Real-Time Detection of Selfish Behavior in IEEE 802.11 Wireless Networks

Invited Paper

Jin Tang, Yu Cheng, Yong Hao and Chi Zhou
Department of Electrical and Computer Engineering
Illinois Institute of Technology, Chicago, IL, USA 60616
Email: {jtang9, cheng, yhao4, zhou}@iit.edu

***Abstract*—The open and distributed nature of the IEEE 802.11 based wireless network makes it easy for selfish nodes to gain unfair share on the networks by manipulating the protocol parameters. In this paper, we address the detection of such selfish behavior. The two main challenges associated with the detection problem are the unknown selfish behavior strategy and real-time detection of the behavior. While the two challenges are correlated for efficient detection, existing solutions can not address both of them well at the same time. In our work, we propose a new observation method monitoring the number of successful transmissions of the tagged node. This enables us to capture the short-term traffic dynamics which is crucial for real-time detection. Integrating our observation method with the CUSUM test, we develop a detection scheme to deal with both the challenges without any modification to the existing protocols. Moreover, we utilize a discrete Markov chain based model to characterize the behavior of the CUSUM test statistic, which enables us to quantitatively analyze the tunable parameters in the scheme for guaranteed detection performance. The performance of the proposed scheme is validated through ns-2 simulation. We show that the scheme is capable of quickly and accurately detecting the selfish behavior without knowledge of the selfish strategy.**

I. Introduction

The deployment of the IEEE 802.11 based wireless network is dramatically increasing over recent years due to its high-speed access, easy-to-use feature, and economical advantages. As a contention based protocol, 802.11 assumes that every participant in the network acts in compliance with the protocol rules [1], [2]. However, the open and distributed nature of the protocol makes it possible for selfish nodes to deliberately modify the protocol parameters to gain unfair share to the network at the expenses of other normal nodes' channel access. Moreover, to make things worse, the wireless network devices nowadays have developed to be easily programmable [4], [5] for flexible functionalities and reconfigurable capabilities, where selfish behaviors have become much more feasible and do not rely on much expert knowledge. As a result, the network services can easily be disrupted by certain malicious nodes. Thus in this paper, we address the important security issue on how to quickly and accurately detect the selfish behavior in the 802.11 wireless networks.

The random operation of the IEEE 802.11 protocol poses significant difficulties in distinguishing between a malicious behavior and an occasional protocol malfunction. Generally, there are two main challenges on detection of the selfish behavior, namely the *unknown selfish behavior strategy* and *real-time detection* of the behavior. While the two challenges are correlated for efficient detection, existing solutions [4], [6] can not address both of them at the same time, or even require modification to the 802.11 protocols [7]. Considering the challenges, we develop our detection scheme based on the *non-parametric cumulative sum (CUSUM)* test [8] due to its robust ability to quickly find abrupt changes in a process without any prior knowledge of the statistical model for the occurrence of the changes. The CUSUM test statistic is able to accumulate the deviation brought by the selfish behavior of a malicious node from the normal behavior, and raise an alarm to identify the malicious node as long as a threshold is exceeded. Also, the scheme does not require any modification to the protocols.

In order to capture the short-term traffic dynamics which is crucial for real-time detection, we propose a new observation measurement as the input for the CUSUM based scheme. We monitor the number of successful transmissions of the tagged node every T successful transmissions (observation interval) of the whole network. As a selfish node is likely to always obtain more opportunities to transmit in every such observation interval, the cumulative effect of its selfish behavior can quickly be captured by the CUSUM test and an alarm is then raised. The behavior of the CUSUM test statistic under a certain traffic process is crucial for the performance of the detection scheme in terms of the false positive rate and the detection delay. In this paper, we show that the CUSUM test statistic can be modeled by a discrete Markov chain, as the change of the test statistic happens at the end of every observation interval and only the current status determines the next detection decision. The Markovian model enables us to quantitatively analyze the tunable parameters in the scheme for guaranteed performance. We validate the performance of the proposed detection scheme by applying it in an 802.11 wireless network through ns-2 [9] simulation. The results demonstrate the capability of the proposed scheme to quickly and accurately detect the selfish behavior.

In summary, this paper has contributions in three aspects: 1) The proposed CUSUM based scheme is able to simultaneously address the two main challenges on detecting the selfish behavior in 802.11 networks and identify the malicious node. 2) The new observation method can capture the short-term

978-1-4244-3574-6/10/$25.00 ©2010 IEEE

traffic dynamics and work ideally with the CUSUM test. 3) The Markov chain based model accurately characterizes the behavior of the test statistic and provides an analytical tool for performance analysis and system configuration.

The remainder of the paper is organized as follows. Section II reviews more related work. Section III describes the system model. The detection scheme design is presented in Section IV. Section V presents the ns-2 simulation results to validate the performance of the scheme. And Section VI concludes the paper.

II. Related Work

In [7], the authors presented a modification to the 802.11 protocol to facilitate the selfish behavior detection. In their scheme, the receiver assigns a backoff timer for the sender. If the number of idle slots between consecutive transmissions from the sender does not comply with the assigned backoff timer, the receiver will consider that the sender potentially deviates from the protocol and penalize the sender with a smaller backoff timer. Continuous deviations will result in that the receiver labels the sender as a selfish node. However, the above scheme assumes a trustworthy receiver who performs the detection, which may not be the case in a dynamic network environment. Modification to the 802.11 protocol and reliance on the receiver are the main limitations of the work.

The sequential probability ratio test (SPRT) method is used in [6], [10], [11] to detect the 802.11 selfish behavior. The detection decision is made when a random walk of the likelihood ratio of observations (given two hypotheses) rises greater than an upper threshold. The main advantage of SPRT is that it can reach decision very fast, given the complete knowledge of both normal behavior and selfish behavior strategy [13]. However, in a realistic setting, the strategy of selfish nodes is hard to be known in advance; such an issue imposes the major inherent limitation of the SPRT method. Further, the existing work normally assumes that the backoff timer of each node is observable, which is again hard to achieve in practice because the transmission attempts involved in a collision are impossible to be distinguished. Thus in our scheme we monitor the successful transmission of the tagged node as the observation measurement.

The authors in [3], [4] utilize the Kolmogorov-Smirnov (K-S) significance test to address the detection problem assuming an a priori known selfish strategy model. This test is able to make the decision by comparing the distribution of sampled traffic data with the normal-behavior distribution estimated online. Nonetheless, as a batch test method, the K-S statistic has its own drawback. Fixed-size data samples are needed to perform the test each time, which actually makes real-time detection impossible. Even in the modified sequential truncated K-S test, a number N [4] still needs to be predetermined before test starts in order to get a proper significant level for each test step. In this paper, we propose to adopt the CUSUM change point test [8] for the selfish behavior detection, which has the advantages of both real-time detection and no requirement of a priori knowledge of the selfish strategy.

III. System Model

A. IEEE 802.11 CSMA/CA Operation

The nodes in an IEEE 802.11 network operate in a distributed manner and contend for access to the wireless medium following the CSMA/CA function [1]. When a node attempts to transmit a packet, it needs to sense the medium idle for a specified time. If the medium is not idle, the node will enter a backoff stage and defer the transmission according to a timer before attempting the next transmission. This backoff timer is a random value uniformly selected from a set $\{0, 1, ..., CW_{min} - 1\}$, where CW_{min} is called the minimum contention window. The timer will decrease if the medium is continuously sensed idle and freeze whenever the medium is sensed busy. After the timer reaches 0 the node will attempt another transmission. Each unsuccessful transmission due to reasons such as collisions or lost of ACK messages from the reception node will result in the contention window doubling its size until it reaches the maximum contention window CW_{max}. After a successful transmission, the node will reset the contention window to its minimum value CW_{min} and continue sensing the medium if more packets need to be transmitted.

B. Selfish Behavior in IEEE 802.11

As a distributed contention based protocol, the IEEE 802.11 assumes that every node in the network operates in accordance with the protocol rules as described above to obtain a fair share of the wireless medium. However, a node who has the smallest backoff timer will obviously be favored by the protocol as it can always obtain more chances to transmit while other nodes are still in the backoff stage. Since there is no central controlling unit who assigns the backoff timer for each node, a selfish node can continuously choose small backoff timers and then gain significant advantage in channel access probability over others. Moreover, because the increased transmission probability of the selfish node causes more collisions, normal nodes are forced to further exponentially defer their transmissions as they operate according to the protocol, which results in the selfish node gaining more advantage. The selfish behavior can drastically decrease the transmission probability of normal nodes and subsequently severely downgrade their throughput. In some extreme case where the selfish node set its own backoff timer to a very small constant value, it will lead to denial of service (DoS) of the whole network except for the selfish node itself. Thus, a detection scheme capable of quickly and accurately identifying the selfish node is highly desired for the normal operation of an IEEE 802.11 wireless network.

IV. Detection Scheme Design

In this section we describe the CUSUM based selfish behavior detection scheme design, enhanced with an observation method to capture the short-term traffic dynamics. A Markov

chain based model is also developed to analyze the CUSUM test statistic.

A. Traffic Observation and Measurement

Selfish nodes manipulate the backoff timer to gain greater transmission probability, thus the length of the backoff timer, which in particular is the number of idle slots between two transmission attempts of the tagged node, would be ideal for a desired measurement. Unfortunately, this approach is practically impossible since the node identities associated with those transmissions involved in a collision are not observable. Nevertheless, the nodes having successful transmissions are always observable, we thus utilize the number of successful transmissions of the tagged node as the measurement. Next we convert the measurement into a sequence that can be used in the detection algorithm. A common approach to construct the sequence based on fixed time intervals may not be appropriate in this case. This is because the number of transmissions of a node in a fixed time interval is random due to the property of 802.11. Instead, we use the number of successful transmissions of all nodes in the network, T, as the observation interval, which can help capture the short-term traffic dynamics. Also, using T as the observation interval, the interframe durations in the 802.11 protocol such as DIFS and SIFS will not be directly considered in our measurements. And the detection agent, e.g. AP, can easily obtain the measurement sequence based on T.

B. Detection Algorithm Design

Let $\{T_n, n = 0, 1, ...\}$ be the sequence of the number of successful transmissions of the tagged node within each observation interval. A crucial issue for real-time anomaly detection is to capture the short-term dynamics of the observed sequence. Even the normal behavior may vary in a short time range which makes its profiling very hard. However, choosing the number of successful transmissions in the whole network as the observation interval alleviates this dependency on time. The dynamics of the measurement sequence $\{T_n\}$ are a sole reflection of the behavior of the tagged node in the network. Clearly, a selfish node is highly likely to obtain more transmission opportunities in every T successful transmissions over the whole network, which can be utilized as the basic fact for our selfish behavior detection.

Since the behavior of a selfish node is completely unpredictable to a detection agent, it is impossible to have any knowledge of its strategy a priori. Also, we aim to detect the selfish behavior as quickly as possible after it happens and make real-time decisions. Because of these two factors, we design our detection scheme based on the non-parametric CUSUM test [8] due to its robust ability to quickly find abrupt changes in a process without any prior knowledge of the statistical model for the occurrence of the changes.

Let u be the upper bound of the expectation of T_n. We then have the CUSUM test statistic

$$\begin{aligned} X_n &= (X_{n-1} + (T_n - u))^+ \\ X_1 &= 0 \end{aligned} \tag{1}$$

where $(x)^+ = x$ if $x \geq 0$ and 0 otherwise.

Clearly, when the tagged node associated with the sequence $\{T_n\}$ starts to act selfishly, the number of its successful transmissions increases and consequently $(T_n - u)$ will continuously be positive. In the contrast, when the node operates according to the 802.11 protocol, $(T_n - u)$ will mostly be negative. This property makes the CUSUM statistic suitable to detect the selfish behavior. Note that if the tagged node acts normal, X_n will stay around 0 no matter how long the normal behavior has been observed. However, when the node turns to selfish, X_n will quickly accumulate to a large positive.

As we want to utilize the above CUSUM test statistic to make detection decision, a threshold h is needed to be the actual indicator of the detection. When X_n accumulates to a large enough number and exceeds h, the selfish behavior will be detected. Thus the decision rule in each step of the test is

$$\delta_n = \begin{cases} 1 & if \quad X_n \geq h \\ 0 & if \quad X_n < h \end{cases} \tag{2}$$

where δ_n is also an indicator function of whether the detection event happens or not. We reset X_n back to 0 as soon as it exceeds the threshold and start the detection over again.

C. Discrete Markov Chain Based Model

Consider the sequence $\{X_n\}$ as a discrete random process, which takes values from a finite set $A = \{0, 1, 2, ..., h\}$. The process is said to be in state j at time n if $X_n = j$ and in state i at time $n-1$ if $X_{n-1} = i$, where $i, j \in A$. The transition between the states happens at the end of every observation interval T. According to (1), the current state X_n depends only on the state X_{n-1} and is independent of any other previous states, where the transition probability is

$$P_{ij} = P\{X_n = j | X_{n-1} = i\}. \tag{3}$$

Thus the random process $\{X_n\}$ satisfies the Markov property and can be modeled as a discrete Markov chain.

Given the decision threshold h, the Markov chain is then described by a $(h+1) \times (h+1)$ transition probability matrix as

$$\mathbf{P} = \begin{pmatrix} P_{00} & P_{01} & P_{02} & \dots & P_{0h} \\ P_{10} & P_{11} & P_{12} & \dots & P_{1h} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ P_{h0} & P_{h1} & P_{h2} & \dots & P_{hh} \end{pmatrix}.$$

This transition probability matrix is divided into four distinct groups based on the observed traffic condition T_n and the property of X_n.

Group 1 of the matrix covers where $i \in \{0, 1, ..., h-1\}$ and $j = 0$. And elements in this group satisfy

$$\mathbf{P}(i, 0) = P\{T_n \leq (u - i)\} \quad \text{if } u - i \geq 0 \tag{4}$$

$$\mathbf{P}(i, 0) = 0 \quad \text{otherwise.} \tag{5}$$

This group is related to the transitions to state 0. According to (1), the state X_n is always reset to 0 from i when $i + T_n - u \leq 0$. Thus the transition probability is $P\{T_n \leq (u-i)\}$ as shown

in (4). However, as it is impossible to reach state 0 when $u - i < 0$, we obtain (5).

Group 2 covers where $i \in \{0, 1, ..., h-1\}$ and $j \in \{1, 2, ..., h-1\}$. Elements in the group follow

$$\mathbf{P}(i,j) = P\{T_n = (j - i + u)\} \quad \text{if } j - i + u \geq 0 \tag{6}$$

$$\mathbf{P}(i,j) = 0 \quad \text{otherwise.} \tag{7}$$

This group is about the transitions to all the states other than 0 and h. Again according to (1), the state X_n reaches j from i when $j = i + T_n - u$. Then the transition probability is $P\{T_n = (j - i + u)\}$ as shown in (6). Also, this kind of transition is impossible when $j - i + u < 0$. As a result, we have (7).

Group 3 is the part of the transition probability matrix where $i \in \{0, 1, ..., h-1\}$ and $j = h$. And elements in this group satisfy

$$\mathbf{P}(i,h) = 1 - \sum_{j=0}^{h-1} P_{ij}. \tag{8}$$

This group is about the transitions to state h. Note that state h is related to any values of X_n when $X_n \geq h$. Thus the transition probability from i to h is $1 - \sum_{j=0}^{h-1} P_{ij}$ as shown in (8).

Finally, group 4 covers where $i = h$ and $j \in \{0, ..., h\}$. Elements in the group satisfy

$$\mathbf{P}(h,j) = 1 \quad \text{if } j = 0 \tag{9}$$

$$\mathbf{P}(h,j) = 0 \quad \text{otherwise.} \tag{10}$$

This group is related to the transition from h to any other states. As we reset X_n back to 0 as soon as it exceeds h, the only transition from h is to 0. Thus this transition probability is 1 whereas all the others are 0.

Based on the Markov chain model, we can calculate the mean time between the two time points when the test statistic X_n exceeds the threshold h as a function of u, h and the distribution of T_n. In particular, it is actually computing the expected number of steps to transition from one state h to the next state h in the Markov chain. And this problem can be solved using a set of linear equations associated with the transition probability matrix $\mathbf{P}$ [14]. Note that under normal traffic condition, the result is actually the mean time between false positives, which is the inverse of the false positive rate and is a very important factor to characterize the performance of the detection scheme. In next section we will use actual 802.11 traffic to obtain the distribution of T_n and subsequently find appropriate values for both u and h to achieve certain level of false positive rate.

V. Performance Evaluation

In this section we evaluate the performance of the proposed detection scheme through ns-2. In our simulation, we establish an 802.11 wireless network consisting of 10 competing nodes and an access point (AP). The 10 nodes send constant traffic towards the AP and the AP also acts as the detection agent. The minimum contention window CW_{min} of normal nodes is set to 32 according to the protocol. Also, among the 10 nodes there is 1 tagged node which can modify its contention window size to act either as a normal node or a selfish node. Through the simulation, we show that the proposed scheme preserves the capability to quickly and accurately detect the selfish behavior.

A. Parameter Specification Using the Markov Chain Model

As described in the previous section, using the the Markov chain based model, the mean time between false positives is a function of u, h and the distribution of T_n under normal traffic condition. Ideally, the distribution of T_n under normal traffic condition should follow a binomial distribution, as each successful transmission might be from the tagged node with probability $1/N$ assuming a total of N nodes. However, as we use $T = 30$ to ensure the detection sensitivity of the proposed scheme, the short-term fairness issue [12] of the 802.11 protocol makes the binomial distribution not accurate due to the correlation among successful transmissions. We did find this inaccuracy from our analysis and experimental results, but how to analytically obtain the accurate distribution of T_n still remains an issue. Therefore, we use the traffic trace obtained from the normal operation of the simulated 802.11 network as a training data set to derive the distribution of T_n.

Using the derived distribution of T_n, we can specify values for h and u to complete the Markov chain based model according to $(4) - (10)$. Then using the model, the mean time between false positives can be calculated as described in the previous section. Based on this, we are able to calculate that with $h = 8$ and $u = 5$, the mean time between false positives is 3237.7. And the related false positive rate is very small which is only a little more than 0.03%. We will use these parameter values in next subsection to see the detection delay of the proposed scheme.

B. Evaluation for the Detection Scheme

We now evaluate the proposed detection scheme against the selfish behavior of the tagged node. We fix $h = 8$ and $u = 5$ as thus the false positives rate is low according to our previous analysis.

The tagged node still follows the binary exponential operation of the 802.11 protocol, but manipulates its minimal contention window size CW_{min} to gain advantage in channel access probability over other normal nodes. The extreme case of $CW_{min} = 1$ may result in denial of service of the whole network except for the tagged node whereas the case of $CW_{min} = 32$ implies that the tagged node is acting as a normal node.

Figure 1 demonstrates the sensitivity of the detection statistic X_n, i.e., the detection delay, to the moderate selfish behavior of the tagged node whose minimum contention window is set to 16. The selfish behavior happens in the 20th sample and is detected after 9 samples when X_n accumulates and exceeds the threshold h. After the selfish behavior ends, X_n is immediately reset to 0.

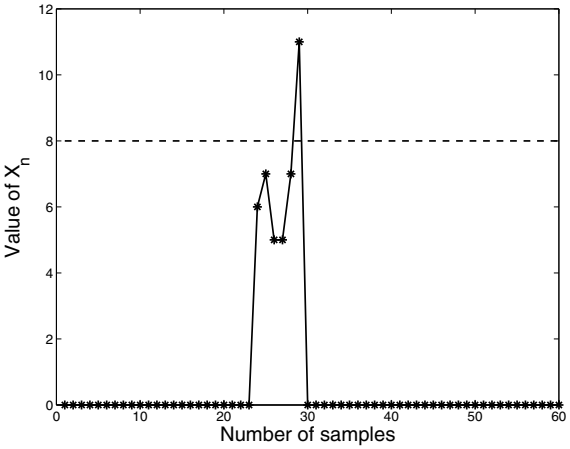

Fig. 1. Detection sensitivity.

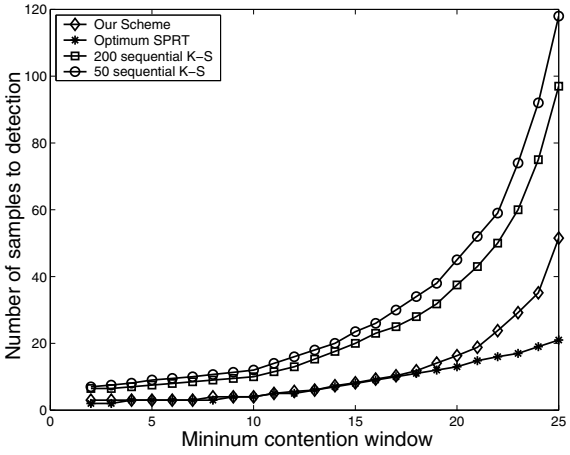

Fig. 2. Comparison of detection delay of different schemes.

We compare the proposed scheme to existing solutions for 802.11 selfish behavior detection in terms of the detection delay. The intensity of the selfish behavior is categorized by the size of the minimum contention window CW_{min}. We are interested in the detection of the selfish behaviors with CW_{min} less than or equal to 25, since larger window will actually have minimal effect on the wireless network. As shown in Figure 2, we first see that the proposed scheme itself is able to quickly detect the selfish behaviors of various intensities. And the specified parameter values do help us achieve a balance between the false positive rate and the detection delay. Comparing with other detection schemes, our scheme is just a little slower than the optimum SPRT detector which assumes perfect knowledge of the selfish behavior strategy. However, as schemes that do not require the selfish behavior strategy a priori, our scheme clearly outperforms the sequential K-S test as proposed in [4].

VI. Conclusion

In this paper we address the selfish behavior detection in IEEE 802.11 wireless networks. While realizing that the two main challenges associated with efficient detection is the unknown selfish behavior strategy and real-time detection of the behavior, we develop our detection scheme based on the CUSUM change point test since the test preserves the ability to quickly find abrupt changes in a process without any prior knowledge of the statistical model for the occurrence of the changes. Also, we propose a new observation method monitoring the number of successful transmissions of the tagged node. The method captures the short-term traffic dynamics and works ideally as the input for our real-time detection scheme. Moreover, by knowing that the CUSUM test statistic in our case satisfies the Markov property, we characterize the behavior of the test statistic using a discrete Markov chain. This enables us to quantitatively analyze the tunable parameters in the scheme for guaranteed performance. Finally, we validate the performance of the scheme through ns-2 simulation. The results demonstrate that the scheme can quickly and accurately detect the selfish behavior without any knowledge of the selfish strategy. In our future work, we will find how to analytically obtain an accurate distribution of T_n, which can help us better characterize the performance of the scheme. Also, we will expand the current work to a multi-hop setting, where distributed selfish behavior can happen and it is very hard for one node to observe the behavior of every other node in the network. We will try to employ cooperative decentralized detection among several observing nodes and detection agents to address the problem.

References

[1] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," in *IEEE Journal on Selected Areas of Communication*, vol. 18, no. 3, pp. 535-547, Mar. 2000.

[2] H. Zhai, X. Chen and Y. Fang, "How Well Can the IEEE 802.11 Wireless LAN Support Quality of Service?" in *IEEE Trans. Wireless Communications*, vol. 4, no. 6, pp. 3084-3094, Nov. 2005.

[3] A. Toledo and X. Wang, "A Robust Kolmogorov-Smirnov Detector for Misbehavior IEEE 802.11 DCF," in *Proc. IEEE ICC*, 2007, pp. 1564–1569.

[4] A. Toledo and X. Wang, "Robust Detection of Selfish Misbehavior in Wireless Neetworks," in *IEEE Journal on Selected Areas in Communication*, vol. 25, no. 6, pp. 1124-1134, Aug. 2007.

[5] The MAdWiFi Driver, [Online:]http://www.madwifi.org/.

[6] S. Radosavac, J. S. Baras and I. Koutsopoulos, "A Framework for MAC Protocol Misbehavior Detection in Wireless Networks," in *Proc. ACM Workshop on Wireless Security*, 2005, pp. 33–42.

[7] P. Kyasanur and N. Vaidya, "Selfish MAC Layer Misbehavior in Wireless Networks," in *IEEE Trans. Mobile Computing*, vol. 4, no. 5, pp. 502-516, 2005.

[8] H. V. Poor and O. Hadjiliadis, *Quickest Detection*, first edition, Cambridge, 2008.

[9] network simulator 2, [Online:] http://www.isi.edu/nsnam/ns.

[10] S. Radosavac, G. Moustakides, J. Baras and I. Koutsopoulos, "An Analytic Framework for Modeling and Detecting Access Layer Misbehavior in Wireless Networks," in *ACM Trans. Information and Systems Security*, vol. 11, no. 4, article no. 19, Jul. 2008.

[11] Y. Rong, S. Lee and H. Choi, "Detecting Stations Cheating on Backoff Rules in 802.11 Networks using Sequential Analysis," in *Proc. IEEE INFOCOM*, 2006, pp. 1–13.

[12] C. E. Koksal, Hi. Kassab and H. Balakrishnan, "An Analysis of Short-Term Fairness in Wireless Media Access Protocols," in *Proc. ACM SIGMETRICS*, 2000.

[13] A. Wald, *Sequential Analysis*, John Wiley and Sons, New York, 1947.

[14] J. R. Morris, *Markov Chains*, Cambridge, 1997.