Hindawi
Security and Communication Networks
Volume 2017, Article ID 2459780, 8 pages
https://doi.org/10.1155/2017/2459780

Research Article

The Performance Evaluation of an IEEE 802.11 Network Containing Misbehavior Nodes under Different Backoff Algorithms

Trong-Minh Hoang,[1] Van-Kien Bui,[2] and Thanh-Tra Nguyen[1]

[1]*Posts and Telecommunications Institute of Technology, Hanoi, Vietnam*
[2]*Panasonic R&D Center, Hanoi, Vietnam*

Correspondence should be addressed to Trong-Minh Hoang; hoangtrongminh@ptit.edu.vn

Received 11 July 2016; Revised 25 October 2016; Accepted 29 December 2016; Published 14 February 2017

Academic Editor: Francesco Gringoli

Copyright © 2017 Trong-Minh Hoang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Security of any wireless network is always an important issue due to its serious impacts on network performance. Practically, the IEEE 802.11 medium access control can be violated by several native or smart attacks that result in downgrading network performance. In recent years, there are several studies using analytical model to analyze medium access control (MAC) layer misbehavior issue to explore this problem but they have focused on binary exponential backoff only. Moreover, a practical condition such as the freezing backoff issue is not included in the previous models. Hence, this paper presents a novel analytical model of the IEEE 802.11 MAC to thoroughly understand impacts of misbehaving node on network throughput and delay parameters. Particularly, the model can express detailed backoff algorithms so that the evaluation of the network performance under some typical attacks through numerical simulation results would be easy.

1. Introduction

IEEE 802.11 based wireless networks are presented as one of the most widely deployed wireless technologies in the world to provide many applications for both special and commercial domains nowadays. The original IEEE 802.11 MAC layer employs the carrier sense multiple access/collision avoidance (CSMA/CA) protocol with binary exponential backoff algorithm to get fair multiple access [1]. To enhance the performance, several alternative backoff algorithms were proposed in recent years. Among them, the Exponential Increase Exponential Decrease (EIED) backoff algorithm can be substituted for BEB in some scenarios due to its good performance [2, 3].

Likely characteristics of common wireless networks, network performance of the IEEE 802.11 based network can be violated by several native or smart attacks from both inside or outside aspects. Particularly, the backoff procedure in a node can be affected by attacks that make a normal node become a malicious node, in which, backoff freezing problem comes to the serious issue while stopping backoff process of several nodes around the malicious node. However, to the best of our knowledge, previous analytical models did not consider the backoff freezing problem and EIED simultaneously. Furthermore, the performance of different backoff algorithms in IEEE 802.11 MAC layer misbehavior has been never compared in literature.

This paper proposes a novel analytical model to analyze and validate a saturated IEEE 802.11 wireless network employing BEB or EIED backoff algorithm in case of existing misbehavior nodes. Particularly, the numerical results of network performance for both BEB and EIED backoff algorithms are presented to compare in main parameters. The paper is organized as follows: In Section 2 we briefly review the state of the art of related studies. Section 3 presents our proposed analytical model. We adopt some main simulation results with our analysis in Section 4 and our conclusions and future works are drawn in Section 5.

2. Related Work

Network performance of IEEE 802.11 MAC is the interesting aim of recent studies because it is a base step to evaluate and improve the standard in varying application environments. To approach this, using analytical model is a traditional method due to its clarity. However, the accuracy and complexity of a model strongly depend on precise assumptions. Hence, the simple and accurate model proposed by Bianchi [4] has been initiated to number of papers which enhance more conditions for compensating accuracy such as the backoff freezing issue that has been fully considered in [5–7]. However, the previous proposals are focused to analyze the binary exponential backoff algorithm only.

An Exponential Increase Exponential Decrease backoff algorithm was proposed in [2] which has got several interesting characteristics. Numerical results in [2, 3] show that throughput improvement of IEEE 802.11 saturated network with EIED backoff algorithm overcame BEB backoff algorithm in the same conditions. Unfortunately, backoff freezing phenomenon in these studies has not been mentioned.

IEEE 802.11 MAC layer misbehavior can be caused by naive attack or smart attack in [8] and several attacks modify the backoff algorithm as declared in [9]. To the best of our knowledge, several proposals are based on the Markov chain [4] to validate network performance parameter for the case of having misbehavior nodes [10–12]. However, these models ignored the backoff freezing issue and investigated the BEB algorithm only. Hence, our analytical model is proposed to compensate a lack of previous studies for evaluating influenced performance under common attacks in terms of throughput and delay parameters.

3. The Proposed Analytical Model

3.1. The Backoff Algorithm State Model. Consider a single-hop IEEE 802.11 wireless network in saturated traffic condition. The network contains two kinds of node as normal node and misbehavior node, which contained cheating backoff rules. The number of nodes in the network is n, and the number of misbehavior nodes is l. The IEEE MAC layer is employed by BEB or EIED backoff algorithm in all normal nodes. Let τ_1, p_1, τ_2, p_2 be transmission probability and collision probability for two kinds of node, respectively. Note that any formula without notation (BEB) or (EIED) indicates that it is used for both cases of network using BEB and EIED algorithm. Denote by τ_1(BEB) the transmission probability of normal node when it employed BEB backoff algorithm and τ_1(EIED) for a normal node employing EIED backoff algorithm. Assume all channel in the network is no prone error and there is no hidden terminal problem.

The backoff state of a node employing BEB algorithm is modelled by a 2-dimension Markov chain [5]. Two stochastic processes are presented to backoff stages(t) and backoff time counter value $b(t)$. For convenience, let $W_{\min}$, $W_{\max}$, W_j denote $\mathrm{CW}_{\min} + 1$, $\mathrm{CW}_{\max} + 1$, and $\mathrm{CW}_j + 1$ in the jth retry/retransmission, m is the maximum backoff stage, and R is the maximum retry limit. The contention window size of BEB algorithm is illustrated as follows:

$$W_j = \begin{cases} 2^j W_0 = 2^j W_{\min}, & j \in [0, m-1],\ R > m \\ 2^m W_0 = 2^m W_{\min}, & j \in [m, R],\ R > m \\ 2^j W_0 = 2^j W_{\min}, & j \in [0, R],\ R \le m, \end{cases} \tag{1}$$

in which $m = \log_2(W_{\max}/W_{\min})$ and $W_{\min} = W_0$. The transmission probability of a normal node using BEB algorithm is given by

$$\tau_1 \text{ (BEB)} = \frac{1 - {p_1}^{R+1}}{1 - p_1} \frac{2}{\sum_{i=0}^{R} {p_1}^i \left(2^i W_0 + 1\right) - \left(1 - {p_1}^{R+1}\right)}. \tag{2}$$

The EIED backoff algorithm was introduced in [2], where the contention window size is doubled after every unsuccessful transmission and is halved after each successful transmission. Whenever the retry counter reaches the limit value, the CW is kept and not reset to zero. It can be described as follows.

After a successful transmission, the contention window decreases as a constant value r_D:

$$\mathrm{CW} = \max\left[\frac{(\mathrm{CW} + 1)}{r_D}, \mathrm{CW}_{\min} + 1\right] - 1. \tag{3}$$

After an unsuccessful transmission, the contention window increases as a constant value r_I:

$$\mathrm{CW} = \min\left[r_I \times (\mathrm{CW} + 1), \mathrm{CW}_{\max} + 1\right] - 1. \tag{4}$$

In this paper, we focus on a special case of EIED algorithm, where $r_I = r_D = 2$. A backoff state model of a node based on two-dimension Markov chain is illustrated in Figure 2. The state (i^+, k) indicates that a node has a successful transmission, and the state (i^-, k) indicates that a node stays in backoff process when a transmission is failed. Due to the anomalous slots, we can consider a window $W_i^+ = W_i - 1$ to include the first idle backoff slot after a successful transmission [5].

Denote by $b_{j,k} = \lim_{t\to\infty} \Pr\{s(t) = j, b(t) = k\}$ the stationary probability of backoff state (j, k). The probability that a node transmits during a generic slot time is equal to the sum of all stationary states with $k = 0$. The transition probabilities of the Markov model are given as follows:

$$\mathrm{P}\left\{i^+, k \mid i^+, k+1\right\} = 1, \quad k \in \left[0, W_i - 3\right],\ i \in [0, m-1]$$

$$\mathrm{P}\left\{i^-, k \mid i^-, k+1\right\} = 1, \quad k \in \left[0, W_i - 2\right],\ i \in [1, m]$$

$$\begin{aligned}
\mathrm{P}\left\{i^{+},k \mid (i+1)^{+},0\right\} &= \frac{(1-p)}{(W_i-1)}, \quad k \in [0,W_i-3],\ i \in [0,m-2]\\
\mathrm{P}\left\{i^{+},k \mid (i+1)^{-},0\right\} &= \frac{(1-p)}{(W_i-1)}, \quad k \in [0,W_i-3],\ i \in [0,m-1]\\
\mathrm{P}\left\{(i+1)^{-},k \mid i^{-},0\right\} &= \frac{p}{W_i}, \quad k \in [0,W_i-2],\ i \in [1,m-1]\\
\mathrm{P}\left\{(i+1)^{-},k \mid i^{+},0\right\} &= \frac{p}{W_i}, \quad k \in [0,W_i-2],\ i \in [0,m-1].
\end{aligned} \tag{5}$$

The first and second lines of 3.1 demonstrate that the backoff counter is decreased by 1 in duration times t and $t+1$. Four remaining equations in 3.1 show that the backoff stage is reduced by *1* after a successful transmission and increased by *1* after an unsuccessful transmission. Owing to the chain regularities, there is a simple relation between all states belonging to the same row (corresponding to the same stage i):

$$\begin{aligned}
b_{i^{+},k} &= \frac{W_i-k-1}{W_i-1}b_{i^{+},0};\\
b_{i^{-},k} &= \frac{W_i-k}{W_i}b_{i^{-},0}.
\end{aligned} \tag{6}$$

The equations in (7) and in (8) modelled the horizontal relation between all states that backoff counter is equal to zero:

$$\begin{aligned}
b_{i^{-},0} &= \left(b_{(i-1)^{+},0}+b_{(i-1)^{-},0}\right)\times p_1, \quad 2 \le i \le m-1\\
b_{i^{+},0} &= \left(b_{(i+1)^{+},0}+b_{(i+1)^{-},0}\right)\times (1-p_1), \quad 1 \le i \le m-2.
\end{aligned} \tag{7}$$

At the first and the last stage, we have

$$\begin{aligned}
b_{0^{+},0} &= \left(b_{0^{+},0}+b_{1^{+},0}+b_{1^{-},0}\right)\times (1-p),\\
b_{(m-1)^{+},0} &= b_{m^{-},0}\times (1-p),\\
b_{1^{-},0} &= b_{0^{+},0}\times p,\\
b_{m^{-},0} &= \left(b_{(m-1)^{-},0}+b_{(m-1)^{+},0}+b_{m^{-},0}\right)\times p.
\end{aligned} \tag{8}$$

By using an inductive method for this calculation, we obtain that

$$\begin{aligned}
b_{i^{+},0} &= \frac{{p_1}^{i+1}}{(1-p_1)^{i}}b_{0^{+},0},\\
b_{i^{-},0} &= \frac{{p_1}^{i}}{(1-p_1)^{i-1}}b_{0^{+},0}.
\end{aligned} \tag{9}$$

Denote $x = p_1/(1-p_1)$. Since all the states can be expressed as a function of the probabilities, by imposing the normalization condition, we can solve the Markov chain:

$$\begin{aligned}
1 &= \sum_{i=0}^{m-1}\sum_{k=0}^{W_i-2}b_{i^{+},k}+\sum_{i=1}^{m}\sum_{k=0}^{W_i-1}b_{i^{-},k}\\
&= \sum_{i=0}^{m-1}b_{i^{+},0}\frac{W_i}{2}+\sum_{i=1}^{m}b_{i^{-},0}\frac{W_i+1}{2}\\
&= \frac{b_{0^{+},0}}{2}\left(W_0+p\sum_{i=1}^{m-1}x^{i}W_i\right)\\
&\quad+\frac{b_{0^{-},0}}{2}\left((1-p)\sum_{i=1}^{m-1}x^{i}(W_i+1)+x^{m}(W_m+1)\right).
\end{aligned} \tag{10}$$

The transmission probability of a normal node when using EIED algorithm is

$$\tau_1\,(\mathrm{EIED}) = \sum_{i=0}^{m-1}b_{i^{+},0}+\sum_{i=1}^{m}b_{i^{-},0} = \frac{1-x^{m+1}}{1-x}b_{0^{+},0}. \tag{11}$$

Given the transmission probability of normal node τ_1 and misbehavior node τ_2, we can express a conditional collision probability of a normal node through a probability that a tagged node gets a transmission, which is originated by at least one of the contending nodes:

$$p_1 = 1-(1-\tau_1)^{n-l-1}(1-\tau_2)^{l}. \tag{12}$$

In common case, a misbehavior node always has an initiated backoff window smaller than in normal node. When misbehavior node has a fixed contention window mechanism, the contention window size is not changed in every backoff stage. Let W^{*} be equal to the contention window size of misbehavior node plus 1. The backoff counter of a selfish node is chosen randomly from *zero* to $W^{*}-1$. The transmission probability of a misbehavior node can be reduced from (1) as

$$\tau_2 = \frac{2}{(W^{*}+1)-(1-p_2)} = \frac{2}{W^{*}+p_2}. \tag{13}$$

The collision probability of misbehavior node is

$$p_2 = 1-(1-\tau_2)^{n-l}(1-\tau_2)^{l-1}. \tag{14}$$

Then, we can solve τ_1, p_1, τ_2, p_2 by using numerical method based on (8), (11), (12), (13), and (14) in the case of EIED algorithm.

3.2. Channel State Model. To model the IEEE 802.11 MAC in wireless multihop fashion, we clarify states around of a node by a channel state model. A backoff freezing process is

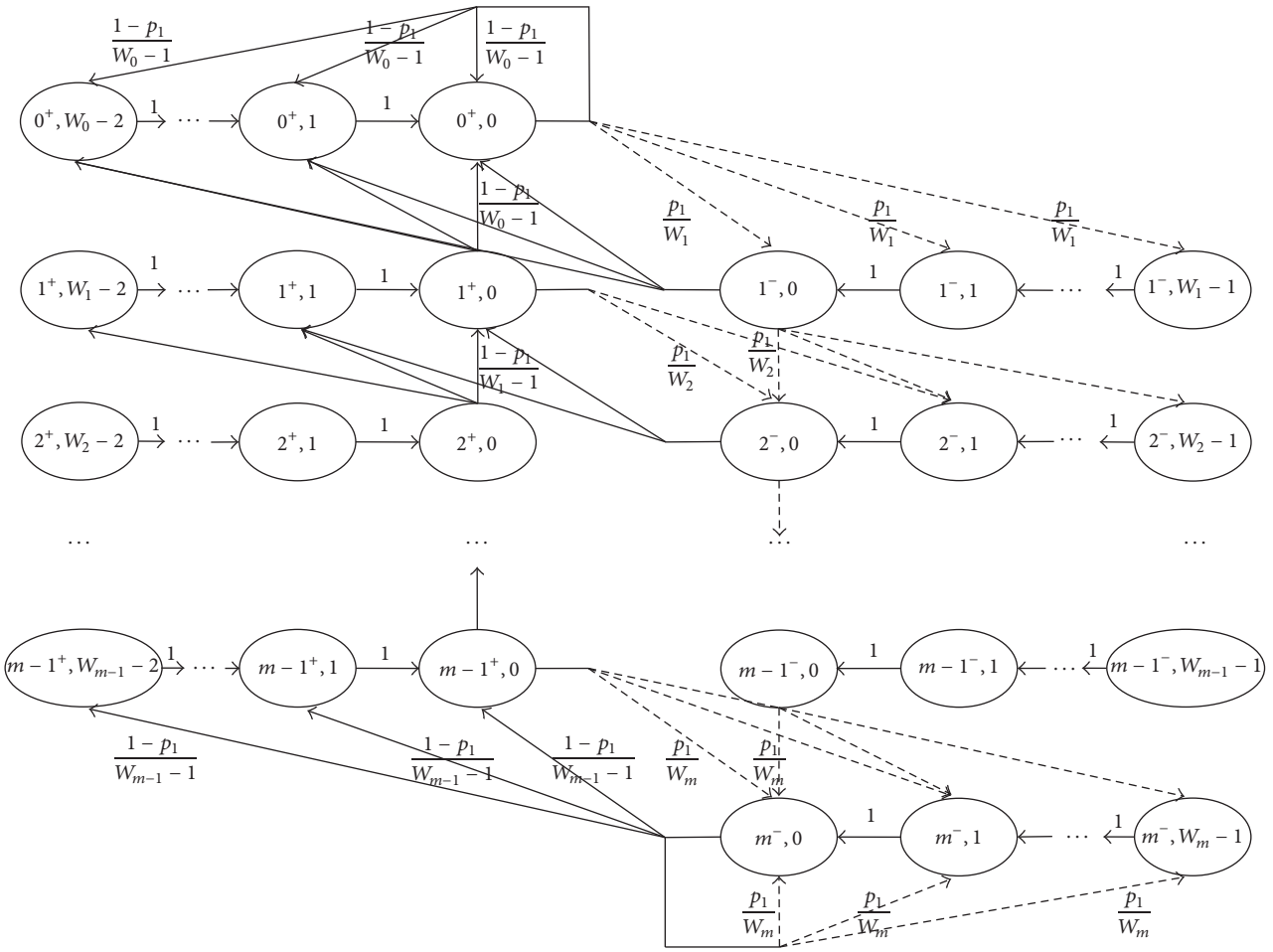


Figure 1: The backoff state model of a node employing EIED algorithm.

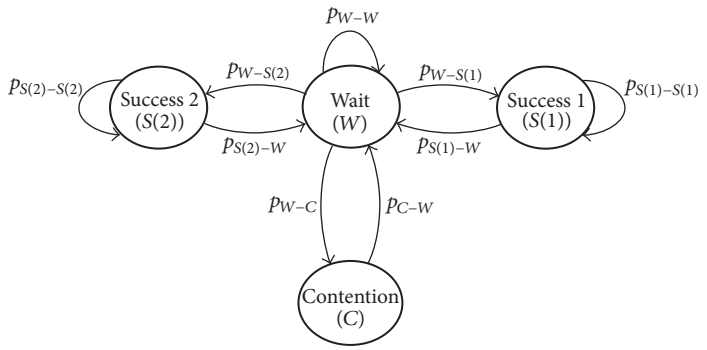


Figure 2: Channel state model.

modelled by a channel state model based on Markov chain in Figure 1. The four states are *Wait, Success 1, Success 2*, and *Contention*. *Wait* state is channel state in idle state; *Success 1* is channel state which presents a successful transmission of a normal node; *Success 2* is channel state which presents a successful transmission of a misbehavior node; and *Contention* is a channel state which presents a channel in collision process.

The transition probabilities are explained as follows.

Wait to Wait. It is the transition probability from state Wait to itself, and we have

$$p_{W-W} = (1-\tau_1)^{n-l}(1-\tau_2)^{l}. \tag{15}$$

Wait to Success 1. The channel is sensed busy because of a successful transmission of a normal node.

$$p_{W-S(1)} = (n-l) \times \left[\tau_1 (1-\tau_1)^{n-l-1}(1-\tau_2)^{l}\right]. \tag{16}$$

Wait to Success 2. A misbehavior node accesses the channel and initiates a successful transmission.

$$p_{W-S(2)} = l \times \left[\tau_2 \left(1-\tau_1\right)^{n-l} \left(1-\tau_2\right)^{l-1}\right]. \quad (17)$$

Wait to Contention. The channel experiences a collision due to some concurrent transmissions. Thus, the transition probability from *Wait* state to *Contention* state is

$$p_{W-C} = 1 - p_{W-W} - p_{W-S(1)} - p_{W-S(2)}. \quad (18)$$

Success 1 to Success 1. It is the event when a normal node transmits multiple consecutive packets. This event indicates the influence of DCF freezing/resumption process of the backoff counter. A normal node employing BEB algorithms always starts a transmission at the first backoff stage; hence

$$p_{S(1)-S(1)}\,(\text{BEB}) = \frac{1}{W_0}. \quad (19)$$

In case of using EIED algorithm, the probability that a node extracts a new zero backoff counter depends on the current backoff stage of this node. Denote by d_i the probability that a node transmits a new packet at backoff stage i. We have $d_0 = b_{0^+,0}$, $d_1 = b_{1^+,0}, \ldots, d_{m-1} = b_{(m-1)^+,0}$, and $d_m = b_{m^-,0} - (\sum_{i=0}^{m-1} d_i p_1^{m-i})$. A node can start a new transmission with zero backoff value if and only if its current state belongs to $(0^+, 0), (1^+, 0), \ldots, (m-1^+, 0)$. Therefore, this transition probability can be computed as

$$p_{S(1)-S(1)}\,(\text{EIED}) = \frac{\sum_0^{m-1} d_i \times (1/W_i)}{\sum_0^{m-1} d_i}. \quad (20)$$

Success 2 to Success 2. The probability that a misbehavior node extracts new zero backoff counter is

$$p_{S(2)-S(2)} = \frac{1}{W^*}. \quad (21)$$

The steady-state probabilities of Markov chain are determined as follows:

$$\begin{aligned}
&\pi_W \\
&= \frac{1}{1 + p_{W-C} + p_{W-S(1)}/\left(1 - p_{S(1)-S(1)}\right) + p_{W-S(2)}/\left(1 - p_{S(2)-S(2)}\right)} \\
&\pi_C = \pi_W \times p_{W-C}; \\
&\pi_{S(1)} = \pi_W \times \frac{p_{W-S(1)}}{1 - p_{S(1)-S(1)}}; \\
&\pi_{S(2)} = \pi_W \times \frac{p_{W-S(2)}}{1 - p_{S(2)-S(2)}}.
\end{aligned} \quad (22)$$

The average length of stationary state of channel model is calculated as

$$E[T] = \pi_W T_W + \pi_C T_C + \left(\pi_{S(1)} + \pi_{S(2)}\right) T_S. \quad (23)$$

Here, T_s is the time the channel is sensed busy because of a successful transmission, T_c is the time the channel is sensed busy by each station during a collision, and T_w is the duration of an empty slot time.

From the view of a node, the average slot duration in the backoff countdown process is greater than $E[T]$ because of the freezing backoff issue. Hence,

$$E\,[\text{slot}] = \frac{E\,[T]}{\pi_W}. \quad (24)$$

3.3. Performance Parameters. In this section, we derive throughput, packet drop rate, and delay performance metrics as follows.

(a) Throughput Analysis. The saturation throughput of network is defined as the fraction of channel occupied and successfully transmitted payload bits:

$$\text{Th} = \left(\pi_{S(1)} + \pi_{S(2)}\right) \times \frac{E\,[P]}{E\,[T]}. \quad (25)$$

The normalized throughput of a normal node and a misbehavior node can be expressed as follows:

$$\begin{aligned}
\text{Th}_1 &= \frac{\pi_{S(1)}}{n-l} \times \frac{E\,[P]}{E\,[T]}, \\
\text{Th}_2 &= \frac{\pi_{S(2)}}{l} \times \frac{E\,[P]}{E\,[T]}.
\end{aligned} \quad (26)$$

(b) Packet Drop Probability. The packet drop probability is defined as the probability that a packet is dropped when the retry limit is reached and it is equal to

$$\begin{aligned}
P_{\text{drop1}} &= p_1^{R+1}, \\
P_{\text{drop2}} &= p_2^{R+1}.
\end{aligned} \quad (27)$$

(c) Access Delay Analysis. The average packet delay for a successfully transmitted packet is defined to be the time interval from the time the packet is at the head of its MAC queue ready to be transmitted, until an acknowledgement for this packet is received. The packet delay of a normal node employing BEB algorithm is calculated similar to study in [13], in which $E[T_{\text{drop}}]$ is the average number of slot times required for a packet to experience $R + 1$ collisions in the $(0, 1, \ldots, R)$ retry stages. Thus, $T_{\text{delay}}(\text{BEB}) = E[T_{\text{drop}}] \times E[\text{slot}]$.

$$\begin{aligned}
&T_{\text{delay1}}\,(\text{BEB}) \\
&= \sum_{j=0}^{R} \left(\frac{W_j + 1}{2} \times \frac{p_1^j - p_1^{R+1}}{1 - p_1^{R+1}}\right) \times E\,[\text{slot}]\,.
\end{aligned} \quad (28)$$

The packet delay of a normal node using EIED algorithm is

$$T_{\text{delay1}}\,(\text{EIED}) = \frac{\sum_{i=0}^{m} T_i \times d_i}{\sum_{i=0}^{m} d_i}, \quad (29)$$

Table 1: Simulation parameters.

Physical slot time σ	9 μs
SIFS	16 μs
DIFS	34 μs
PHY header	128 bits
MAC header	160 bits
Retry limit	7
Basic rate R_{basic}	6 Mbps
Data rate R_{data}	6 Mbps
L_{ACK}	304 bits
$E[P]$	12000 bits
CW_{min}	15
CW_{max}	1023

where T_i is the average delay when a normal node starts at the ith stage in the backoff process, with the probability density function being equal to d_i. For each i, T_i is calculated as follows:

$$T_i = \sum_{j=0}^{R} \left(\frac{W_{\min(i+j,m)} + 1}{2} \times \frac{{p_1}^j - {p_1}^{R+1}}{1 - {p_1}^{R+1}} \right) \times E\,[\text{slot}]\,. \quad (30)$$

Similarly, the packet delay of misbehavior node is given by

$$T_{\text{delay}(2)} = \sum_{j=0}^{R} \left(\frac{W^* + 1}{2} \times \frac{p_2^j - p_2^{R+1}}{1 - p_2^{R+1}} \right) \times E\,[\text{slot}]\,. \quad (31)$$

4. Numerical Results and Discussions

To validate the network performance of two backoff algorithms for both normal node and malicious node in a saturated wireless single-hop network, we use MATLAB Tool to verify throughput, packet drop probability, and packet delay parameters. Analytical results will be examined under standard parameters of the IEEE 802.11a as shown in Table 1.

Let L_{DATA} be the average length of DATA packet, $L_{\text{DATA}} = H + E[P]$, where H is the length of header which composes physical header and MAC header. The transmission durations of DATA and ACK packets are $T_{\text{DATA}} = L_{\text{DATA}}/R_{\text{data}}$; $T_{\text{ACK}} = L_{\text{ACK}}/R_{\text{basic}}$. With the basic mechanism, the time durations of each steady-state T_W, T_S, T_c are given by

$$\begin{aligned} T_W &= \sigma \\ T_C &= T_{\text{DATA}} + \text{SIFS} + T_{\text{ACK}} + \text{DIFS} \\ T_S &= T_{\text{DATA}} + \text{SIFS} + T_{\text{ACK}} + \text{DIFS}. \end{aligned} \quad (32)$$

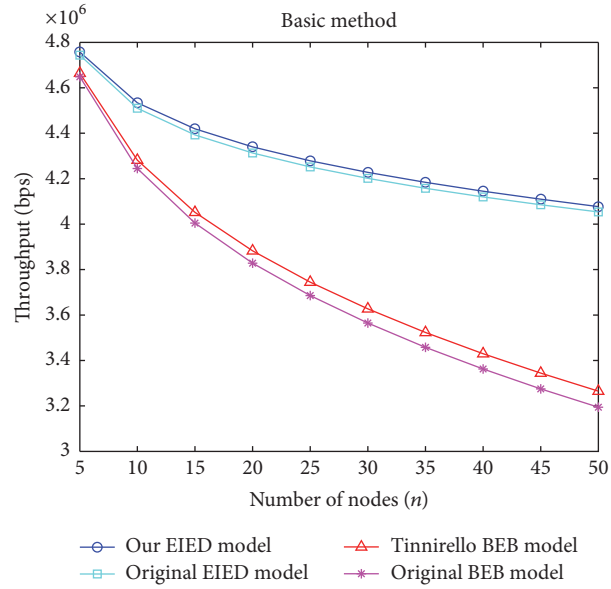


Figure 3: Network throughput versus number of nodes.

Firstly, we verify network throughput in basic mechanism under backoff freezing phenomenon with previous studies in the same input parameters. As seen in Figure 3, the EIED algorithm can provide a better throughput more than BEB algorithm as proven in [2, 3]. Notably, the backoff freezing issue does not change significantly throughput curve but keeps good value when the number of nodes increases in this case.

A misbehavior node chooses a backoff with fixed window to gain more opportunity of channel preemption. We illustrate the normal node throughput and malicious node throughput for both BEB and EIED algorithms. We consider a network containing 12 nodes with one malicious node and its contention window varying from 2 to 32 as shown in Figure 4. We can see that the throughput of cheating node decreases very fast when W^* value increases. In addition, misbehavior node in network utilizing EIED algorithm achieves higher throughput than the case of BEB algorithm.

Figures 5 and 6 show the delays and packet drop rates of the different backoff algorithms by varying network size. We consider two cases: a network having one malicious node whose contention window is equal to 8 and a normal network without any malicious nodes. A misbehavior node always keeps a smaller delay and packet drop rate because its opportunity of channel occupation is higher. Although EIED algorithm can provide a better total throughput and reduce packet drop probability, the throughput and delay parameters when having a malicious node in network are worse than in BEB algorithm. Therefore, we can conclude that in the case of using EIED algorithm the fairness of network is reduced if there is an attack at MAC layer.

5. Conclusion

Our presented contribution in this paper is twofold. Firstly, we propose a novel analytical model to model IEEE 802.11

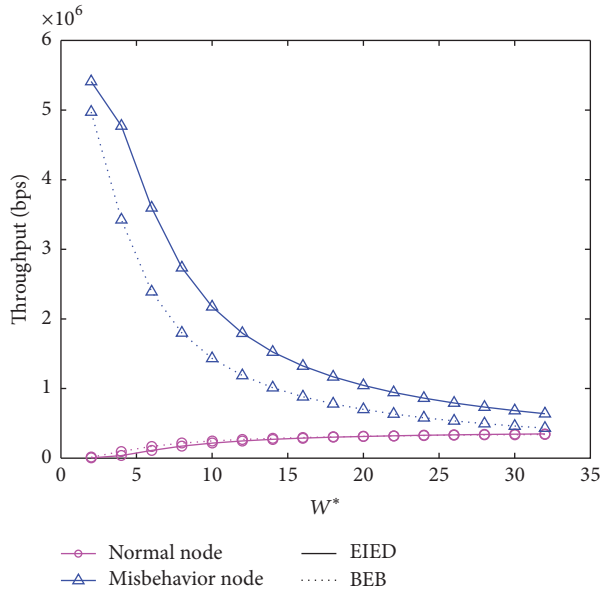


Figure 4: Single node throughput versus contention window size.

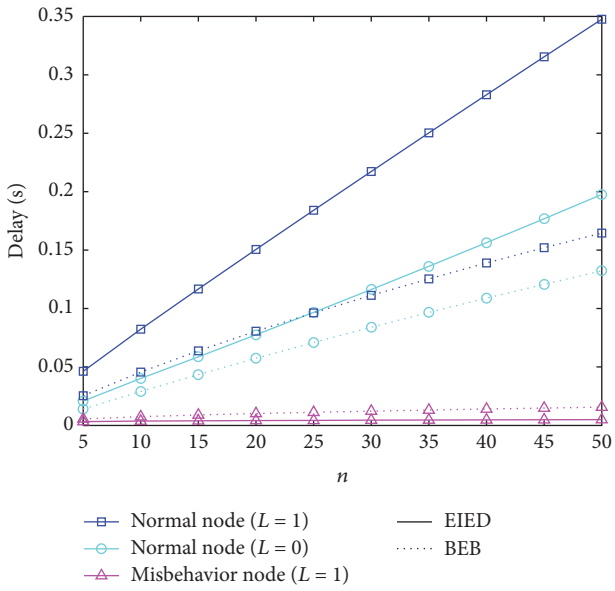


Figure 5: Delays versus number of nodes.

MAC employing EIED backoff algorithms with freezing backoff phenomenon covered. Secondly, the network performance of different backoff algorithms under common attacks at MAC layer is studied through numerical results. We can see that the performance of EIED backoff algorithm is better than that of BEB algorithm under normal condition. However, when the network contained malicious node, the network performance metrics of the network employing BEB backoff algorithm are better than those when employing EIED algorithm. In our next works, these network performance metrics will be validated by a discrete simulation tool.

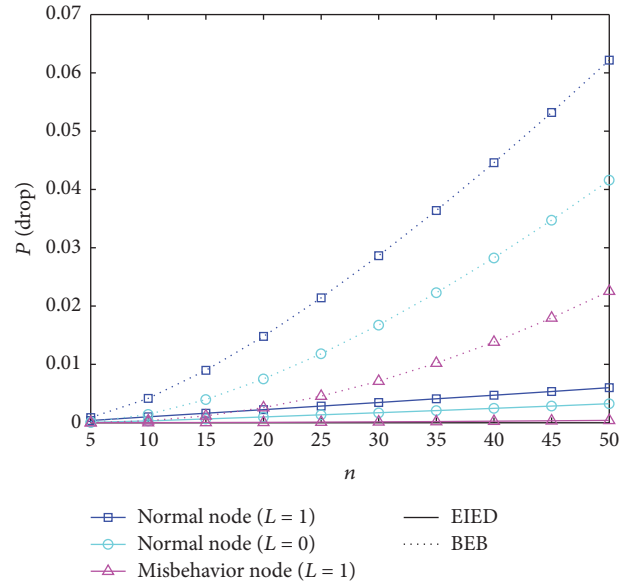


Figure 6: Packet drop rate versus number of nodes.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this article.

References

[1] IEEE, "IEEE standard for 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," IEEE Standard 802.11-2007, 2007, Revision of IEEE Std 802.11-1999.

[2] H. Wu, Y. Peng, K. Long, S. Cheng, and J. Ma, "Performance of reliable transport protocol over IEEE 802.11 wireless LAN: analysis and enhancement," in *Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '02)*, vol. 2, pp. 599–607, IEEE, New York, NY, USA, June 2002.

[3] C. Ye, Y. Li, and A. Reznik, "Performance analysis of exponential increase exponential decrease back-off algorithm," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '10)*, pp. 1–6, Miami, Fla, USA, December 2010.

[4] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535–547, 2000.

[5] I. Tinnirello, G. Bianchi, and Y. Xiao, "Refinements on IEEE 802.11 distributed coordination function modeling approaches," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 3, pp. 1055–1067, 2010.

[6] H. Chen, "Revisit of the Markov model of IEEE 802.11 DCF for an error-prone channel," *IEEE Communications Letters*, vol. 15, no. 12, pp. 1278–1280, 2011.

[7] T.-M. Hoang, V.-K. Bui, and T. Nguyen, "Analyzing impacts of physical interference on a transmission in IEEE 802.11 mesh networks," in *Proceedings of the 9th International Conference on Telecommunication Systems Services and Applications (TSSA '15)*, pp. 1–6, November 2015.

[8] L. Guang, C. Assi, and A. Benslimane, "MAC layer misbehavior in wireless networks: challenges and solutions," *IEEE Wireless Communications*, vol. 15, no. 4, pp. 6–14, 2008.

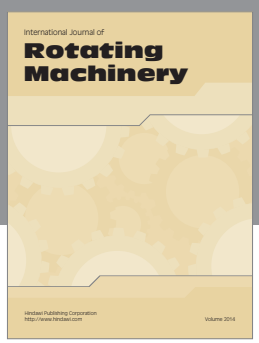
[9] V. R. Giri and N. Jaggi, "MAC layer misbehavior effectiveness and collective aggressive reaction approach," in *Proceedings of the 33rd IEEE Sarnoff Symposium 2010*, 5, 1 pages, April 2010.

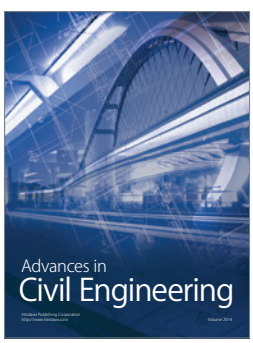
[10] C. Liu, Y. Shu, W. Yang, and O. W. W. Yang, "Throughput modeling and analysis of IEEE 802.11 DCF with selfish node," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '08)*, pp. 1–5, New Orleans, La, USA, December 2008.

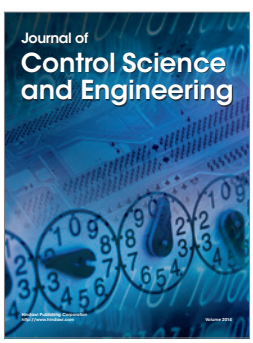
[11] C. Liu, Y. Shu, M. Li, and O. W. W. Yang, "Delay modeling and analysis of IEEE 802.11 DCF with selfish nodes," in *Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '08)*, pp. 1–4, Dalian, China, 2008.

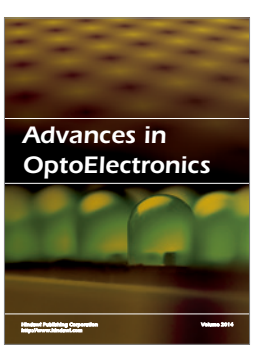
[12] K.-J. Park, J. Choi, K. Kang, and Y.-C. Hu, "Malicious or selfish? analysis of carrier sense misbehavior in IEEE 802.11 WLAN," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, vol. 22, pp. 351–362, 2009.

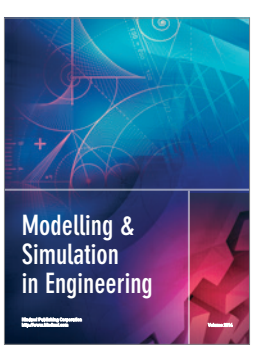
[13] P. Chatzimisios, A. C. Boucouvalas, and V. Vitsas, "IEEE 802.11 packet delay: a finite retry limit analysis," in *Proceedings of the IEEE Global Communication Conference (GLOBECOM '03)*, vol. 2, pp. 950–954, San Francisco, Calif, USA, December 2003.

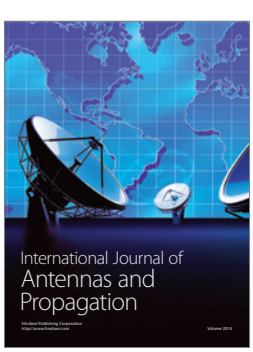


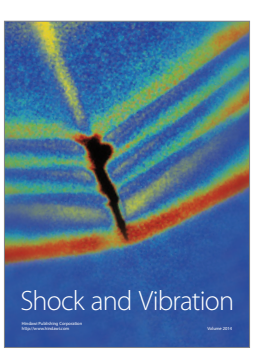


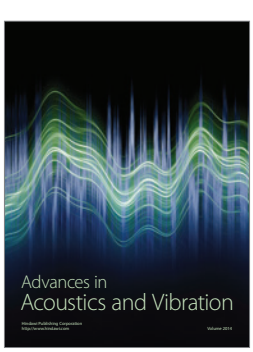












Hindawi

Submit your manuscripts at
https://www.hindawi.com