i} < CW_{lb}^{i}$ directly identifies a Tx as misbehaved, where $CW_{lb}^{i}$ is the lower bound.** Unlike [20], [23], there is no need for $\lambda$[5] to ensure correct detection, because the value of $CW_{lb}^{i}$ is deterministic and can be easily calculated by the Rx through monitoring the transmissions of Tx. As a consequence, the detection procedure is simple and accurate. In the presence of interference, we can improve the positive alarms by introducing multiple-frame monitoring in addition to per-frame monitoring. Note that choosing $CW_{act}^{i} \geq CW_{lb}^{i}$ is not sufficient to indicate a well-behaved Tx. However, even if a selfish Tx tries to keep on selecting small $cw$ by applying the strategies we described in [11], as long as it follows PRB (i.e., choosing $cw_i$ larger than $CW_{lb}^{i}$), the negative impacts are significantly mitigated as will be shown in Section V. The same detection methods can be applied to detect a selfish node that selects a larger $cw$ in order to reduce power consumption. This requires modifications to the PRB by introducing an upper bound $CW_{ub}$. Accordingly, a

[2] $\alpha_l$ **is a multiplicative factor used to increase the lower bound of** $CW$ ($\alpha_l > 1$). $W_t$ is the threshold to reset the current lower bound of $CW$ to 0.

[3] Note that the default value of $CW_{lb}$ is set to $CW_{lb}^{def} = 1$.

[4] In a single handshaking process, a node will play two different roles, i.e. transmitter (Tx) or receiver (Rx). To avoid confusion in the following sections, we use transmitter (Tx) to refer to the source of a MAC DATA frame whereas receiver (Rx) refers to the destination of a MAC DATA frame.

[5] $\lambda$ is a configurable parameter that is selected according to the desired correct diagnosis ratio and mis-diagnosis ratio.

node that keeps on choosing larger $cw$ will be identified if $CW^i_{act} > CW^i_{ub}$. Moreover, as the detection is based on per-frame monitoring, it is faster than other detection systems [20], [23] **(where the detection system needs to be triggered after statistical analysis for a monitoring period, which includes more than one frame transmission). It is to be noted that in a multihop network, problems arising from hidden and exposed terminals cause impairments for the detection system; for instance, when a transmitter is trying to communicate with a receiver that is exposed to another communication (of which the transmitter is not aware), the receiver may falsely designate the transmitter as a selfish host because the latter did not backoff for a longer period. Accordingly, we suggest that a better detection system must be designed to deal with problems arising from selfish, hidden and exposed hosts. It is important however to mention that the PRB access method is a prevention scheme; the design for a detection system in a multihop network is a challenging research that is outside the scope of this work.**

## IV. Modeling and Analysis

In this section, we present the details of our proposed throughput model for BEB and PRB protocols[6]. We have used the same assumptions made in [4] in our model. First, we present the analysis of BEB. Second, we develop the mathematical model for PRB. Both normal case and attack case are considered in the models. We first study $\tau$, the transmission probability of a single station during a randomly selected time slot. Then, we express the throughput model for the whole network as a function of the variable $\tau$.

### A. Normal Case

*1) Analysis of BEB:* We briefly present the model developed by Bianchi for BEB [4]. Let $b(x)$ be the stochastic process representing the backoff time counter for a given station. A discrete and integer time scale is adopted, e.g., $x$ and $x+1$ represent the beginning of two consecutive time slots. Let $W_i$ be the contention window size which is defined as $W_i = 2^i W_0$, where $W_0 = CW_{min}$ is the initial contention window value and let $W_m = CW_{max}$[7] be the maximum value of the contention window (at the last backoff stage). Let $s(x)$ be the stochastic process representing the backoff stage $(0, ..., m)$ of the station at time $x$. Denoted $p$ as the conditional collision probability which is constant and independent regardless of the number of retransmissions incurred. The system can be modelled as a two dimensional stochastic process $\{s(x), b(x)\}$ with the discrete time Markov chain depicted in Figure 1. The only non-null one-step transition probabilities are:

$$\begin{cases} P\{i,k|i,k+1\} = 1 & k \in (0, W_i - 2), i \in (0, m) \\ P\{0,k|i,0\} = \frac{1-p}{W_0} & k \in (0, W_0 - 1), i \in (0, m) \\ P\{i,k|i-1,0\} = \frac{p}{W_i} & k \in (0, W_0 - 1), i \in (1, m) \\ P\{m,k|m,0\} = \frac{p}{W_m} & k \in (0, W_m - 1) \end{cases} \tag{1}$$

Therefore, the probability $\tau$ that a station transmits in a randomly chosen slot time (access probability) is given by:

$$\begin{aligned} \tau &= \sum_{i=0}^{m} b_{i,0} = \frac{b_{0,0}}{1-p} \\ &= \frac{2(1-2p)}{(1-2p)(W_0+1) + pW_0(1-(2p)^m)} \end{aligned} \tag{2}$$

Here, $\tau$ is the transmission probability for a single station. We can use it to further develop the throughput model as explained later.

*2) Analysis of PRB:* Recall that in PRB, a station adjusts its lower bound ($CW_{lb}$) for the contention window for next stage upon each successful transmission if the chosen $cw_i$ at a stage $i$ is lower than the specified $W_t$ as explained in **Algorithm 2. Therefore, we let $l(x)$ be the stochastic process representing the lower bound for a particular contention stage.**

First, we have $W_t \in [0, W_0 - 1]$, where $W_t$ is the threshold and $W_0$ is the minimum $CW$ upper bound[8]. When $t = 0$, PRB operates the same way as BEB. Let $j$ be a variable representing the lower bound stage of a contention window:

$$2^{j_{min}} - 1 = 0 \Longrightarrow j_{min} = 0 \tag{3}$$

$$\alpha_l \cdot 2^{j_{max}} = W_t \Longrightarrow j_{max} = \lceil \log_2 \frac{W_t}{\alpha_l} \rceil \tag{4}$$

And we define $M_j$ as the lower bound of a particular contention window at stage $j$:

$$M_j = 2^j \tag{5}$$

where $j \in [0, \lceil \log_2 \frac{W_t}{\alpha_l} \rceil]$. Let $M_t$ be the maximum lower bound stage and define it as follows:

$$M_t = 2^t = W_t / \alpha_l \tag{6}$$

With these, we obtain a three dimensional stochastic process $\{l(x), s(x), b(x)\}$ to model the protocol behavior as a discrete time Markov chain depicted in Figure 2. In the Markov chain, the only non-null one step transition probabilities are given by:

$$\begin{cases} P\{j,i,k|j,i,k+1\} & = 1 \\ P\{j+1,0,k|j,i,0\} & = \frac{1-p}{W_0 - M_{j+1} + 1} \times \frac{M_t - M_j + 1}{W_i - M_j + 1} \\ P\{0,0,k|j,i,0\} & = \frac{1-p}{W_0} \times \frac{W_i - M_t}{W_i - M_j + 1} \\ P\{j,i,k|j,i-1,0\} & = \frac{p}{W_i - M_j + 1} \\ P\{j,m,k|j,m,0\} & = \frac{p}{W_m - M_j + 1} \end{cases} \tag{7}$$

where the corresponding ranges for $j$, $i$, $k$ are given by:

$$\begin{cases} j \in [0,t], i \in [0,m], k \in [0, W_i - 2] \\ j \in [0,t-1], i \in [0,m], k \in [M_{j+1} - 1, W_0] \\ j \in [0,t], i \in [0,m], k \in [0, W_0 - 1] \\ j \in [0,t], i \in [1,m], k \in [M_j - 1, W_i - 1] \\ j \in [0,t], i \in [m,m], k \in [M_j - 1, W_m - 1] \end{cases} \tag{8}$$

The transition probabilities in (7) are explained as follows:

- $P_{(j,i,k+1) \to (j,i,k)}$: A station will decrease its backoff counter by 1 after it senses the channel is idle for each time slot otherwise it will freeze its counter.
- $P_{(j,i,0) \to (j+1,0,k)}$: If a station succeeds in the current transmission, it will increase its current $CW$ lower bound

[6] Initial work has been presented in [13].

[7] For convenience, we use $CW$ and $W$ interchangeably to refer as the contention window size adopted by a station.

[8] In the following discussion, without loss of generality we always assume that $W_t \leq W_0$. The case that $W_t > W_0$ will not be discussed in this paper.

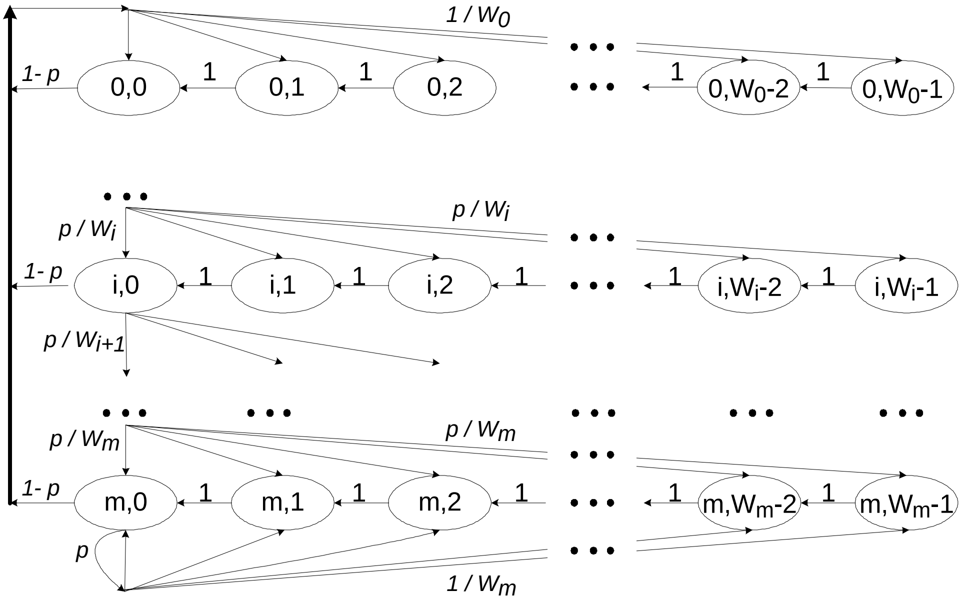


Fig. 1. Markov Chain Model (2-D): BEB

from $j$ to $j+1$ only if the current selected $cw$ is less than $M_t$.

- $P_{(j,i,0)\to(0,0,k)}$: Once the backoff counter $k$ reaches 0, a station can start to transmit. Upon the successful transmission, if the current selected $cw$ is greater or equal to $M_t$, the $CW$ lower bound will reset to 0.
- $P_{(j,i-1,0)\to(j,i,k)}$: If a station fails to transmit a packet (due to collision or packet error), it will increase the current $CW$ upper bound while keeping the lower bound unchanged.
- $P_{(j,m,0)\to(j,m,k)}$: If a station faces failed transmission and its current $CW$ upper bound reaches the maximum value $CW_{max}$ ($i = m$), it will keep on using the same upper bound $CW_{max}$ until successful transmission.

Let $b_{j,i,k} = \lim_{x\to\infty} P\{l(x) = j, s(x) = i, b(x) = k\}$, $j \in [1,t]$, $i \in [0,m]$, $k \in [M_j - 1, W_i - 1]$ be the stationary distribution of the chain. We consider two different cases in our study to derive the station transmission probabilities; namely, the case of $j = 0$ and $j > 0$.

*a) case $j = 0$:* In the presence of a failed transmission, a station will double its upper bound until reaching $CW_{max}$. According to the state balance condition, we can then write (the derivation is shown in the Appendix):

$$b_{0,i,k} = \frac{W_i - k}{W_i} \begin{cases} \sum_{j=0}^{t}\sum_{i=0}^{m} b_{j,i,0}\dfrac{(1-p)(W_i - M_t)}{W_i - M_j + 1} & i = 0 \\ p \cdot b_{0,i-1,0} & 0 < i < m \\ p \cdot (b_{0,m-1,0} + b_{0,m,0}) & i = m \end{cases} \tag{9}$$

where $k \in [0, W_i - 1]$.

*b) case $t \geq j > 0$:* $b_{j,i,k}$ is given by (the derivation is shown in the Appendix):

- if $k \geq M_j - 1$, then

$$b_{j,i,k} = \frac{W_i - k}{W_i - M_j + 1} \begin{cases} \sum_{i=0}^{m} \dfrac{b_{j-1,i,0}M_t(1-p)}{W_i - M_j + 1} & i = 0 \\ p \cdot b_{j,i-1,0} & 0 < i < k \\ p \cdot (b_{0,m-1,0} + b_{0,m,0}) & i = m \end{cases} \tag{10}$$

- if $0 \leq k < M_j - 1$, then

$$b_{j,i,k} = b_{j,i,k+1} \tag{11}$$

The ratio $\frac{W_i - k}{W_i - M_j + 1}$ accounts for the distribution of probabilities for each state in the corresponding stages $j$ and $i$. As shown in Figure 2, when the stage moves from the left side to the right side, the probability decreases by $\frac{1}{W_i - M_j + 1}$ ($k \geq M_j - 1$). However, unlike BEB, when $0 \leq k < M_j - 1$, $b_{j,i,k}$ always gets a single input from $b_{j,i,M_j-1}$ which means PRB eliminates the chance that the state $b_{j,0,k}$ ($k < M_j - 1$) be directly selected from $b_{j-1,i,0}$.

Clearly, it is not trivial to obtain a closed-form expression for $b_{j,i,k}$. Hence, we solve the system throughput model via numerical simulations based on Matlab. In Section V-A, we give details about the procedure of the numerical simulations. From (10) and (11), we can express $b_{j,i,k}$ into a function of two variables $b_{0,0,0}$ and $p$. From the normalization condition (12), we can write $1 = b_{0,0,0} \cdot \Phi(p)$, where $\Phi(p)$ is a function of $p$ only.

Therefore, $b_{0,0,0}$ is equal to $\frac{1}{\Phi(p)}$.

$$\begin{aligned} 1 &= \sum_{j=0}^{t}\sum_{i=0}^{m}\sum_{k=0}^{W_i-1} b_{j,i,k} \\ &= \sum_{i=0}^{m}\sum_{k=0}^{W_i-1} b_{0,i,k} + \sum_{i=0}^{m}\sum_{k=0}^{M_j-2} b_{j,i,k} + \sum_{i=0}^{m}\sum_{k=M_j-1}^{W_i-1} b_{j,i,k} \\ &= \sum_{j=0}^{t}\sum_{i=0}^{m} \frac{W_i - M_j + 2}{2} b_{j,i,0} \end{aligned} \tag{12}$$

***Single Station Transmission Probability:*** Now we can express the probability $\tau$ that a station transmits in a randomly

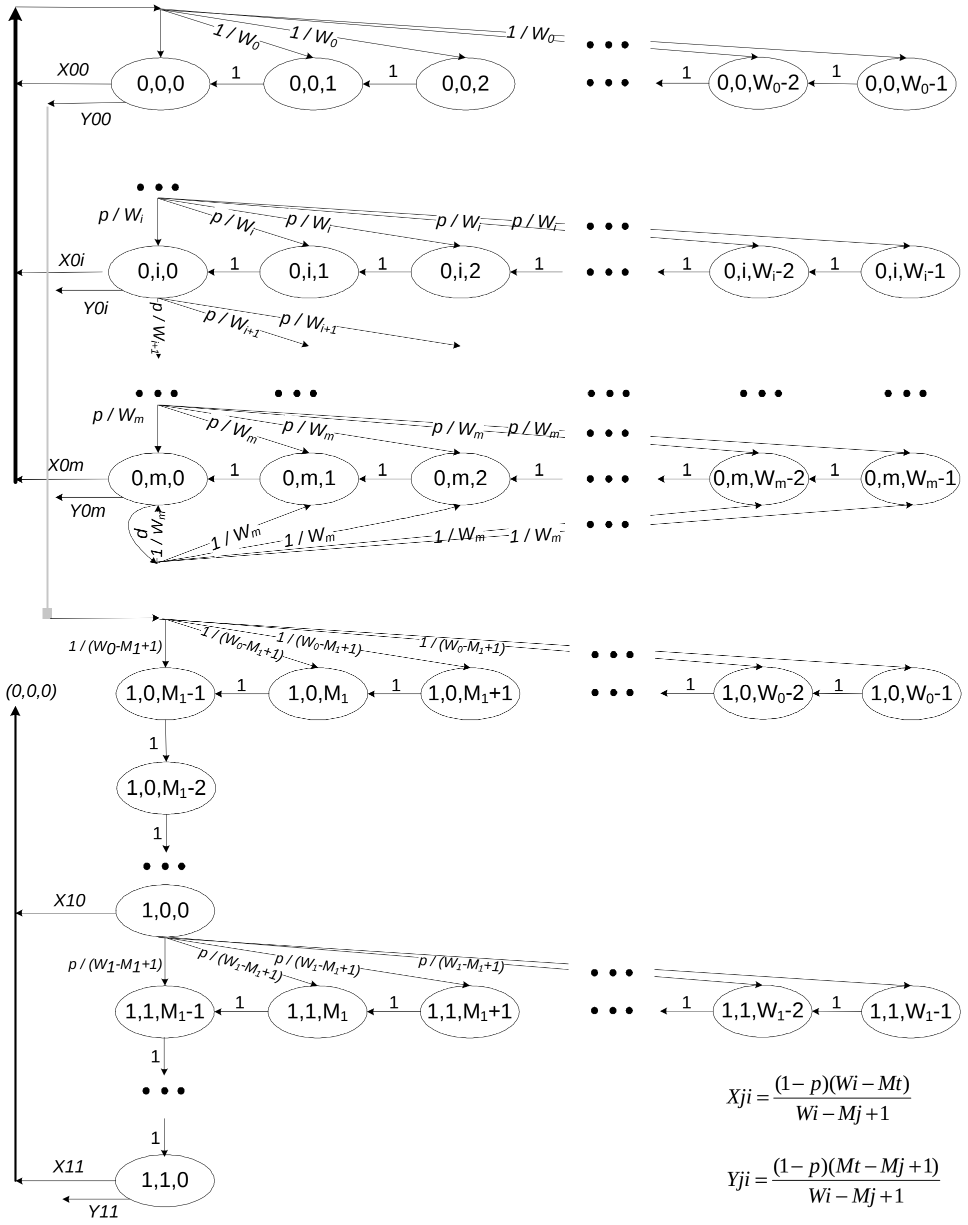


Fig. 2. Markov Chain Model (3-D): PRB

selected time slot: once the backoff time counter reaches 0 (i.e., $k = 0$) a transmission will start regardless of the backoff stage ($\forall i$) and lower bound ($\forall j$):

$$\begin{aligned}
\tau &= \sum_{j=0}^{t}\sum_{i=0}^{m} b_{j,i,0} = \sum_{i=0}^{m} b_{0,i,0} + \cdots + \sum_{i=0}^{m} b_{t,i,0} \\
&= \frac{b_{0,0,0}}{1-p} + \cdots + \frac{b_{t,0,0}}{1-p} = \frac{1}{1-p}\sum_{j=0}^{t} b_{j,0,0} \\
&= \Psi(p, W_0, m, t, b_{0,0,0})
\end{aligned} \tag{13}$$

From (9), (A-15) and (13), we can see that $\tau$ is a function of only one unknown variable $p$. The other variables $(W_0, m, t)$ have known values and $b_{0,0,0}$ can be numerically solved as explained in Section V-A.

Now, we assume that $n$ identical stations share the channel independently; therefore the probability that each station encounters contentions is independent of the other stations. Moreover, the probability $\tau$ that a station transmits a packet during a slot time is the same for the $n$ stations. Then $p$ is the probability that at least one station transmits in the same time slot (i.e., collision) which is given by (14):

$$p = 1 - (1-\tau)^{n-1} \tag{14}$$

Finally, the functions (13) and (14) represent a nonlinear system with two unknown variables $\tau$ and $p$. It can be proved that this system has a unique solution:

- The expression of $p$ in (14) is continuous and is *monotone*, increasing with $\tau$ which is proved by the fact that the first order derivation of $p$ is always larger than 0: $p^{(1)} = (n-1)(1-\tau)^{n-2} \geq 0$. Moreover, $\tau = 0$ when $p = 0$ and $\tau = 1$ when $p = 1$.
- The expression of $\tau$ in (13) is *continuous* with $p$. In order to obtain the unique solution, $\tau$ needs to be continuously

decreasing with $p$, i.e., more contentions lead to lower transmission probability. Note that, from (A-15) and (13), $\tau$ reaches the maximum value when $p \rightarrow 0$ and the minimum value when $p \rightarrow 1$. Furthermore, from our numerical results it also shows that $\tau$ is continuously decreased with the increment of $p$.

***Total Network Throughput Model:*** Here we present the total network throughput model for both BEB and PRB. Some notations are given as following:

- $P_{tr}$: the probability that there is at least one transmission in a considered time slot is given by (15);

$$P_{tr} = 1 - (1-\tau)^n \tag{15}$$

- $P_s$: the probability that a transmission is successful by the probability that exactly one station transmits on the channel, conditioned on the fact that at least one station transmits, is given by (16);

$$P_s = \frac{n\tau(1-\tau)^{n-1}}{P_{tr}} = \frac{n\tau(1-\tau)^{n-1}}{1-(1-\tau)^n} \tag{16}$$

- $E[PL]$: the average packet payload size;
- $T_o$: the duration of an empty slot time;
- $T_s$: the average time the channel is sensed busy for a successful transmission is given by (see Figure **??** for details):

$$\begin{cases} T_s^{RTS} & = T_{RTS} + sifs + \delta + T_{CTS} + sifs + \delta + T_H \\ & +E[PL] + sifs + \delta + T_{ACK} + difs + \delta \\ T_s^{bas} & = T_H + E[PL] + sifs + \delta + T_{ACK} + difs + \delta \end{cases} \tag{17}$$

where $H = hdr_{MAC} + hdr_{PHY}$ and $hdr_{MAC}$, $hdr_{PHY}$ are the size of MAC header and physical header respectively. $T_H$ is the transmission time of $H$. $T_{RTS}$, $T_{CTS}$ and $T_{ACK}$ are the transmission time of RTS, CTS, ACK respectively. $\delta$ is the maximum propagation delay. $T_s^{RTS}$ is $T_s$ of the four-way handshaking access and $T_s^{bas}$ is $T_s$ of the basic access.

- $T_f$: the average time the channel is sensed busy for a failed transmission is given by:

$$\begin{cases} T_f^{RTS} & = T_{RTS} + difs + \delta \\ T_f^{bas} & = H + E[PL] + difs + \delta \end{cases} \tag{18}$$

- $\Gamma$: the normalized system throughput.

Hence, the expression for the system throughput $\Gamma$ is given by (19). Note that, the difference between BEB and PRB is the transmission probability $\tau$ which is defined by (2) and (13) respectively.

$$\Gamma = \frac{P_s P_{tr} E[PL]}{(1-P_{tr})T_o + P_{tr}P_sT_s + P_{tr}(1-P_s)T_f} \tag{19}$$

***Individual Node Throughput Model:*** Here we present the individual node throughput model for both BEB and PRB. Some notations are given as follows:

- $U_v^s$: the probability that a station $v$ successfully transmits during a time slot is given by:

$$U_v^s = \tau_v \prod_{q=1,q\neq v}^{n} (1-\tau_q) \tag{20}$$

- $U^s$: the sum of the probabilities of successful transmissions for all stations:

$$U^s = \sum_{v=1}^{n} U_v^s \tag{21}$$

- $U^o$: the probability that the channel is idle is given by:

$$U^o = \prod_{v=1}^{n} (1-\tau_v) \tag{22}$$

- $U^f$: the probability that collisions occur is given by:

$$U^f = 1 - U^o - U^s \tag{23}$$

Hence, the throughput $\Omega(v)$ of an individual station $v$ is given by:

$$\Omega(v) = \frac{U_v^s E[PL]}{U^oT_o + U^sT_s + U^fT_f} \tag{24}$$

## *B. Attack Case*

In Section IV-A, the presented models for BEB and PRB are under the assumption of a saturated channel. Since the objective of a selfish station is to maximize its own throughput, it will always tend to use the full channel capacity (i.e., the system will operate at the saturation point).

*1) Analysis of BEB:* From Equation (2), we can model several selfish strategies that manipulate $CW$. For example, a selfish node chooses $cw$ from $[0, \gamma CW_{min}]$ $(0 \leq \gamma < 1)$[9], instead of $[0, CW_{min}]$ can be modeled as:

$$\tau_{BEB_s} = \frac{2(1-2p_s)}{(1-2p_s)(W_0^{\gamma}+1) + pW_0^{\gamma}(1-(2p_s)^m)} \tag{25}$$

where $W_0^{\gamma}$ represents $\gamma W_{min}$ and $p_s$ is the collision probability for a selfish node. Another example is that a selfish node selects $CW_{min} = CW_{max} = W_s$, where $W_s$ is the contention window specified by the selfish node. The transmission probability of a selfish node is given by:

$$\tau_{BEB_s} = \frac{2(1-2p_s)}{(1-2p_s)(W_s+1) + p_sW_s(1-(2p_s)^i)} \tag{26}$$

In the case that a selfish node always assigns $CW_{max}$ to $CW_{min}$ which can be specified by $W_\beta$, there will be no backoff $(i = 0)$ and (26) can be simplified as:

$$\tau_{BEB_s} = \frac{2}{W_\beta + 1} \tag{27}$$

From (25) and (26), it is clear that a selfish node will have more chance to access the channel than in normal case. Further more, the access probability for a well-behaved node is given by:

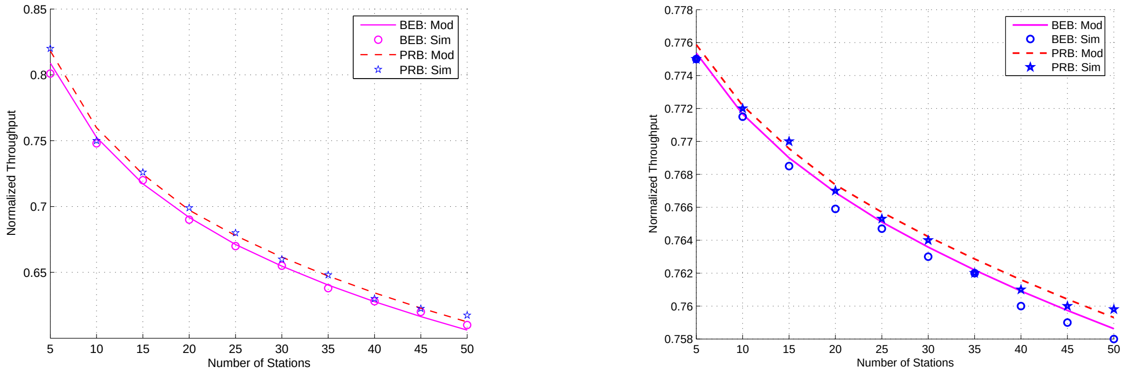
$$\tau_{BEB_w} = \frac{2(1-2p_w)}{(1-2p_w)(W_0+1) + p_wW_0(1-(2p_w)^i)} \tag{28}$$

where $p_w$ is decided by:

$$p_w = 1 - (1-\tau_w)^{n-n_s-1}(1-\tau_w)^{n_s} \tag{29}$$

where $n_s$ is the number of selfish stations in the network.

[9] $\gamma$ is the misbehavior coefficient to determine the percentage of selfish misbehavior.



(a) Basic Access

(b) Four-way Handshaking

Fig. 3. Overall Throughput of PRB and BEB vs. Number of Contending Stations

*2) Analysis of PRB:* Similar to BEB, we can model selfish attack strategies by manipulating (A-3), (A-15) and (13). For example, a selfish node chooses $cw$ from $[0, \gamma CW_{min}]$ $(0 \leq \gamma < 1)$ instead of $[0, CW_{min}]$ can be modeled as:

$$b_{0,0,0} = \sum_{j=0}^{t}\sum_{i=0}^{m} b_{j,i,0}\cdot\frac{(1-p)(W_0^{\gamma} - M_t)}{W_0^{\gamma} - M_j + 1} \tag{30}$$

and

$$b_{j,0,0} = \sum_{i=0}^{m}\frac{b_{j-1,0,0}(1-p)(M_t - M_{j-1} + 1)p^i}{W_0^{\gamma} - M_{j-1} + 1} \tag{31}$$

Equations (30) and (31) account for the facts that a selfish station selects $W_s$ larger than $M_t$ but smaller than the standard value $CW_{min}$. If a selfish station selects $W_s$ smaller than $M_t$, it has to increase its lower bound upon a successful transmission with probability 1 instead of $\frac{(1-p)(M_t - M_{j-1}+1)}{2^i W_s - M_{j-1}+1}$ which is always less than or equal to 1. Clearly, in PRB a selfish station selecting smaller $cw$ will experience more states to transit back to state $b_{0,0,0}$ whereas in BEB a selfish station can transit to $b_{0,0,0}$ immediately upon a successful transmission.

**Algorithm 3** Procedure for Numerical Simulations

```
 1: InitBEB (payload, $N$, MAC parameters)
 2: InitPRB ($\alpha_l$, $W_t$)
 3: $\tau_o = \tau_{init}$
 4: Init ($p$) from Equation (14)
 5: Represent $b_{j,i,0}$ as a function of $b_{0,0,0}$ using Equations (A-4), (31), (A-
    12) and (A-13)
 6: Using the normalization condition (12), and the result of the previous
    step, determine $b_{0,0,0}$
 7: Compute ($\tau_n$) from Equation (13)
 8: while abs($\tau_n - \tau_o$) $> \sigma$ do
 9:     $\tau_n = Max(\tau_o, \tau_n) - abs(\tau_n - \tau_o)/2$
10:     Compute $p$ from Equation (29)
11:     Update $\tau_n$ using steps 5, 6 and 7
12: end while
13: Calculate $P_{tr}$ from Equation (15)
14: Calculate $P_s$ from Equation (16)
15: Compute throughput $\Gamma$ from Equation (19)
```

## V. Performance Analysis

In this section, we first validate our proposed PRB model in Section V-A. In Section V-B, we compare the performance between PRB and BEB[10].

### A. Model Validation

| Parameters | Value |
|---|---|
| Propagation | Free Space |
| Channel Capacity | 1 Mbps |
| Payload $E[PL]$ | 1050 Bytes |
| MAC Header | 52 Bytes |
| Physical Header | 28 Bytes |
| RTS | 44 Bytes |
| CTS | 38 Bytes |
| ACK | 38 Bytes |
| Propagation Delay | 2 $\mu s$ |
| SIFS | 10 $\mu s$ |
| DIFS | 50 $\mu s$ |
| Slot Time | 20 $\mu s$ |
| $CW_{min}$ | 32 |
| $CW_{max}$ | 1024 |

TABLE I

Parameters for Analytical and Simulation Results

We validate our proposed 3-D Markov Chain throughput model for PRB by comparing the numerical results (Matlab) with the simulation results using the network simulator ns-2 [9]. **The procedure to perform numerical experiments under Matlab is shown in Algorithm 3. Here, since we do not have a close form for $\tau$ one needs to determine $b_{0,0,0}$ in order to determine the transmission probability. The normalization condition helps in constructing a $2\times2$ matrix $C$ such that $c_{ji} = K_{ji} \times b_{0,0,0}$, where $K_{ji}$ are constants whose values can be easily determined from Equations (12), (A-4), (31), (A-12) and (A-13). Using (12), one can write $b_{0,0,0} = \frac{1}{\sum_{j=0}^{t}\sum_{i=0}^{m} c_{ji}}$. Once we have $b_{0,0,0}$, the transmission and collision probabilities can be determined; these steps are iterated until we reach to a feasible solution.**

Now, we compare the numerical and simulation results under both the basic and the four-way handshaking mechanisms. For this purpose, we consider an ad hoc network with $n_s = 1$ selfish station out of $n$ stations, where $n$ stations are randomly generated in a $100m \times 100m$ area and each station is within

[10] All the evaluations are under the saturated conditions. Development of models under non-saturated conditions will be left to our future work.

the transmission range of the others. The simulated stations have a buffer size of 64 packets. All the parameters that are used for performance evaluations are summarized in Table I. In Figure 3, we present the total network throughput of BEB (designated as "BEB") and PRB (designated as "PRB") under the normal case, i.e., no selfish attack. The model results (designated as "Mod") are quite close to the simulation results (designated as "Sim"). Clearly, from the two figures we can see that the performance of PRB is comparable to that of BEB and performs even slightly better than BEB under both basic access and RTS/CTS handshaking scheme. This is due to the fact that a well-behaved station will not continuously choose smaller $cw$; and hence few times increment of $CW$ will not cause performance degradation. Moreover, as a station under PRB can not always capture the channel by deliberately choosing smaller $cw$, this allows other stations to have more chance to access the channel. Thus increasing the fairness between stations as well as improving the throughput by reducing the collision probabilities.

### *B. Efficiency of PRB*

In this section, we evaluate the efficiency of our proposed algorithm PRB in mitigating the negative effects that the manipulation of $cw$ could cause on well-behaved hosts. We compare the performance of BEB and PRB using the two different scenarios: 1) normal case; 2) attack case[11].

*1) Normal Case:* Figure 4 plots the normalized network throughput for BEB and PRB when varying $W_t$ (Figure 4(a)) and $\alpha_l$ (Figure 4(b)) under normal case. It is clear that in the absence of any selfish nodes, BEB and PRB have similar network throughput when using different PRB parameters. In PRB, $CW_{lb}$ is used to prevent a node from selecting smaller $cw$ upon successful transmission; whereas a well-behaved node will have little chance to continuously selecting smaller $cw$ accidentally. The figures show a comparable network throughput between BEB and PRB under the no attack scenario. Moreover, as the number of flows increases, there is a rapid decrease in the normalized throughput. This is because more collisions will happen as the network environment becomes more congested, i.e., when more data flows join the network.

*2) Attack Case:* Without loss of generality, we consider a selfish station that tries to capture the channel by selecting smaller $cw$ from $[0, \gamma CW_{min}]$ $(0 \leq \gamma < 1)$. In PRB, as the selfish station intends to avoid quick and easy detection as explained in Section III-B.3, it has to increase the lower bound if it selects a $cw$ less than the threshold upon a successful transmission. We consider the worst case for PRB; that is, a selfish station will always choose a $cw$ equal to the current lower bound.

Figure 5 compares the throughput obtained by a selfish flow (designated as "Selfish") and a well-behaved flow (designated as "Normal") using our proposed PRB with that obtained using the IEEE BEB when varying the misbehavior coefficient $\gamma$, i.e., $\gamma$ equals to 0.2 and 0.6 respectively. For convenience,

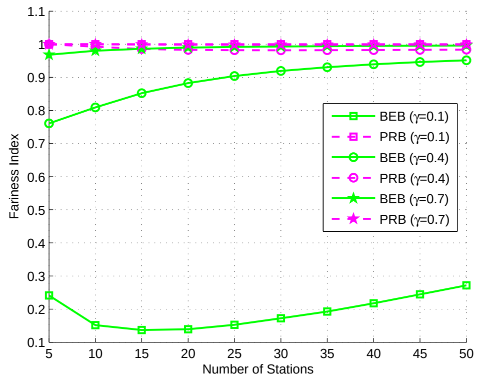


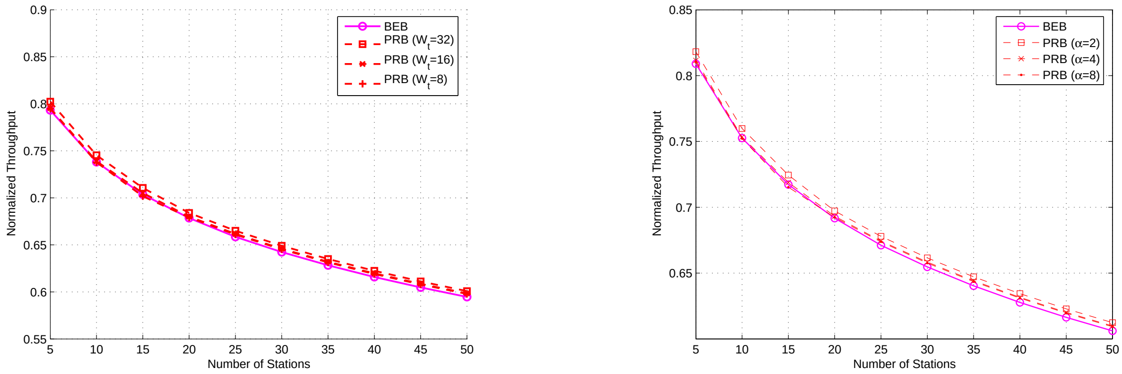
Fig. 7. Fairness Index vs. Number of Stations, when varying $\gamma$

the figures also show the total network throughput when using both schemes. As seen in Figure 5(a), when $\gamma = 0.2$ corresponding to $W_s = 6$, the normalized throughput for a selfish flow has dramatically decreased by $60\%$ (from $53\%$ using BEB to $24\%$ using PRB) when the number of stations is 5. As the number of stations increases, PRB still performs better than BEB. Similar results can be obtained from Figure 5(b). When the misbehavior is not very severe, i.e., $\gamma = 0.6$ (which corresponds to $CW_{min} = 19$) for a selfish station, the throughput of a selfish flow is slightly lower than a normal flow indicating the fairness index[12] is close to 1. Moreover, in terms of the total network throughput (designated as "Total"), PRB slightly outperforms BEB by $4\%$ ($\gamma = 0.2$) and $6\%$ ($\gamma = 0.6$). Note that, when BEB is used, the selfish flow achieves much higher normalized throughput over the normal flow of a well behaved station (as can be seen from Figure 5(a)).

Figure 6 shows the throughput analysis for PRB when varying the threshold $W_t$ and the increment factor $\alpha_l$ ($\alpha_l > 1$). As shown in Figure 6(a), the throughput for a selfish flow is continuously decreasing as $W_t$ increases. This is because, a selfish station needs to experience more states before it resets its contention window to $[0, CW_{min}]$ with higher $W_t$. For example, when $W_t = 4$, the throughput for a selfish flow is 0.46 whereas the normalized throughput is 0.24 when $W_t = 32$. This is due to the fact that a selfish node can still obtain more channel bandwidth by selecting a value equal to the threshold if $W_t$ is chosen small (a small $W_t$ allows a fast resetting of the lower bound of the contention window back to 0). Therefore, $W_t$ is required to be selected to a relatively larger value. Similarly, as shown in Figure 6(b), the throughput for a selfish flow is continuously decreasing as $\alpha_l$ decreases. For example, when $\alpha_l = 8$, the throughput for a selfish flow is 0.46 whereas it is 0.24 when $\alpha_l = 2$. This is due to the fact that, given a fixed threshold $W_t$, smaller $\alpha_l$ requires a node to experience more lower bound stages than a larger $\alpha_l$ which may result in a lower bound reaching the threshold ($W_t$) too

[11] For brevity, we only consider the basic access case in this section, i.e. two-way handshaking DATA/ACK.

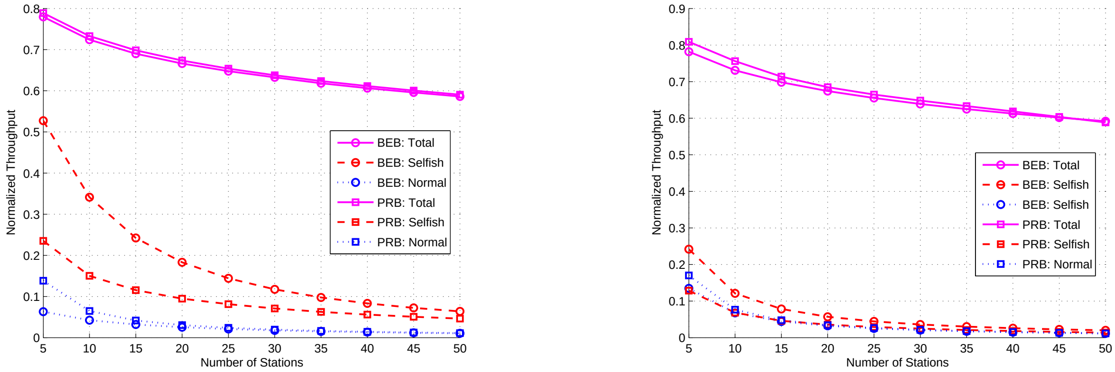
[12] Jain's fairness index [19] is given by: $F_J = \frac{(\sum_{i=1}^{N} T_i)^2}{N \sum_{i=1}^{N} T_i^2}$, where $N$ is the number of flows and $T_i$ is the throughput of a flow $i$. $F_J$ is equal to 1 when all the flows equally share the channel capacity, and is equal to $1/N$ when a single flow occupies the full bandwidth.



(a) Throughput analysis, varying $W_t$

(b) Throughput analysis, varying $\alpha_l$

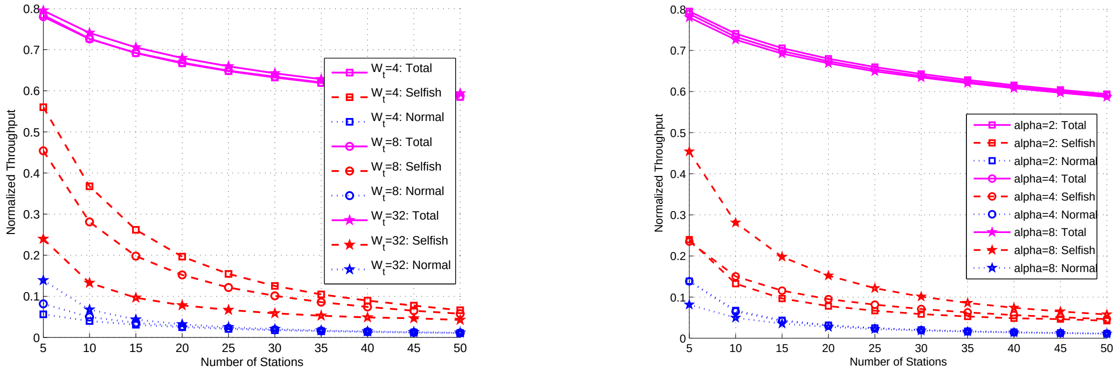
Fig. 4. Throughput vs. Number of Stations (Normal Case)



(a) $\gamma = 0.2$

(b) $\gamma = 0.6$

Fig. 5. Selfish/Normal Flow Throughput vs. Number of Stations (Attack Case, $W_t = 32$), when varying $\gamma$



(a) Throughput analysis, varying $W_t$

(b) Throughput analysis, varying $\alpha_l$

Fig. 6. Efficiency of PRB Parameters: $W_t$ and $\alpha_l$ ($\gamma = 0.2$)

fast.

Figure 7 compares the fairness index between BEB and PRB as a function of the number of stations when selecting the misbehavior coefficient $\gamma$ as $0.1$, $0.4$ and $0.7$ respectively. As seen from the figure, when $\gamma = 0.1$ (i.e., a severe attack), the fairness index for BEB varies from the range $(0.1, 0.3)$. However, the fairness index of PRB is quite close to $1$. As we increase $\gamma$, a selfish node will behave more normally resulting in a significantly increased fairness index, e.g., $F_J = 0.78$ when $\gamma = 0.4$ and $n = 5$ for BEB. Note that PRB still maintains a fairness index close to 1 in this case. Furthermore, as $\gamma$ equals to $0.7$ corresponding to $W_s = 22$ (close to normal case), $F_J$ for both BEB and PRB are close to 1. Moreover, it is clear that $F_J$ is increasing as the number of stations increases. This is due to the fact that, as more flows join in the network, both selfish and normal flows will face more collisions. This causes selfish flows to backoff more frequently than in a less congested environment, causing other well-behaved flows to have more chance to access the channel (as the number of well-behaved stations are much larger than selfish stations, e.g., $n_s = 1$ in this figure). Hence, there is an increase in the overall throughput for well-behaved flows. This clearly shows the superiority of PRB in achieving a fair access, and unlike BEB, to the channel among selfish and well behaved hosts.

## VI. NS-2 Simulation and Analysis

We use ns2 [9] to evaluate the performance of our proposed algorithm PRB. Although PRB is efficient regardless of the attack strategies an attacker might apply, e.g., deliberately choosing smaller $cw$ or larger $cw$, in the following discussion we only consider a selfish node that chooses smaller $cw$ in order to improve its own throughput while deteriorating the performance of other well-behaved flows.

### *A. Simulation Setup*

**Simulation Scenario:** a ring network with one node at the center and the rest nodes uniformly distributed on the circle. The ring radius is $200m$. All the nodes are fixed. The transmission range for each node is $250m$ and the carrier sense range is $550m$. Each node on the circle is the source of a single data flow and the source of each flow has the center point as the destination. The traffic type is constant bit rate (CBR). The packet size is $512bytes/packet$ and each flow has the same packet arrival rate. The channel bit rate is $2Mbps$. The total time for each simulation run is 500 seconds. Each data point on the following figures is averaged over 5 runs. The default parameters for PRB are configured as follows: $\alpha_l = 2$, $W_t = 31$, $CW_{lb}^{spec} = 4$.

To model the selfish misbehavior, we consider the worst case of PRB; that is a selfish source node always chooses a backoff $cw$ from $[CW_{lb} + 0, CW_{lb} + \gamma CW_{min}]$[13] ($\gamma \geq 0$), where $\gamma$ is the misbehavior coefficient indicating the percentage of deviation from the standard with a default value $0.1$.

**Simulation Metrics:** We use the following metrics to study the performance of our proposed approach:

- *Packet Delivery Ratio:* the ratio of the data packets successfully delivered to the destination by all the flows to those generated by the sources;
- *Average Packet Delay:* the average end-to-end delay for each successfully delivered data packet, which includes all the possible delays caused by route buffering, MAC interface queue, retransmission delays.
- *Fairness Index:* We use the Jain's fairness index as defined in [19].

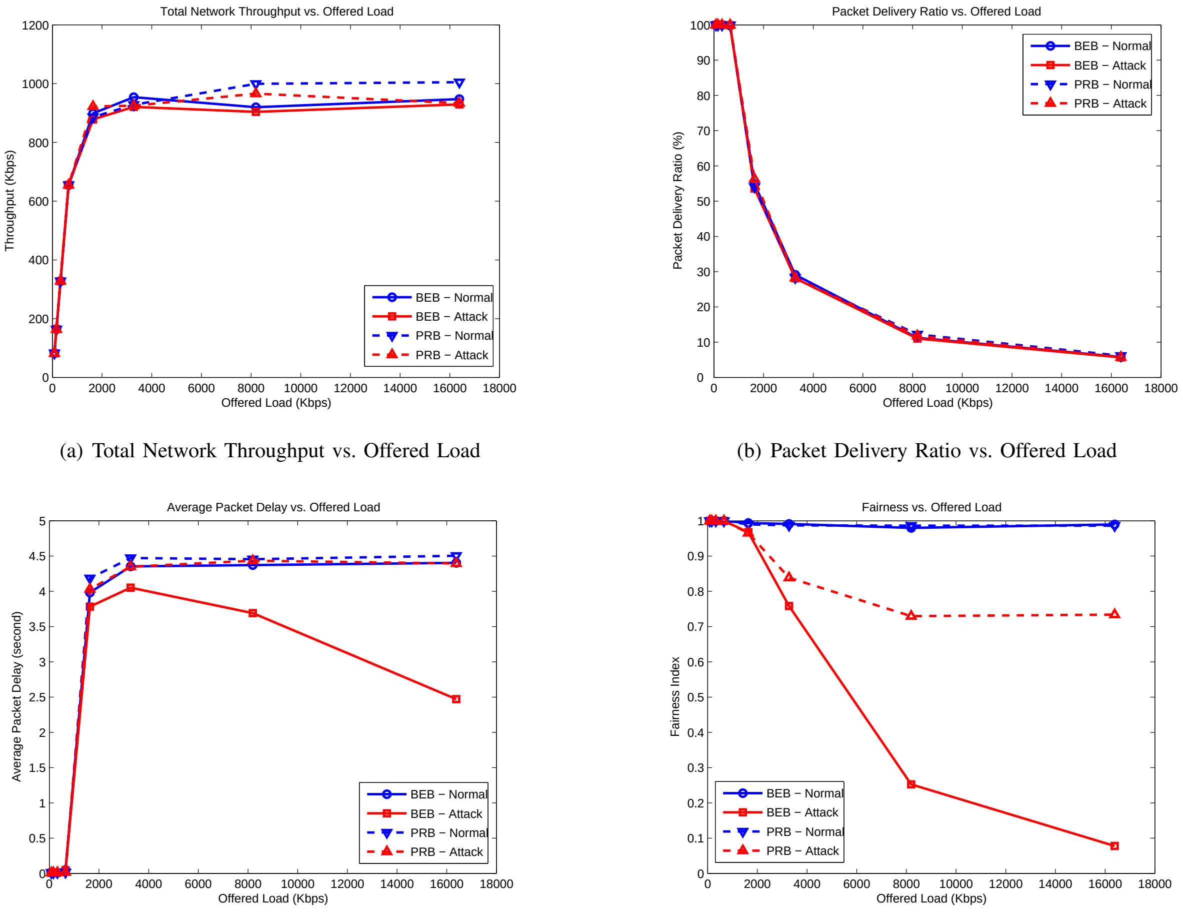
### *B. Simulation Results*

*1) Manipulation of CW:* We start our evaluation by comparing the overall network performance between BEB and PRB when varying the offered load. First, we observe that the total network throughput for BEB and PRB are similar under the normal case (designated as "Normal") and the attack case ("Attack") as shown in Fig. 8(a). Initially, when the channel is less congested, BEB and PRB perform identically in both cases. However, as the channel becomes more congested, e.g., when the offered load is $16386Kbps$, BEB and PRB exhibit different behavior. In either of the two cases (normal or attack), we notice that the increment of $CW$ lower bound (as in PRB) instead of resetting to 0 (as in BEB) will not cause performance penalty. On the contrary, it will slightly improve the total network throughput, e.g., the performance margin between BEB and PRB ranges from $20Kbps$ to $50Kbps$. This is due to the fact that, in a congested environment, a node may successfully send a packet after $i^{th}$[14] contention stages. Directly resetting the lower bound to 0 might cause this node to experience the same contention procedures again if the current channel maintains the same congestion conditions. Therefore, a gentle decrement of $CW$ is preferred [3] [8]; here, PRB shares a similar property with LMIMD [8] and SD [3] by forcing a node to choose a relatively large $cw$ than BEB. However, unlike LMIMD and SD which both focus on adaptively changing the upper bound of $CW$, PRB uses a different method by adjusting the lower bound. With proper selection of PRB parameters, we can achieve a much better throughput gain as discussed later. Similar results can be seen in Fig. 8(b) which shows the packet delivery ratio when varying the traffic load. Clearly, when the channel is less congested, in either BEB or PRB, all the generated packets can be successfully delivered to the destination which yields $100\%$ packet delivery ratio; alternatively, the delivery ratio decreases as the offered load increases.

Fig. 8(d) shows the results of fairness when varying the offered load. It is clear that BEB and PRB performs similarly when the offered load is below $2000Kbps$ with or without attack. This first proves the fact that selfish behavior has little impact in a less congested environment. Next, the fairness index of BEB sharply decreases as the offered load increases in the presence of attacks whereas PRB achieves higher and stable fairness index at higher loads; e.g., $F_J^{BEB} = 0.078$ and

[13] PRB is also efficient to mitigate other smart $cw$ selection strategy as we explained in III-B. For brevity, only naive attack strategy [11] that a node always selects a smaller $cw$, i.e., $0 \leq \gamma \leq 1$, is discussed in this section.

[14] Please refer to Section IV for details.



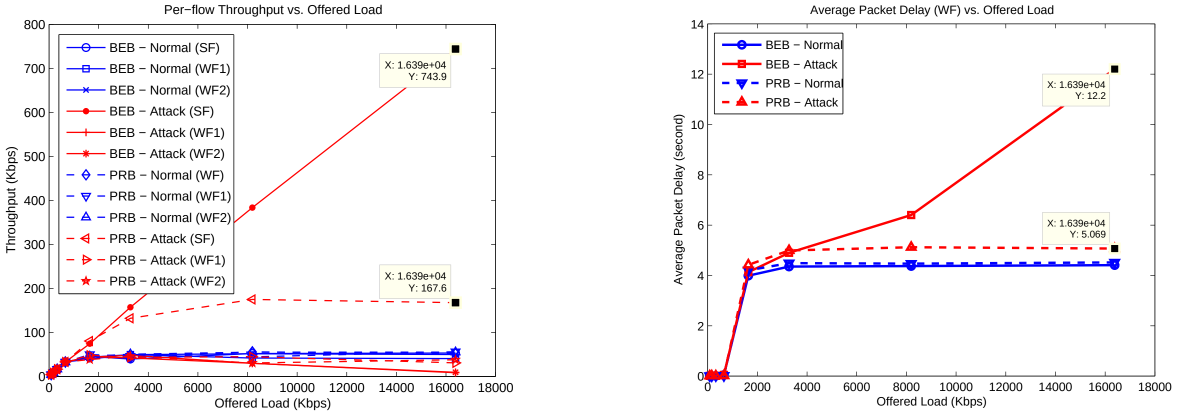
(a) Total Network Throughput vs. Offered Load

(b) Packet Delivery Ratio vs. Offered Load

(c) Average Packet Delay vs. Offered Load

(d) Fairness Index vs. Offered Load

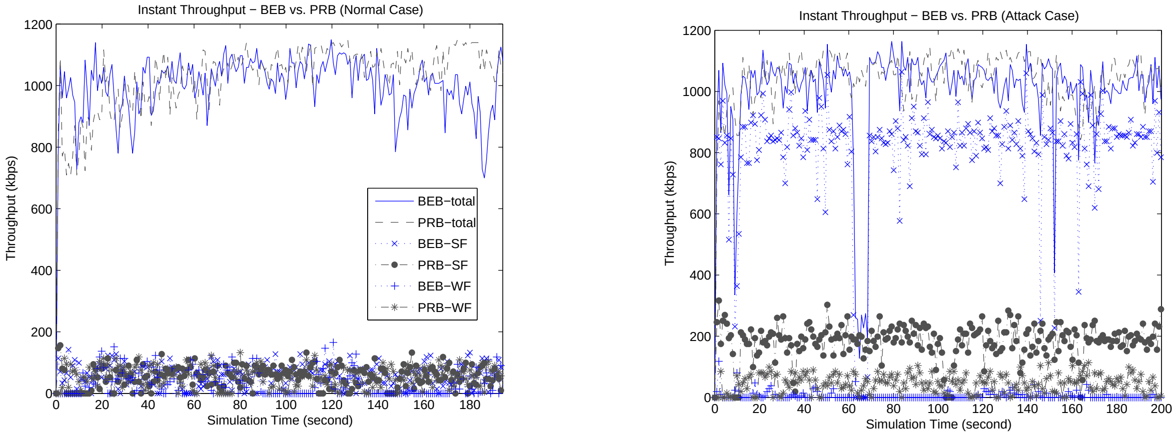
Fig. 8. BEB vs. PRB: Load Tests - Overall Network Performance



(a) Per-flow Throughput vs. Offered Load

(b) Per-flow End-to-end Delay vs. Offered Load

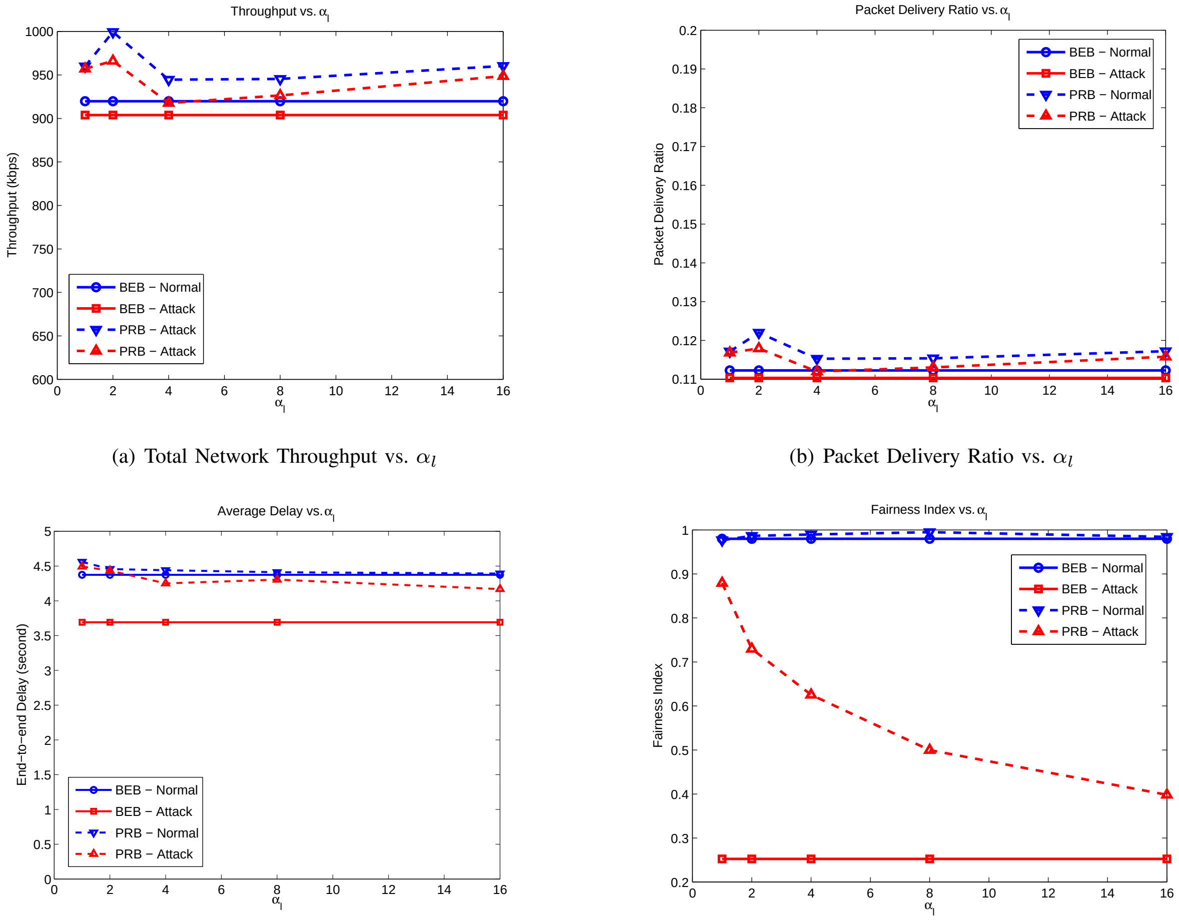
Fig. 9. BEB vs PRB: Load Tests - Per-flow Performance



(a) Normal Case

(b) Attack Case

Fig. 10. Instantaneous Throughput - BEB vs. PRB (Normal vs. Attack)



(a) Total Network Throughput vs. $\alpha_l$

(b) Packet Delivery Ratio vs. $\alpha_l$

(c) Average Delay vs. $\alpha_l$

(d) Fairness vs. $\alpha_l$

Fig. 11. Effects of varying $\alpha_l$

$F_J^{PRB} = 0.734$ when the load is $16386Kbps$. Once a node starts acting selfishly, it will increase its chance to capture the channel by selecting a much smaller $cw$ especially in a congested environment. This results in a continuous backoff of its neighboring nodes, which will allow the selfish flow to dominate the medium. Hence, the throughput of a selfish flow (*SF*) will keep increasing as the load increases which leads to a severe throughput degradation of well-behaved flows (*WF*), especially when the channel reaches to a saturated condition. Fig. 9 shows these results.

Fig. 9(a) shows the performance comparison between one selfish flow and two well-behaved flows (*WF*: *WF1* and *WF2*). Clearly, in BEB the *SF* throughput is continuously increasing as the load increases while the throughput for *WF1* and *WF2* is close to 0. This again shows that a *SF* can successfully exploit the protocol and take unfair advantage over other well behaved hosts. However, in PRB a *SF* throughput is significantly reduced and kept stable as the load changes; e.g., the *SF* throughput drops from $743.9Kbps$ (BEB) to $167.6Kbps$ (PRB) when the load is $16386Kbps$. Also, in PRB the delay for *SF* is close to that of *WF* and is kept stable at various loads. Moreover, the selfish behavior also results in a continuous backoff of neighboring nodes which will significantly reduce packet delays for the selfish flow and increased delays for the well-behaved flows as shown in Fig. 9(b). For example, in the presence of attacks, in BEB the averaged delay of well-behaved flows (designated as "WF") is $12s$ when the traffic load is $16386Kbps$ whereas in PRB the delay is reduced to $5s$. Since the selfish flow occupies a large portion of the total network bandwidth, e.g., 80% when the load is $16386Kbps$, it will also lead to a decreased average delay for the whole network as shown in Fig. 8(c). Table II arranges more detailed results on the per-flow performance in terms of normalized throughput (normalized over total network throughput) and end-to-end delays. We can see that PRB (designated as "**P**") significantly outperforms BEB (designated as "**B**"), e.g., when the load is $16386Kbps$, the normalized throughput of *SF* has dropped by over 75% and the average delay of *WF1* and *WF2* has reduced by over 56.8% and 57.5%. Hence, PRB is fairly efficient to deal with selfish hosts in a congested environment.

Fig. 10 shows the instantaneous throughput of a 20 flows scenario, where each flow is transmitting at $100pkt/s$. As shown in Fig. 10(a), under normal case, we see that there is no difference between BEB and PRB in terms of the total network throughput and the per-flow throughput. In the presence of a selfish host, the total throughput of BEB becomes unstable, e.g., the instantaneous throughput drops from $1000Kbps$ to $269Kbps$ during the period between 60s and 70s as shown in Fig. 10(b). This is because, when a selfish node selects a smaller $CW_{min}$, the selection of $cw$ in the presence of a failed transmission will be bounded by a smaller $CW$ upper bound ($2^i CW_{min}$). This results in a selfish host continuously selecting a very small $cw$ in a congested environment and may frequently collide with the other stations for a short period. However, in PRB the choice of a new $cw$ is bounded by both the lower bound and the upper bound. Therefore, a selfish host cannot keep on selecting a sequence of small $cw$ while avoiding the detection system. Fig. 10(b) shows that the total throughput of PRB is stable and is kept at $1000Kbps$. Furthermore, PRB successfully mitigates the impacts of the selfish host by reducing its throughput by 71%, i.e., from $800Kbps$ (BEB-SF) to $230Kbps$ (PRB-SF).

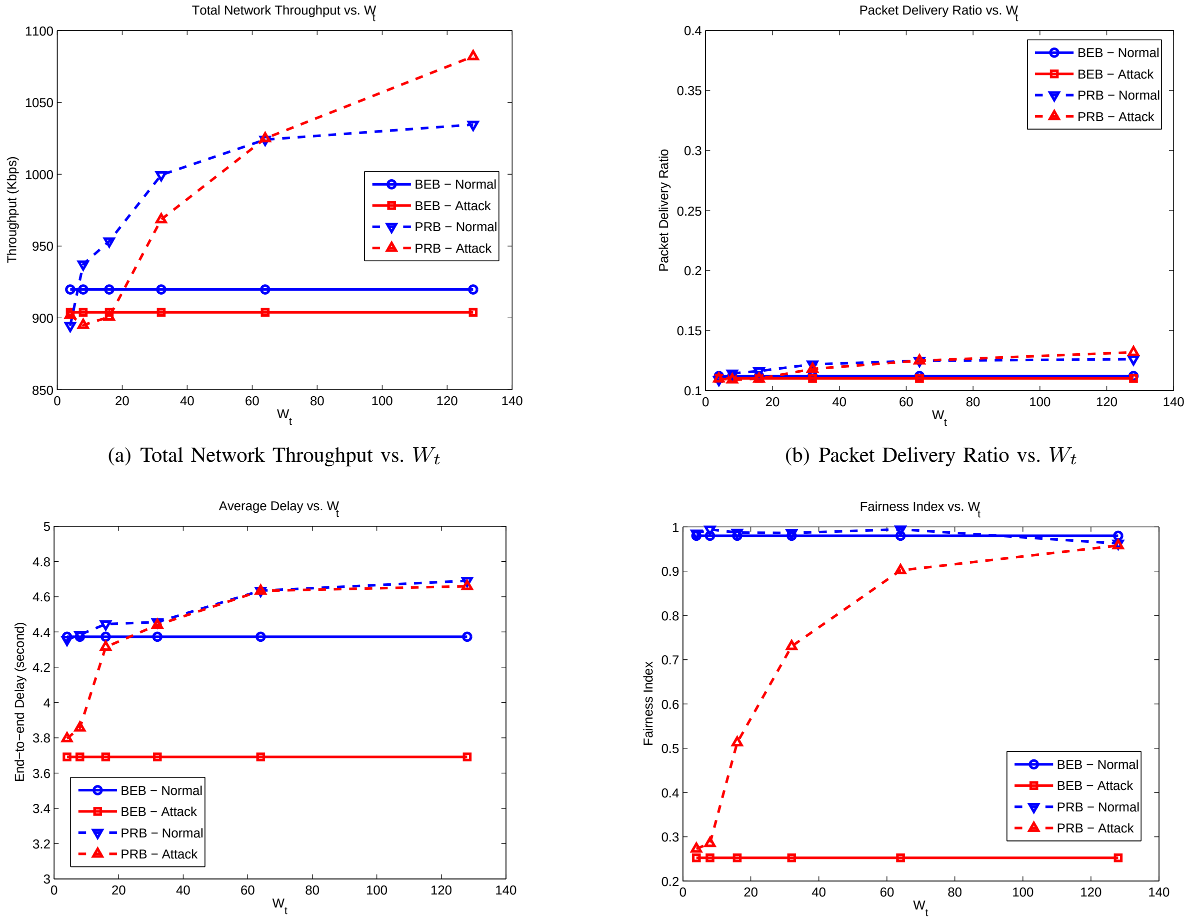
| Normalized Throughput vs. Load (Kbps) - BEB (**B**) vs. PRB (**P**) | | | | | | |
|---|---|---|---|---|---|---|
| Load | *SF*(**B**) | *WF1*(**B**) | *WF2*(**B**) | *SF*(**P**) | *WF1*(**P**) | *WF2*(**P**) |
| 82 | 0.04997 | 0.05167 | 0.05017 | 0.04884 | 0.05004 | 0.05164 |
| 163 | 0.04947 | 0.04997 | 0.05057 | 0.04991 | 0.04981 | 0.05051 |
| 327 | 0.05066 | 0.04973 | 0.05018 | 0.05004 | 0.04999 | 0.05014 |
| 655 | 0.05009 | 0.04996 | 0.05008 | 0.05037 | 0.04996 | 0.05012 |
| 1640 | 0.08455 | 0.04973 | 0.05115 | 0.08720 | 0.05206 | 0.04159 |
| 3278 | 0.17057 | 0.05234 | 0.04551 | 0.14289 | 0.04693 | 0.04997 |
| 8194 | 0.42429 | 0.03298 | 0.03292 | 0.18102 | 0.04624 | 0.03175 |
| 16386 | 0.80032 | 0.00907 | 0.01017 | 0.17949 | 0.03290 | 0.04060 |

| End-to-end Delay (second) vs. Load (Kbps) - BEB (**B**) vs. PRB (**P**) | | | | | | |
|---|---|---|---|---|---|---|
| Load | *SF*(**B**) | *WF1*(**B**) | *WF2*(**B**) | *SF*(**P**) | *WF1*(**P**) | *WF2*(**P**) |
| 82 | 0.00380 | 0.01302 | 0.01467 | 0.00416 | 0.01683 | 0.01166 |
| 163 | 0.00383 | 0.01020 | 0.04103 | 0.00413 | 0.01201 | 0.01166 |
| 327 | 0.00401 | 0.01273 | 0.00544 | 0.00460 | 0.01539 | 0.01980 |
| 655 | 0.00487 | 0.08186 | 0.01956 | 0.00601 | 0.01900 | 0.01877 |
| 1640 | 0.17129 | 4.02226 | 4.22241 | 0.07024 | 4.09403 | 4.47843 |
| 3278 | 0.04741 | 4.89544 | 5.02124 | 0.51656 | 5.08882 | 5.08355 |
| 8194 | 0.04393 | 6.77095 | 6.43815 | 1.34062 | 5.37855 | 5.27151 |
| 16386 | 0.06189 | 11.74258 | 13.10184 | 1.33668 | 5.06308 | 5.54411 |

TABLE II

PER-FLOW PERFORMANCE: BEB VS. PRB WHEN COMPARING ONE SELFISH FLOW *SF* WITH TWO WELL-BEHAVED FLOWS *WF1* AND *WF2*

We next explore the effects of varying PRB core parameters ($\alpha_l$, $W_t$); the results are presented in Fig. 11 and Fig. 12. In this scenario, 20 flows exist in the network with each flow sending packets at a rate of $2000pkt/s$ (i.e., highly congested environment). Fig. 11 shows that PRB can slightly improve the network throughput when choosing $\alpha_l$ larger or equal to 1, i.e., indicating an increased lower bound. When $\alpha_l$ equals to 2 the network throughput reaches its maximum in either attack or normal case (Fig.11(a)). Further, the use of $\alpha_l$ ($\alpha_l \geq 1$) in PRB results in better fairness than BEB with or without selfish hosts (Fig.11(d)). Another observation is that $F_j$ decreases as $\alpha_l$ increases. That is simply because a greedy increment of the lower bound of $CW$ (i.e., a large $\alpha_l$) will always result in a selfish host exceeding the threshold ($W_t$) very quickly which forces the host to reset its lower bound to 0 much faster. Hence, we suggest the use of a smaller $\alpha_l$ for effective performance of PRB. Fig. 12 illustrates the results when varying the threshold $W_t$. It is shown that when PRB is used, the network throughput is continuously improving as $W_t$ increases. First, we note that in a congested environment a node may experience several contention stages, which may result in doubling $CW$ upper bound ($CW_{ub}$) upon each failed transmission. Directly resetting $CW_{ub}$ to $CW_{min}$ after a successful transmission might force the node to experience the same contention as before. This is because the choice of a new $cw$ is bounded by $[CW_{lb}, CW_{ub}]$. Therefore, the margin between $CW_{ub}$ and $CW_{lb}$ determines the number of choices (i.e., $CW_{ub} - CW_{lb} + 1$) a node could have in selecting a new $cw$ for the next transmission. Given the same number of contending stations, a small margin clearly results in more collisions. Hence, a large margin is preferred when the number of contending stations and the traffic load are high. We should mention here that schemes such as LMIMD



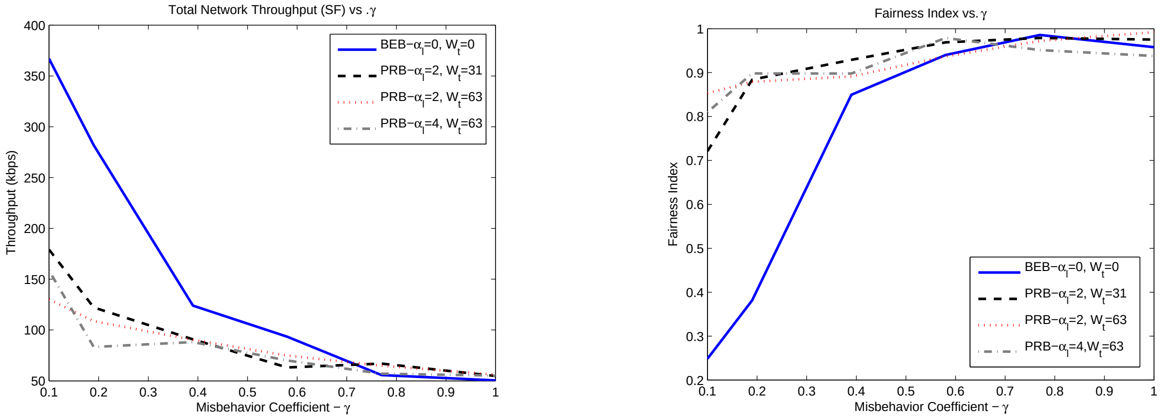
(a) Total Network Throughput vs. $W_t$

(b) Packet Delivery Ratio vs. $W_t$

(c) Average Delay vs. $W_t$

(d) Fairness vs. $W_t$

Fig. 12. Effects of varying $W_t$



(a) Per-flow Throughput vs. $\gamma$

(b) Fairness vs. $\gamma$

Fig. 13. Efficiency of PRB when varying $\gamma$

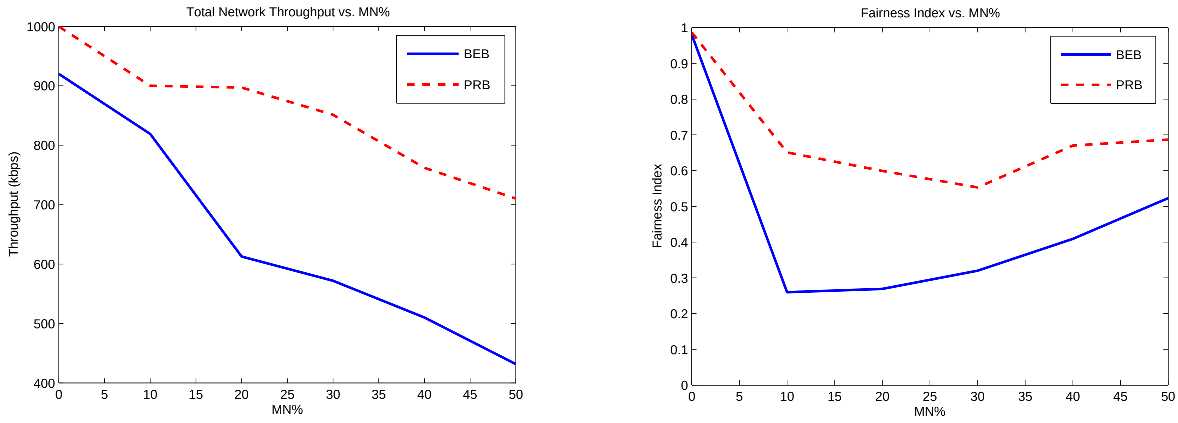
[8] and SD [3] are designed to address this issue. Another important factor which determines the contention frequency in any access protocol is $CW_{lb}$. In PRB, a large $CW_{lb}$ forces a node selecting $cw$ ($cw < W_t$) for the previous transmission to backoff for a longer duration for the next transmission. Alternatively, a station selecting $cw$ ($cw \geq W_t$) will have more chance to capture the channel for the next transmission because it will reset the lower bound of the contention window to its minimum. Therefore, increasing $W_t$ will enable the lower bound to reach a larger value; those nodes with larger lower bound will defer for a longer period and nodes with smaller lower bound will defer for a shorter period. This hence will result in splitting nodes into different groups each selecting its backoff from different contention ranges. Accordingly, the collision probability will be reduced and a higher throughput can be achieved, as shown in Fig.12(a). Notice also, a higher $W_t$ will also achieve better fairness (Fig.12(d)); a small $W_t$ will yield a quick reset for the lower bound to the default value (i.e., 0) whereas a large $W_t$ will force selfish hosts to select larger $cw$ giving more chance for well behaved hosts to access the channel. Figure 12(d) clearly shows a better fairness as $W_t$ increases. Now, although a larger $W_t$ achieves better fairness and a significant improvement of the total network throughput, that however comes at the cost of increased end-to-end delays due to the increment of lower bound as can be seen from Figure 12(c).

Fig. 13 compares the performance of BEB and PRB when varying the misbehavior coefficient $\gamma$ for different pair of PRB parameters. Clearly, PRB always outperforms BEB in terms of achieving fairness among competing flows (better fairness index) and in terms of the per-flow throughput, more specifically, the throughput for the selfish flow. As can be seen from the figure, when $\gamma = 1$ (no attack), the throughput for BEB-SF and PRB-SF is $55.99Kbps$ and $55.30Kbps$ respectively. However, under BEB, the throughput for *SF* increases rapidly as its misbehavior gets more intense. For example, when $\gamma = 0.1$, *SF* gets $367Kbps$ at the cost of severe degradation for *WF* throughput. On the other hand, in PRB, *SF* obtains $130Kbps$ ($\alpha_l = 2$ and $W_t = 63$) when $\gamma = 0.1$.

Fig. 14 illustrates the overall network performance between BEB and PRB when varying the number of misbehaved nodes (designated as $MN\% = \frac{NUM_{SelfishSTA}}{NUM_{TotalSTA}}$) in a 20-flow scenario ($\gamma = 0.1$). First, the results obtained by Fig. 14(a) show that the throughput of BEB and PRB decreases when increasing $MN\%$. Since the goal of each *SF* is to maximize its throughput, a selfish node will select a $CW$ as small as possible which will also exacerbate the unfairness among stations. When the number of stations acting selfishly increases, we observe a degradation in the network performance (Fig. 14(a) and Fig. 15(b)). For example, if we consider the worst case where each node in the network does not backoff ($cw = 0$), continuous collisions will occur and consequently no node can transmit any packet which will ultimately cause the whole network to collapse. Fig. 14(a) reflects this fact, where the misbehavior coefficient ($\gamma$) is 0.1. The figure shows that as the $MN\%$ increases, the total throughput (for BEB and PRB) decreases. Here, since the selection range for $cw$ is quite small, a larger number of MNs will obviously cause more collisions. PRB, however, reduces the effects by reducing the probability that a node selects a small $cw$ ($cw < W_t$); and hence PRB reduces the collision frequency caused by multiple selfish nodes by delaying their access to the channel. Also, this delay will help the well-behaved nodes to increase their access probability, i.e., during the backoff of selfish nodes there will be less contending stations and less selfish nodes.

An interesting observation can be seen in Fig. 14(b); that is in either BEB or PRB, the fairness index first decreases, however, it starts to increase when the $MN\% \geq 10\%$. As seen from its definition, $F_J$ represents the throughput margin between each individual flow, e.g., the higher the margin the lower the $F_J$. Initially, the appearance of multiple selfish nodes will exacerbate the contention situation for well-behaved nodes, resulting in further reduction of their throughput (as shown in Fig. 15(a)) which in turns indicates a reduction in $F_J$. However, as more and more $SF$ join the network, the payoff obtained by previously existing $SF$ will be reduced. Eventually, as the $MN\%$ increases, the network will converge to a point in which no significant payoff can be obtained by any $SF$; i.e., the channel is fairly shared by all the stations which again indicates an $F_J$ close to 1. Note that, although in this case all the nodes can access the medium with equal probability, the number of collisions might increase (due to the small range of $CW$)[15] which will consequently lead to a degradation of the total network throughput. This reflects by our results (as shown in Fig. 14) that the total network throughput continuously decreases as $MN\%$ although $F_J$ first decreases then starts to rise up. To further backup the results shown above, we illustrate the probability distribution $P_{cw}$ of selected contention window $cw$ in Fig. 16 for both the attack and normal cases using both BEB and PRB access protocols. In each scenario, the simulation time is $200s$, all the parameters are set to their default values and we compute the probability of $cw$ for each packet as a function of $cw$ which satisfies the relation: $\sum_{cw=0}^{CW_{max}} P_{cw} = 1$. First, as we can see from Fig. 16(a), PRB reduces the probability of the selection of small $cw$ because of the increment of $CW_{lb}$; e.g., the probability to choose a $cw < 10$ is reduced by 5%. Second, for contention windows where most transmission occur, $P_{cw}^{BEB}$ is close $P_{cw}^{PRB}$. These two observations show that: 1) for a very short period, (e.g., few seconds) PRB slightly degrades the total network throughput by reducing $P_{cw}^{PRB}$ where $cw$ is small; 2) for a long period (which is the general case for most applications), PRB will adaptively change $P_{cw}^{PRB}$ to increase the throughput, e.g., $P_{cw}^{PRB}$ is greater than $P_{cw}^{BEB}$ when $cw$ varies from 30 to 60. In case of attack, as shown in Fig. 16(b), $SF$ in BEB maintains a higher $P_{cw}$ than that of the $WF$. However, via the adjustment of $CW_{lb}$ in PRB, $P_{cw}$ of $SF$ has dropped by more than $40\%$ for $cw \leq 3$. Also, it is clear that $P_{cw}^{PRB}$ of $SF$ has been dramatically increased compared with $P_{cw}^{BEB}$ and is close to the normal case when $cw$ varies from 10 to 30 due to the default $W_t$. Overall, we conclude that PRB, and unlike BEB, could significantly improve the network performance in the presence of selfish nodes by

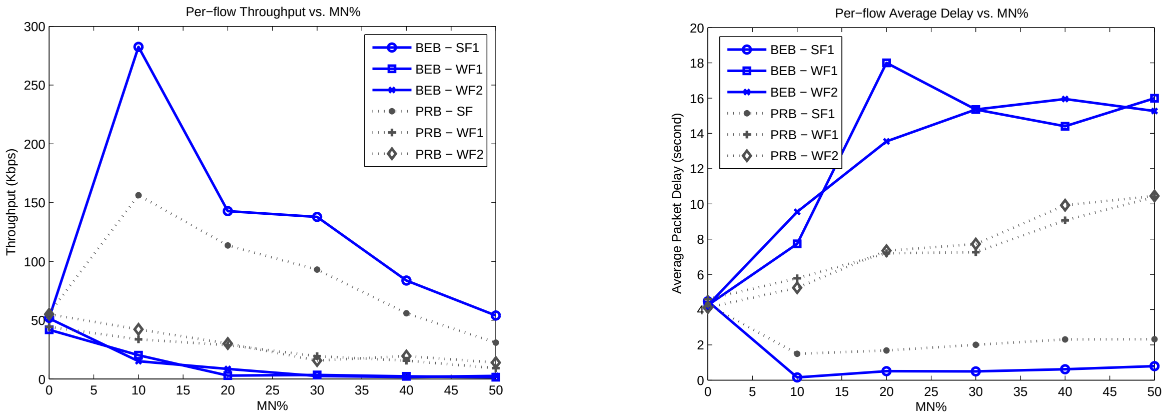
[15] It will depend on the number of contending stations and the position of these stations.



(a) Total Network Throughput vs. $MN\%$

(b) Fairness vs. $MN\%$

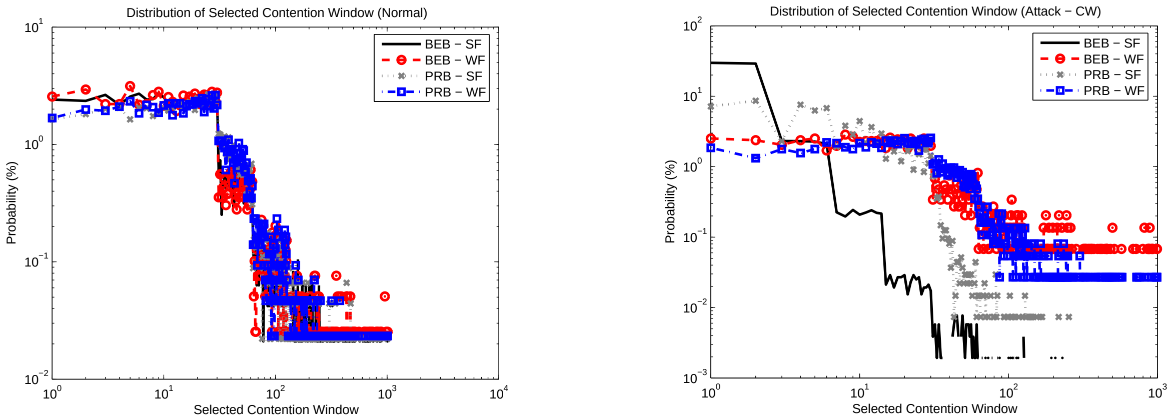
Fig. 14. Efficiency of PRB when varying MN%: Total Network Performance



(a) Per-flow Throughput vs. $MN\%$

(b) Per-flow Average Delay vs. $MN\%$

Fig. 15. Efficiency of PRB when varying MN%: Per-flow Performance



(a) Normal Case

(b) Attack Case

Fig. 16. Probability Distribution of Selected Contention Window $cw$: Manipulation of $CW$

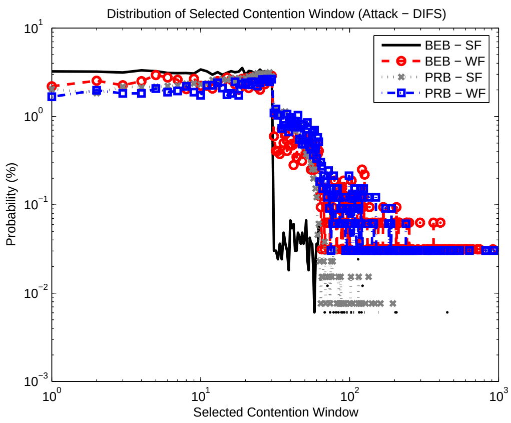


Fig. 17. Probability Distribution of Selected Contention Window $cw$: Manipulation of DIFS

adaptively changing the $CW_{lb}$. PRB however requires some minor modifications to the standard.

## VII. Conclusion and Future Work

Wireless medium access control (MAC) protocols currently deployed in MANET use distributed contention resolution mechanisms for sharing the wireless channel. In such environment, selfish hosts that fail to adhere to the MAC protocol may obtain an unfair share of the channel bandwidth at the expense of well-behaved hosts. In this paper we presented a Predictable Random Backoff (PRB) algorithm that is capable of reducing the impacts of selfish hosts on the network performance and in particular on well-behaved hosts. PRB is based on minor modifications for BEB and forces each node to generate a predictable backoff interval. Hosts that do not follow the operation of PRB are easily detected and isolated. We analytically evaluated PRB using a three-dimensional Markov chain model in order to derive the system throughout. Using both simulation and numerical results, we showed the accuracy of the developed model. We have also shown that PRB has similar performance to BEB under normal case and a superior performance and better fairness index in the presence of selfish hosts. We have presented detailed analysis of both access protocols in the presence and absence of selfish hosts.

For future work, we intend to further optimize the operation of PRB; for instance, throughput improvement could be achieved by more conservatively decreasing the contention window upon successful transmissions. We will also be looking at adaptively changing the threshold ($W_t$) in order to reduce the impacts of smart selfish nodes. We plan to further compare the performance of BEB and PRB with and without attack and considering mobility, the network size and traffic type. We also intend to look at the detection and reaction systems.

## Appendix

*a) case $j = 0$:* When $j = 0$, PRB and BEB behave similarly. In the presence of a failed transmission, a station will double its upper bound until reaching $CW_{max}$. According to the state balance condition, we can then write:

$$\begin{aligned}
b_{0,i,W_i-1} &= b_{0,i-1,0} \cdot \frac{p}{W_i} \\
b_{0,i,W_i-2} &= b_{0,i-1,0} \cdot \frac{p}{W_i} + b_{0,i,W_i-1} \\
&\vdots \\
b_{0,i-1,0} \cdot \frac{p}{W_i} + b_{0,i,1} &= b_{0,i,0} \cdot p + b_{0,i,0} \cdot (1-p) \\
&\quad \cdot (\frac{W_i - M_t}{W_i} + \frac{M_t}{W_i}) \\
b_{0,i-1,0} \cdot p &= b_{0,i,0}
\end{aligned} \tag{A-1}$$

where in (A-1) $j = 0$, $i \in (0, m)$, $k \in [0, W_i - 1]$. When $i = m$, $b_{0,m,0}$ can be written as:

$$\begin{aligned}
b_{0,m-1,0} \cdot p + b_{0,m,0} \cdot p &= b_{0,m,0} \cdot p + b_{0,m,0} \cdot (1-p) \\
&\quad \cdot (\frac{W_0(W_m - M_t)}{W_0 W_m} + \frac{(W_0 - M_1 + 1)M_t}{(W_0 - M_1 + 1)W_m}) \\
b_{0,m-1,0} \cdot p &= b_{0,m,0} \cdot (1-p)
\end{aligned} \tag{A-2}$$

where $j = 0$, $i = m$, $k \in [0, W_m - 1]$. When $i = 0$ and $k = 0$, $b_{0,0,0}$ is given by:

$$b_{0,0,0} = \sum_{j=0}^{t} \sum_{i=0}^{m} b_{j,i,0} \cdot \frac{(1-p)(W_i - M_t)}{W_i - M_j + 1} \tag{A-3}$$

Therefore, the relation between $b_{0,i,0}$ and $b_{0,i-1,0}$ is:

$$\begin{aligned}
b_{0,i,0} &= p^i b_{0,0,0} \\
b_{0,m,0} &= \frac{p^m}{1-p} b_{0,0,0}
\end{aligned} \tag{A-4}$$

By using (A-1) to (A-4), we derive the functions for $b_{0,i,k}$:

$$b_{0,i,k} = \frac{W_i - k}{W_i} \begin{cases} \sum_{j=0}^{t} \sum_{i=0}^{m} b_{j,i,0} \frac{(1-p)(W_i - M_t)}{W_i - M_j + 1} & i = 0 \\ p \cdot b_{0,i-1,0} & 0 < i < m \\ p \cdot (b_{0,m-1,0} + b_{0,m,0}) & i = m \end{cases} \tag{A-5}$$

where $k \in [0, W_i - 1]$.

*b) case $t \geq j > 0$:* First, from Figure 2 we can derive the relation between $b_{1,0,W_0-1}$ and $b_{0,0,0}$:

$$\begin{aligned}
b_{1,0,W_0-1} &= b_{0,0,0} \frac{M_t(1-p)}{W_0(W_0 - M_1 + 1)} + b_{0,1,0} \frac{M_t(1-p)}{W_1(W_0 - M_1 + 1)} \\
&\quad + \cdots + b_{0,m,0} \frac{M_t(1-p)}{W_m(W_0 - M_1 + 1)} \\
&= \frac{M_t(1-p)}{W_0 - M_1 + 1} (\frac{b_{0,0,0}}{W_0} + \frac{b_{0,1,0}}{W_1} + \cdots + \frac{b_{0,m,0}}{W_m}) \\
&= \frac{b_{0,0,0} M_t(1-p)}{W_0(W_0 - M_1 + 1)} (1 + \frac{p}{2} + \cdots + (\frac{p}{2})^{m-1} + \frac{(\frac{p}{2})^m}{1-p}) \\
&= \frac{b_{0,0,0} M_t(1-p)}{W_0(W_0 - M_1 + 1)} (\frac{1 - (\frac{p}{2})^m}{1 - \frac{p}{2}} + (\frac{p}{2})^m \frac{1}{1-p})
\end{aligned} \tag{A-6}$$

Next, we can obtain the relation between $b_{1,0,0}$ and $b_{1,0,W_0-1}$:

$$\begin{aligned}
b_{1,0,M_1-1} &= (W_0 - M_1 + 1) \cdot b_{1,0,W_0-1} \\
b_{1,0,M_1-1} &= b_{1,0,M_1-2} = \cdots = b_{1,0,1} \\
b_{1,0,1} &= b_{1,0,0} \cdot (1 - p + p) = b_{1,0,0}
\end{aligned} \tag{A-7}$$

From (A-6) and (A-7), we can easily write:

$$b_{1,0,0} = \frac{b_{0,0,0} M_t(1-p)}{W_0} (\frac{1 - (\frac{p}{2})^m}{1 - \frac{p}{2}} + (\frac{p}{2})^m \frac{1}{1-p}) \tag{A-8}$$

In the presence of a failed transmissions due to collision or packet failure, we have:

$$\begin{aligned} b_{1,1,W_1-1} &= b_{1,0,0} \cdot \frac{p}{W_1 - M_1 + 1} \\ b_{1,1,W_1-2} &= b_{1,1,M_1-1} + b_{1,0,0} \cdot \frac{p}{W_1 - M_1 + 1} \\ b_{1,1,M_1-1} &= b_{1,0,0} \cdot p \end{aligned} \tag{A-9}$$

As we can see in (A-9), a new random backoff counter is re-selected from the range $[M_1 - 1, W_1 - 1]$ (PRB) instead of $[0, W_1 - 1]$ (BEB). Therefore this reduces the chance that a station keeps on selecting smaller $cw$. Next, note that when the system reaches a state where $k = M_1 - 1$, it will continue on changing states with a probability of 1 until $k = 1$. Hence, we have the following:

$$b_{1,1,M_1-1} = b_{1,1,M_1-2} = \cdots = b_{1,1,1} \tag{A-10}$$

Further more, we can derive the following equations:

$$\begin{aligned} b_{1,1,1} &= b_{1,1,0} \cdot p + b_{1,1,0} \cdot \frac{(1-p)(W_1 - M_t)}{W_0(W_1 - M_1 + 1)} \cdot W_0 \\ &= b_{1,0,0} \cdot \frac{(1-p)(M_t - M_1 + 1)}{(W_0 - M_2 + 1)(W_1 - M_1 + 1)} \cdot (W_0 - M_2 + 1) \\ &= b_{1,1,0} \end{aligned} \tag{A-11}$$

In the presence of a failed transmission, we obtain:

$$b_{j,i,0} = b_{j,i-1,0} \cdot p \tag{A-12}$$

where $0 < i < m$. Similar to (A-4), we write:

$$b_{j,m,0} = \frac{p}{1-p} \cdot b_{j,m-1,0} \tag{A-13}$$

Next we consider the transitions between $b_{j-1,i,0}$ and $b_{j,0,k}$:

$$\begin{aligned} b_{2,0,W_0-1} &= b_{1,0,0} \frac{(M_t - M_1 + 1)(1-p)}{(W_0 - M_1 + 1)(W_0 - M_2 + 1)} \\ &+ \cdots + b_{1,m,0} \frac{(M_t - M_1 + 1)(1-p)}{(W_m - M_1 + 1)(W_0 - M_2 + 1)} \\ &= b_{1,0,0} \frac{(1-p)(M_t - M_1 + 1)}{W_0 - M_2 + 1} ( \frac{1}{W_0 - M_1 + 1} \\ &+ \frac{p}{W_1 - M_1 + 1} + \cdots + \frac{p^m}{W_m - M_1 + 1} ) \end{aligned} \tag{A-14}$$

By using the relations from (A-6) to (A-14), we write:

$$\begin{aligned} b_{j,0,0} &= b_{j-1,0,0}(1-p)(M_t - M_{j-1} + 1)( \frac{1}{W_0 - M_{j-1} + 1} \\ &+ \frac{p}{W_1 - M_{j-1} + 1} + \cdots + \frac{p^m}{W_m - M_{j-1} + 1} ) \\ &= \sum_{i=0}^{m} \frac{b_{j-1,0,0}(1-p)(M_t - M_{j-1} + 1)p^i}{W_i - M_{j-1} + 1} \end{aligned} \tag{A-15}$$

When $j = t$, upon a successful transmission the state $(t, i, 0)$ will always go back to $(0, 0, 0)$ with probability $1 - p$.

Next, according to the Markov chain regularities, for each $k \in [0, W_i - 1]$, $b_{j,i,k}$ can be written as (A-16) where $t \geq j > 0$.

- if $k \geq M_j - 1$, then

$$b_{j,i,k} = \frac{W_i - k}{W_i - M_j + 1} \begin{cases} \sum_{i=0}^{m} \frac{b_{j-1,i,0} M_t (1-p)}{W_i - M_j + 1} & i = 0 \\ p \cdot b_{j,i-1,0} & 0 < i < k \\ p \cdot (b_{0,m-1,0} + b_{0,m,0}) & i = m \end{cases} \tag{A-16}$$

- if $0 \leq k < M_j - 1$, then

$$b_{j,i,k} = b_{j,i,k+1} \tag{A-17}$$

## References

[1] IEEE802.11 wireless LAN media access control (MAC) and physical layer (PHY) specifications. 1999.

[2] I. Aad, J. P. Hubaux, and E. W. Knightly. Denial of service resilience in ad hoc networks. In *Proc. of ACM MobiCom*, September 2004.

[3] I. Aad, Q. Ni, C. Barakat, and T. Turletti. Enhancing IEEE 802.11 MAC in congested environments. In *Proceedings of IEEE ASWN*, Boston, 2004.

[4] G. Bianchi. Performance analysis of the IEEE 802.11 distributed coordination function. *IEEE Journal on Selected Areas in Communications*, 18(3):535–547, March 2000.

[5] S. Buchegger and J.-Y. L. Boudec. Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks). In *The ACM Symposium on Mobile Adhoc Networking and Computing (MOBIHOC 2002)*, Lausanne, Switzerland, June 9–11 2002.

[6] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux. On selfish behavior in CSMA/CA networks. *Proc. of INFOCOM*, March 2005.

[7] A. Cárdenas, S. Radosavac, and J. S. Baras. Detection and prevention of MAC layer misbehavior for ad hoc networks. In *ACM SASN*, October 2004.

[8] J. Deng, P. K. Varshney, and Z. J. Haas. A new backoff algorithm for the IEEE 802.11 distributed coordination function. *CNDS*, January 2004.

[9] K. Fall and K. Varadhan. NS notes and documentation. Technical report, UC Berkley, LBL, USC/ISI. In *Xerox PARC*, 2002.

[10] L. Guang and C. Assi. On the resiliency of ad hoc networks to MAC layer misbehavior. In *Workshop on PE-WASUN, ACM MSWiM*, October 2005.

[11] L. Guang and C. Assi. Mitigating smart selfish MAC misbehavior in ad hoc networks. In *Proc. of IEEE WiMob*, June 2006.

[12] L. Guang, C. Assi, and A. Benslimane. Interlayer attacks in mobile ad hoc networks. In *Proc. of Springer LNCS MSN*, December 2006.

[13] L. Guang, C. Assi, and A. Benslimane. Modeling and analysis of predictable random backoff in selfish environments. In *Proc. of ACM/IEEE MSWiM*, October 2006.

[14] V. Gupta, S. Krishnamurthy, and M. Faloutsous. Denial of service attacks at the MAC layer in wireless ad hoc networks. In *Proc. of MILCOM*, 2002.

[15] M. Heusse, F. Rousseau, R. Guillier, and A. Duda. Idle sense: an optimal access method for high throughput and fairness in rate diverse wireless LANs. *ACM SIGCOM*, August 2005.

[16] Y.-C. Hu, D. B. Johnson, and A. Perrig. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks*, 1(1):175–192, 2003.

[17] Y.-C. Hu and A. Perrig. A survey of secure wireless ad hoc routing. *IEEE Security & Privacy, special issue on Making Wireless Work*, May/June 2004.

[18] Y.-C. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for adhoc networks. In *Proc. of MobiCom*, September 2002.

[19] R. Jain. *The Art of Computer Systems Performance Analysis*. John Wiley and Sons, 1991.

[20] P. Kyasanur and N. Vaidya. Selfish MAC layer misbehavior in wireless networks. *IEEE Transactions on Mobile Computing.*, September 2005.

[21] P. Papadimitratos and Z. Haas. Secure routing for mobile ad hoc networks. In *Proc. of CNDS*, 2002.

[22] P. Papadimitratos and Z. Haas. Secure link state routing for mobile ad hoc networks. In *Proc. IEEE Workshop on Security and Assurance in Ad Hoc Networks*, 2003.

[23] M. Raya, J. P. Hubaux, and I. Aad. DOMINO: A system to detect greedy behavior in ieee 802.11 hotspots. In *Proc. of ACM MobiSys*, June 2004.

[24] S. Zhong, L. E. Li, Y. G. Liu, and Y. R. Yang. On designing incentive-compatible routing and forwarding protocols in wireless adhoc networks—an integrated approach using game theoretical and cryptographic techniques. In *Proceedings of the Eleventh ACM Annual International Conference on Mobile Computing and Networking (Mobicom)*, Cologne, Germany, August 2005.

[25] Y. Zhou, D. Wu, and S. Nettles. Analyzing and preventing MAC-layer denial of service attacks for stock 802.11 systems. In *Workshop on BWSA, BROADNETS*, October 2004.