EUROPEAN TRANSACTIONS ON TELECOMMUNICATIONS
Euro. Trans. Telecomms. **00**: 1–5 (2010)
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/ett.0000

Wireless Systems

Detecting Backoff Misbehaviour in IEEE 802.11 EDCA

Szymon Szott[1]*, Marek Natkaniec[1] and Roberto Canonico[2]

[1]*Department of Telecommunications, AGH University of Science and Technology, Krakow, Poland*
[2]*Consorzio Interuniversitario Nazionale per l'Informatica - University Frederico II, Napoli, Italy*

SUMMARY

In this paper, we suggest the use of the chi-square test for detecting backoff misbehaviour in IEEE 802.11 EDCA networks. A performance evaluation is performed to compare the chi-square test with two other methods, known in the literature. To perform a suitable comparison, these two methods are extended to support EDCA and the BEB mechanism. We assume a misbehaviour model, which can be easily executed by a selfish user. We show that the chi-square test outperforms the other methods in terms of the probability of misbehaviour detection and time required to positively identify a misbehaving node. Copyright © 2010 AEIT

1. INTRODUCTION

The IEEE 802.11 standard [1] for wireless networks does not provide users with incentives to cooperate when accessing the shared radio channel. Therefore, non-cooperative actions, known as misbehaviour, may become a serious problem. One of the prominent examples of misbehaviour is cheating on the backoff procedure, i.e., a deliberate change of backoff parameters defined in the standard in order to increase the chance of accessing the medium and, as a result, increase throughput. This type of misbehaviour is hidden from detection schemes working at the network layer and can be combined with misbehaviour in upper layers. It is easy to perform because the medium access function, which governs the backoff procedure, can be modified through the wireless card driver. The latest drivers, e.g., [6], allow changing these parameters through the command line. Even equipment vendors can make non-standard modifications to increase the performance of their cards (as reported in [4]). Additionally, new opportunities to misbehave occur in Enhanced Distributed Channel Access (EDCA), one of the medium access functions of IEEE 802.11. EDCA provides Quality of Service (QoS) for both infrastructure and ad-hoc wireless networks. It defines new medium access parameters and therefore provides previously overlooked opportunities to misbehave. Consequently, we address the problem of detecting users who have manipulated their backoff parameters in IEEE 802.11 EDCA.

Several papers have studied the problem of detecting backoff misbehaviour. They are based on recording the observed backoff values of a node and determining whether they are standard compliant. Depending on the detection method they can be classified into the following groups: mean test [2, 5, 8], entropy test [2], sequential probability ratio test [10, 14] and Kolmogorov-Smirnov test [3, 9].

The main disadvantage of existing solutions is that none of them take into account the binary exponential backoff (BEB) feature of 802.11. Furthermore, only [8, 9] consider EDCA albeit in a limited scope. Other methods can be extended to support EDCA, though none of them have been evaluated with EDCA parameters. Some papers (such as [5]) consider only infrastructure WLAN scenarios. Other solutions may be difficult to implement, because they are

*Correspondence to: Szymon Szott, Department of Telecommunications, AGH University of Science and Technology, Al. Mickiewicza 30, 30-059 Krakow, Poland. E-mail: szott@kt.agh.edu.pl

Received
Revised
Accepted

computationally expensive (such as [3, 10]) or based on measured throughput [14].

In this paper, we propose an alternative method for detecting backoff misbehaviour which i) takes BEB into account, ii) considers EDCA, iii) can be used in ad-hoc and infrastructure scenarios, iv) is based on a valid statistical test for determining uniformity and v) is computationally inexpensive.

To verify our approach we compare it with two methods previously proposed in the literature: the mean and entropy tests. We extend these methods to support BEB and EDCA. The evaluation is performed using a realistic misbehaviour model, i.e., such which does not require driver modifications and can be performed by an ordinary WLAN user.

The remainder of this paper is structured as follows. EDCA is briefly described in Section II. The detection tests are presented in Section III. The performance evaluation is given in Section IV. Section V concludes the paper.

2. EDCA

EDCA introduces four Access Categories (ACs) to provide appropriate QoS. These categories are, from the highest priority: Voice (Vo), Video (Vi), Best effort (BE), and Background (BK). Each category has its own set of medium access parameters, which are responsible for traffic differentiation. These parameters are: the Arbitrary Inter-frame Space ($AIFS$), the Contention Window Minimum and Maximum values (CW_{min} and CW_{max}), and the Transmission Opportunity Limit ($TXOP_{Limit}$). The first and last parameter assume fixed values. Therefore, deviation from them is easy to detect. However, detecting deviations from the CW parameters is challenging because they are responsible for the randomness of the backoff procedure, which works as follows.

A node randomly selects a value from the range $[0, CW]$. The initial value of CW is defined by the parameter CW_{min}. The chosen backoff value denotes the time slot in which the node will begin its transmission. The decreasing of this value begins when the channel has been idle for an $AIFS$ period. The countdown is paused when the channel is sensed busy. When the backoff value reaches zero, the node starts to transmit. In order to avoid collisions the BEB mechanism is used. If a collision occurs, CW is doubled until it reaches CW_{max}. A successful transmission resets CW to the value of CW_{min}. This mechanism decreases the probability that two nodes will transmit simultaneously and thus cause a collision.

3. DETECTING BACKOFF MISBEHAVIOUR

We attempt to detect backoff misbehaviour by comparing the measured and expected distributions of backoff values. The most important quality of a backoff distribution is that it is uniform within certain ranges: $[0, CW_{min}], [CW_{min} + 1, 2 \times (CW_{min} + 1) - 1]$, etc. For example, the ranges for the Voice AC are $[0, 7]$ and $[8, 15]$ for IEEE 802.11b. If a node is cheating on the CW values, the distribution of its backoff value will not be uniform within these ranges. Therefore, to detect misbehaviour, it is necessary to perform a uniformity test. To this end we propose the use of the chi-square test which is a typical goodness of fit test for discrete distributions. Firstly, after measuring S backoff samples for each backoff range, we put the observed samples into C_{χ^2} cells. The expected number of samples in each cell is $E = S/C_{\chi^2}$. Secondly, we compute the chi-square statistic

$$\chi^2 = \sum_{i=1}^{R_{AC}} \sum_{j=1}^{C_{\chi^2}} \frac{(O_{i,j} - E_{i,j})^2}{E_{i,j}} \tag{1}$$

where $O_{i,j}$ and $E_{i,j}$ are the observed and expected number of samples in cell j of range i, respectively and R_{AC} is the number of ranges of a given AC. We reject the hypothesis that the observed samples are uniform within the backoff ranges and we assume that the node is misbehaving if

$$\chi^2 > \chi^2_{\alpha, R_{AC}C_{\chi^2}-1} \tag{2}$$

where $\chi^2_{\alpha, R_{AC}C_{\chi^2}-1}$ is a chi-square distribution with $R_{AC}C_{\chi^2} - 1$ degrees of freedom at a significance level α. For the chi-square test, to provide accurate results, the minimum required number of expected samples should be at least E_{min}. It is common to assume $E_{min} = 5$ [7].

To assess the performance of the chi-square test, we compare it with two other tests: the mean test and the entropy test. The former was used in [2, 5, 8], the latter in [2]. We attempted to use the method of [9], however, we could not reach convergence for large CW values.

In the mean test the mean of the observed backoff values (M_{obs}) is compared to the expected mean of the backoff values (M_{ex}). A node is misbehaving if $M_{obs} < \gamma_m M_{ex}$, where γ_m is a tunable parameter which determines the amount of false positives.

The entropy test is a uniformity test based on the entropy for discrete uniform distributions. To decrease the parameter space, the samples observed in each range are put into C_H cells. The entropy of the observed backoff values (H_{obs}) of the C_H cells is calculated to determine if the distribution is uniform. The expected entropy is $H_{ex} = -log_2(\frac{1}{C_H})$. A node is misbehaving if $H_{obs} < \gamma_e H_{ex}$, where γ_e is a tunable parameter which determines the amount of false positives.

4. PERFORMANCE EVALUATION

In order to assess the performance of the chi-square test, we simulate a monitoring station. The monitoring station can observe the channel in promiscuous mode, capture traffic sent by other stations, and extract information on the chosen backoff value. In infrastructure networks the AP can be the monitoring station, whereas in ad-hoc networks each station can monitor its neighbours. We assume perfect estimates of the chosen backoff values. This allows us to evaluate the performance of the chi-square test and compare it to other tests. The problem of how to correctly measure backoff values in a real environment is beyond the scope of this paper. We refer the reader to [5, 9]

Let us denote μ as the misbehaviour coefficient. A misbehaviour strategy of setting $CW_{min}^{misb} = CW_{max}^{misb} = \mu$ would be very simple to detect, since all collected samples would be in the first range. Therefore, to perform a meaningful assessment of the detection tests, we assume the following misbehaviour strategy:

$$\begin{cases} CW_{min}^{misb} = \mu \\ CW_{max}^{misb} = 2^{R_{AC}-1}(\mu + 1) - 1 \end{cases} \tag{3}$$

This strategy can be easily used, because it requires only changing the initial values of CW_{min} and CW_{max}, and not the backoff mechanism. The latest drivers, e.g., [6], allow changing these parameters through the command line.

The ns-2 simulator was used with an enhanced version of the EDCA patch described in [13]. The following ad-hoc scenario was considered. Within a single-hop network there were five transmitting stations and one monitoring station. The 802.11b physical layer was assumed. In particular, the following values of (CW_{min}, CW_{max}) were used for Vo, Vi, BE, and BK: $(7, 15)$, $(15, 31)$, $(31, 1023)$, and $(31, 1023)$, respectively [1]. Each station continuously attempted to transmit 1000 byte packets. Based on the gathered information the monitoring station evaluated the random backoff values with the chi-square, mean and entropy tests. The tests were performed separately for each AC. The probability of false positives P_{FP} was set through the following parameters: $\gamma_m = \gamma_e = 95\%$, $\alpha = 5\%$ and $E_{min} = 5$. Our preliminary study showed that the chi-square and entropy tests perform best for $C_{\chi^2} = C_H = 4$.

In the figures, we refer to Vo and Vi as high priority and BE and BK as low priority. Furthermore, we present misbehaviour M in the form of a percentage which we calculate as $M = \lfloor \frac{CW_{min}-\mu}{CW_{min}-1} \rfloor \times 100\%$. It is obvious that the misbehaving user would choose $\mu \in [1, CW_{min} - 1]$ in order to increase the probability of channel access. Additionally, because $\mu \in \mathbb{N}$, there is a limited number of possible simulation points. Each simulation run was repeated 100,000 times. The standard deviation of the results is either presented in the figures or was too small for graphical representation.

The performance evaluation is performed with the following three simulation scenarios:

1) In order to calculate the probability of detection P_D, we simulate backoff values limited by the CW parameters in Equation 3. P_D is the ratio of the number of simulation runs in which misbehaviour was detected successfully to the total number of simulation runs. Figure 1 presents P_D for three observation periods with respect to the percentage of misbehaviour for the chi-square test. To increase legibility, only the Voice AC is presented in the figure. For other ACs the behaviour is similar. The main conclusion is that the detection rate is high for misbehaviour greater than 25%. Furthermore, there is a trade-off between the detection time and the accuracy of the model for low levels of misbehaviour.

2) The second series of simulations was performed to determine the time required to achieve $P_{FP} < 5\%$. To calculate P_{FP}, we simulated a scenario with no misbehaviour and calculated the probability that in such a case the test would erroneously detect misbehaviour. The results, presented in Figure 2 clearly show the advantage of the chi-square test. It is on average three times quicker in detecting misbehaviour than the mean and entropy test.

3) In the final simulations, we compared the time needed to detect misbehaviour, i.e., so that $P_D > 95\%$. This was done under the condition that $P_{FP} < 5\%$. The results were gathered for μ close to the standard values of CW_{min} for each AC (Table 1). For higher values of μ the misbehaviour is $M = 0\%$. For almost all simulation points the chi-square test requires the shortest observation period to detect misbehaviour. Only for the lowest possible misbehaviour the chi-square test requires more time than the entropy test. It must be noted, however, that in these situations the throughput gain from misbehaviour is the lowest (e.g., for Vi and $M = 7\%$ the throughput gain is approximately 2%).

DOI: 10.1002/ett

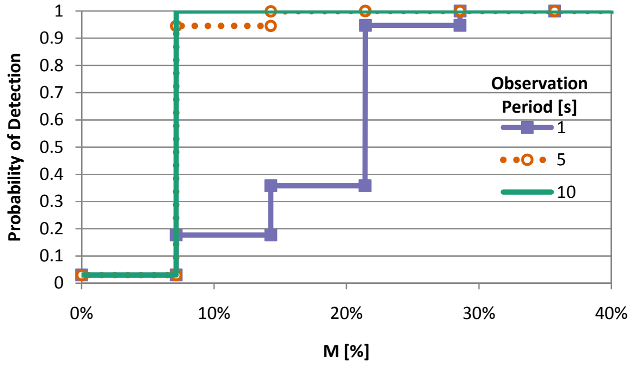

Figure 1. Probability of detection vs. misbehaviour (Voice)

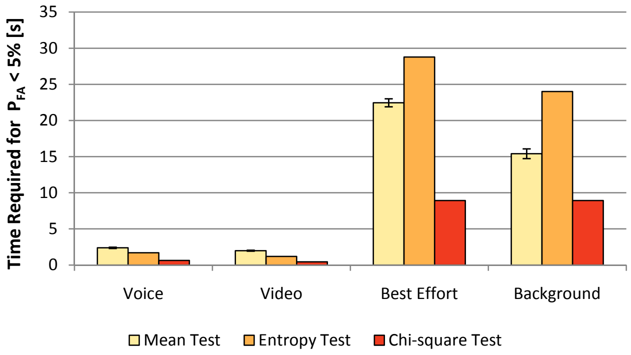

Figure 2. Time required for $P_{FP} < 5\%$

Table 1. Time required to achieve $P_D > 95\%$

AC	μ	M	Time required per test [s]		
			Mean	Entropy	Chi-square
Vo	4	50%	2.38	1.69	0.64
	5	33%	2.38	1.69	0.64
	6	16%	2.38	1.69	2.36
Vi	12	24%	1.99	1.19	1.00
	13	14%	1.99	1.19	2.94
	14	7%	22.02	1.19	5.04
BE	28	10%	22.45	28.79	8.93
	29	7%	22.45	28.79	10.30
	30	3%	>30	28.79	>30
BK	28	10%	15.41	24.00	8.93
	29	7%	>30	24.00	9.59
	30	3%	>30	24.00	>30

5. CONCLUSIONS

In this paper, we have proposed the use of the chi-square test for detecting backoff misbehaviour. The advantage of this test over other detection methods is that the chi-square test is a valid statistical hypothesis test and is computationally inexpensive.

A performance evaluation was performed to compare the chi-square test with two other methods, known in the literature. To perform a suitable comparison, these two methods were extended to support EDCA and the BEB mechanism. We assumed a misbehaviour model, which can be easily executed by an ordinary WLAN user. In almost all the simulations, the chi-square test exceeded the mean and entropy tests in terms of the probability of misbehaviour detection and detection time required to positively identify a misbehaving node. Therefore we conclude that the chi-square test is a suitable candidate for detecting backoff misbehaviour in IEEE 802.11 EDCA networks. It is a comprehensive solution which can be used in monitoring stations in ad-hoc and infrastructure scenarios. Furthermore, this method can easily be implemented in existing wireless drivers and it does not require changes to IEEE 802.11.

The performance comparison between the chi-square test and the sequential probability ratio test [10, 14] and Kolmogorov-Smirnov test [3, 9] is an open issue left for further research. However, both these approaches are more computationally expensive. Furthermore, as future work we envision studying the impact of increasing, instead of decreasing, the CW parameters. It has been shown in the literature, that this type of misbehaviour can be used to downgrade forwarded traffic in ad-hoc networks [11]. Furthermore, we plan to study the impact of other aspects of EDCA (e.g., virtual collisions) on the correct detection of chosen backoff values. Finally, we will address the problem of backoff measurements in a realistic wireless network.

ACKNOWLEDGEMENT

This work has been carried out under the Polish Ministry of Science and Higher Education project no. N N517 176037. It was also partially supported by the Polish Ministry of Science and Higher Education under the European Regional Development Fund, Grant No. POIG.01.01.02-00-045/09-00 Future Internet Engineering.

REFERENCES

1. 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 Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, pages C1–1184, 12 2007.
2. Cárdenas AA, Radosavac S, and Baras JS. Detection and prevention of MAC layer misbehavior in ad hoc networks. In *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 17–22, New York, NY, USA, 2004. ACM.
3. Toledo AL and Wang X. A robust kolmogorov-smirnov detector for misbehavior in IEEE 802.11 DCF. *Communications, 2007. ICC '07. IEEE International Conference on*, pages 1564–1569, June 2007.
4. Bianchi G, Di Stefano A, Giaconia C, Scalia L, Terrazzino G, and Tinnirello I. Experimental assessment of the backoff behavior of commercial ieee 802.11b network cards. In *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pages 1181–1189, May 2007.
5. Raya M, Aad I, Hubaux JP, and El Fawal A. DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots. *IEEE Transactions on Mobile Computing*, 5(12), 2006.
6. Madwifi Project. Madwifi – multiband atheros driver for wireless fidelity. http://madwifi-project.org/.
7. NIST/SEMATECH. e-handbook of statistical methods. http://www.itl.nist.gov/div898/handbook/.
8. Serrano P, Banchs A, and Kukielka JF. Detection of malicious parameter configurations in 802.11e EDCA. In *Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE*, volume 6, pages 5 pp.–3299, Dec. 2005.
9. Serrano P, Banchs A, Targon V, and Kukielka JF. Detecting selfish configurations in 802.11 wlans. *Communications Letters, IEEE*, 14(2):142 –144, February 2010.
10. Radosavac S, Baras JS, and Koutsopoulos I. A framework for mac protocol misbehavior detection in wireless networks. In *WiSe '05: Proceedings of the 4th ACM workshop on Wireless security*, pages 33–42, New York, NY, USA, 2005. ACM.
11. Szott S, Natkaniec M, and Banchs A. Impact of misbehaviour on QoS in wireless mesh networks. In Luigi Fratta, Henning Schulzrinne, Yutaka Takahashi, and Otto Spaniol, editors, *Networking*, volume 5550 of *Lecture Notes in Computer Science*, pages 639–650. Springer, 2009.
12. Szott S, Natkaniec M, Canonico R, and Pach AR. Impact of contention window cheating on single-hop IEEE 802.11e MANETs. In *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, pages 1356–1361, 31 2008-April 3 2008.
13. Wiethoelter S, Emmelmann M, Hoene C, and Wolisz A. TKN EDCA Model for ns-2. Technical Report TKN-06-003, Telecommunication Networks Group, Technische Universität Berlin, June 2006.
14. Rong Y, Lee SK, and Choi HA. Detecting stations cheating on backoff rules in 802.11 networks using sequential analysis. In *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, pages 1–13, April 2006.

DOI: 10.1002/ett