Performance evaluation and trade-offs of optimal back-off misbehavior detection schemes in wireless networks in the presence of interference [*]

Svetlana Radosavac
DoCoMo Communications Laboratories USA[†]
3240 Hillview Ave
Palo Alto, CA
sradosavac@docomolabs-usa.com

John S. Baras
Electrical and Computer Engineering Dep.
and the Institute for Systems Research
The University of Maryland, College Park, MD
baras@umd.edu

ABSTRACT

In this work we evaluate the impact of interference caused by concurrent transmissions of neighboring stations on the performance of quickest detection schemes for detection of back-off misbehavior in the IEEE 802.11 MAC. We evaluate the trade-offs that both the adversary and the detector face under such conditions using a game theoretic framework. Furthermore, we evaluate the worst-case scenarios under which the given detector can efficiently operate under the predetermined conditions and show by both mathematical analysis and simulation how the presence of uncertainty affects the performance of the detector. Finally, we conclude that in the presence of (i) adaptive intelligent adversaries and (ii) variable environment conditions, the adoption of a static detection system is not advisable and propose employment of an adaptive detection system in order to maintain satisfying performance under a wide range of conditions.

1. INTRODUCTION

In recent years, information has become a resource of strategic importance and wireless networks have become the primary means for ensuring availability, offering access to and enabling transfer of data. At the same time, the strategic significance of timely dissemination of information in the network offers strong incentives for malicious entities to launch attacks against critical operations and network functionality. Due to the mentioned issues, the problem of deviation from legitimate protocol operation in wireless networks and efficient detection of such behavior has been studied in great detail and many different solutions to the problem have been offered.

The underlying design principle of every system is to achieve robustness not only against a specific disruption, but also to maintain an acceptable performance level when such disruption occurs. This is not possible to achieve without careful design planning. In order to construct a detection system that ensures robustness of a given system, goal and capabilities of both the detector and the adversary need to be defined. As it is not possible to predict the attacker's behavior, an essential design component is prediction of the worst-case scenario for the system and estimation of error margin and performance bounds. Only then it is possible to realistically evaluate the performance of the system by deriving an optimal detection strategy for various scenarios and determining whether the critical system parameters remain within acceptable boundaries for each scenario.

The problem of back-off misbehavior detection has received considerable attention from the research community in recent years. The authors in [10] focus on MAC layer misbehavior in wireless hot-spot communities. They propose a sequence of conditions on available observations for testing the extent to which MAC protocol parameters have been manipulated. The advantage of the scheme is its simplicity and easiness of implementation, although in some cases the method can be deceived by cheating peers, as the authors point out. A different line of thought is followed by the authors in [7], where a modification to the IEEE 802.11 MAC protocol is proposed to facilitate the detection of selfish and misbehaving nodes. The approach presupposes a trustworthy receiver, since the latter assigns to the sender the back-off value to be used. The receiver can readily detect potential misbehavior of the sender and accordingly penalize it by providing less favorable access conditions through higher back-off values for subsequent transmissions. A decision about protocol deviation is reached if the observed number of idle slots of the sender is smaller than a pre-specified fraction of the allocated back-off. The sender is labeled as misbehaving if it turns out to deviate continuously based on a cumulative metric over a sliding window. In [8, 9] the authors address detection of an *adaptive intelligent* attacker by casting the problem of misbehavior detection within the min-max robust detection framework. The key idea is to optimize the performance of the detection algorithm for the

[*] Research supported by the U.S. Army Research Office under CIP URI grant No. DAAD19-01-1-0494 and by the Communications and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011

[†] Research performed while the author was with the Institute for Systems Research and the Electrical and Computer Engineering Department, University of Maryland College Park

ValueTools 2008, October 21-23, 2008, Athens, GREECE.
Copyright ©2008 ICST ISBN # 978-963-9799-31-8 .

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4367
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4367

worst-case instance of uncertainty. This process is characterized by identifying the least favorable operating point of the detection algorithm, and by deriving the strategy that optimizes the performance of the detection algorithm when operating in that point. The detection performance is measured in terms of number of required observation samples to derive a decision (detection delay) subject to a constant rate of false alarms.

The problem setup in [7, 8, 9, 10] assumes operation of the observer nodes under perfect conditions. Consequently, the proposed detection mechanism assumes that each RTS/CTS signal is observed and registered and the detector performance specifications are obtained under that assumption. However, in wireless networks instances of inaccurate information are encountered frequently: measurement errors, network discrepancies and intense interference cause protocols to operate with imperfect and distorted information. If we consider the scenario where two customers, A and B, want to purchase a detector it is essential to provide them with complete and accurate information about detector performance under a wide range of conditions (i.e. customer A might be operating under suboptimal conditions and is not interested how the detector performs under perfect conditions as he will never be operating in such settings). When a customer is presented with a realistic overview of detector performance, he can then decide whether to purchase offered detection system, invest in his own system (that will result in lower number of lossy observations) or invest in a more sensitive detection system.

In this work, we revisit the problem of back-off misbehavior detection [7, 8, 10] and extend the analysis presented in [8, 9] by evaluating the performance of both the intelligent adversary and the quickest detection system in the presence of interference (which results in lossy observations at the detector side). We attempt to obtain the least favorable distribution of an adaptive intelligent adversary in the IEEE 802.11 MAC in the presence of interference. Following that, we perform a detailed analysis of the proposed misbehavior detection system performance in the presence of interference in terms of probability of detection and number of false alarms. Furthermore, motivated by findings from [1], we adopt a more realistic approach towards constructing an optimal detector. More specifically, [1] and [3] claim that in real anomaly detection systems, the Probability of False Alarm (P_{fa}) needs to be lower than the one used in theoretical analysis presented in current literature. In this work, we follow the proposed approach and adopt significantly lower P_{fa} rates than in any other existing back-off misbehavior detection system [7, 10, 8].

We are not aware of any existing literature that addresses impact of interference on the performance of adversaries and the quickest back-off misbehavior detection system in wireless networks (the importance of taking interference into account while evaluating the performance of detection schemes was briefly mentioned in [8] and [9]). Although the extreme instance of the optimal attack derived in this work is equivalent to Denial of Service attack and has effects similar to jamming attacks, it is important to mention that this work does not address the performance of detection schemes in the presence of jamming attacks. Our work contributes to the current literature in the area of MAC layer misbehavior detection by: (i) providing a detailed mathematical analysis of performance of the quickest detection schemes [9] in the presence of interference, which results in lossy observations of back-off sequences; (ii) providing detailed numerical analysis of performance of optimal adaptive adversaries in such settings and (iii) considering significantly lower False Alarm rates, which enables customers to obtain realistic performance overview of given detection system (previous detection systems considered P_{fa}=0.01, which results in roughly 700 false alarms per minute, which is unacceptable for any customer).

The remainder of the paper is organized as follows. In Sect. 2 we present a general outline of the problem and state the assumptions that will be used throughout the paper. Sect. 3 provides a description of an adversary model followed by the attack detection model in Sect. 4. In Sect. 5 we present a detailed overview of the min-max robust approach in the presence of interference followed by a Markov Chain representation of the system in Sect. 6. We conclude our work with a detailed evaluation of the proposed quickest detection system in the presence of interference in terms of False Alarm rate and detection delay and provide some directions for future work in Sect. 8. In subsequent sections, the terms “misbehavior” and “attack”, “misbehaving node” and “attacker”, “optimal detector” and “quickest detection system” will be used interchangeably with the same meaning.

2. PROBLEM DESCRIPTION AND ASSUMPTIONS

Throughout this work we assume the existence of an intelligent adaptive adversary that is aware of the environment and its changes over a given period of time. Consequently, the adversary is able to adjust its access strategy depending on the level of congestion in its environment. For now we assume that, in order to minimize the probability of detection, the attacker chooses legitimate over selfish behavior when the level of congestion in the network is low. Similarly, the attacker chooses an adaptive selfish strategy in congested environments. This issue will be discussed in more detail in Sect. 5. Due to the previously mentioned reasons, we assume a benchmark scenario where all the participants are backlogged, i.e., have packets to send at any given time in both theoretical and experimental evaluations. We assume that the attacker employs the worst-case misbehavior strategy in this setting, which enables the detection system to estimate the maximal detection delay. It is important to mention that this setting represents the *worst-case* scenario with regard to the number of false alarms per unit of time due to the fact that the detection system is forced to make maximum number of decisions per time unit.

In order to characterize the strategy of an intelligent attacker, we assume that both misbehaving and legitimate node attempt to access the channel simultaneously. We assume that when no interference is present, each station generates a sequence of random back-offs $X_1, X_2, \ldots, X_i$,which are correctly observed at the detector side, over a fixed period of time. According to the IEEE 802.11 specifications [6], the back-off values of each legitimate protocol participant are distributed according to the uniform probability distribution function (pdf) $f_0(x_1, x_2, \ldots, x_i)$. The pdf of the misbehaving participants is unknown to the system and is denoted with $f_1(x_1, x_2, \ldots, x_i)$, where $X_1, X_2, \ldots, X_i$ represent the sequence of back-off values generated by the mis-

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4367
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4367

behaving node over the same period of time.

Throughout this work we assume that a detection agent (e.g., the access point) monitors and collects the back-off values of a given station. It is important to note that observations are not perfect and can be hindered by concurrent transmissions or external sources of noise. It is impossible for a passive monitoring agent to know the back-off stage of a given monitored station due to collisions and to the fact that in practice, nodes might not be constantly backlogged. This issue will be addressed in more detail in the remainder of the paper. Furthermore, in practical applications the number of false alarms in anomaly detection schemes is very high. Consequently, instead of building a "normal" profile of network operation with anomaly detection schemes, we utilize specification based detection. In our setup we identify "normal" (i.e., a behavior consistent with the 802.11 specification) profile of a backlogged station in the IEEE 802.11 without any competing nodes, and notice that its back-off process $X_1, X_2, \ldots, X_i$ can be characterized with pdf $f_0(x_i) = 1/(W+1)$, where W represents the size of the back-off window, for $x_i \in \{0, 1, \ldots, W\}$ and zero otherwise. We claim that this assumption minimizes the probability of false alarms due to imperfect observations. At the same time, a safe upper bound on the amount of damaging effects a misbehaving station can cause to the network is maintained. However, in the presence of interference, the setting presented in [4] is no longer valid. Namely, the perceived back-off values of both legitimate and malicious participants change in the presence of interference and the resulting pdf at the observers' side differs from the actual one.

Before proceeding towards a formal analysis of the interference problem at the observers' side, we first address the issue at the attackers' side. In this work we assume that the goal of the adversary is to deny medium access to legitimate protocol participants. The adversary achieves this by adopting strategies that provide him with higher access probability and consequently increase his own gain. Due to the fact that this strategy corresponds to zero-sum games (i.e. strategy where one participant's loss results in the other participant's gain), this results in decreased gain for legitimate protocol participants. We assume the attacker in the presence of interference attempts to access the medium with the same strategy that was presented in [9], i.e. attempts to maximize his gain while minimizing the probability of detection. However, due to interference, it may miss one or more control messages. We now note that, although the adversary does not gain access to the medium, his main goal is achieved: (i) the adversary transmits Request-to-Send (RTS) message and silences his neighborhood for the duration of the potential data transmission and (ii) the receiver sends Clear-to-Send (CTS) message which silences his own neighborhood, just as if the whole exchange of data were successful and (iii) the back-off window of legitimate nodes exponentially increases (due to the failed transmission attempt), following the specification of the IEEE 802.11 [6], resulting in more significant advantage of misbehaving node who does not follow the protocol and constantly chooses back-off values from the interval $[0, W]$. Hence, the adversary, whose goal is to deny access to legitimate participants, still achieves his goal in the presence of interference and need not change his own strategy.

Before proceeding towards a more detailed interference model in Sect. 5.1 and performance evaluation of optimal detector in such setting, we first present and adversary model and the corresponding quickest detection test for such adversary in Sect. 3 and Sect. 4 respectively.

3. ADVERSARY MODEL

The lack of a proper adversarial model can lead to misconfiguration of the employed detector and significant decrease in system performance due to missed detection, detection delay or large number of false alarms. In order to properly evaluate the defense strategies, obtain performance bounds of the detector and potential damage caused by an adversary, a more stringent definition of adversary capabilities and goals as well as specifications of the corresponding detection system are provided.

3.1 Desired Properties of a Detection System

In this work we assume that an optimal detection system is designed so that it can detect misbehaving nodes as soon as possible with an acceptable false alarm rate and acceptable delay.

3.2 Feasible Design Space

The feasible design space, $\mathcal{S}$, is defined to be any sequential test that satisfies a given false alarm and detection rates. A sequential test is an algorithm which with every new obtained sample x_i, either decides to classify the observed behavior based on $x_1, \ldots, x_i$ or waits for the next sample.

3.3 Capabilities of the Adversary

We assume the adversary has full control over his actions. More specifically, in this setting, we assume the adversary has complete control over its back-off distribution. In order to describe the capabilities of the adversary we define a feasible class of attacks $\mathcal{F}$ that describes his probable set of actions.

3.4 Information Available to the Adversary

Throughout our work we adopt the strict assumption that an adversary is intelligent, i.e. knows everything the detection agent knows and can infer the same conclusions as the detection agent. This assumption enables the detector to obtain the upper bound on the detection delay (lower performance bound of the detection system).

3.5 Goal of the Adversary

We assume the objective of the adversary is to design an access policy which maximizes his gain over the defined period of time, while minimizing the probability of detection, P_d. If the adversary is malicious, his goal is to minimize the gain of the other participants. On the other hand, a greedy adversary attempts to maximize his own gain, which may or may not result in minimizing the gain of the other participants.

If we denote the expected back-off values of legitimate and misbehaving nodes by $\mathbb{E}_0[Y]$ and $\mathbb{E}_1[X]$ respectively and the attacker's probability of accessing the channel with P_1, the following theorem holds:

THEOREM 1. *The probability that the adversary accesses the channel before any other terminal when competing with n neighboring (honest) terminals for channel access in sat-*

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4367
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4367

uration condition is:

$$P_1 = \frac{1}{1 + n\frac{\mathbb{E}_1[X]}{\mathbb{E}_0[Y]}} = \eta\frac{1}{n+1} > \frac{1}{n+1}. \qquad (1)$$

where $\eta \in (1, n+1)$ and n represents the number of legitimate protocol participants and η represents a parameter that gives us an insight into the level of aggressiveness of the adversary. In other words, his probability of accessing the channel is greater than the corresponding probability of any legitimate node by a factor $\eta > 1$. We omit the proof of this theorem and refer the reader to [9] for the proof.

Using the simple modeling introduced in [9] we are now able to quantify the notion of an "attack". Let η be a quantity that satisfies $1 < \eta < n+1$ and consider the class $\mathcal{F}_\eta$ of all pdf's that induce a probability P_1 of accessing the channel that is no less than $\eta/(n+1)$. Using the reasoning presented in [8, 9], the class $\mathcal{F}_\eta$ can be explicitly defined as

$$\mathcal{F}_\eta = \left\{ f_1(x) : \int_0^W x f_1(x)\,dx \le \frac{1 - \frac{\eta}{n+1}}{n\frac{\eta}{n+1}} \frac{W}{2} \right\}. \qquad (2)$$

This class includes all possible attacks for which the incurred relative gain exceeds the legitimate one by $(\eta - 1) \times 100\%$. The class $\mathcal{F}_\eta$ is the uncertainty class of the robust approach and η is a tunable parameter. Notice from (1) that since P_1 is a probability the *gain factor* η must not exceed $n+1$ in order for the previous inequality to produce a nonempty class $\mathcal{F}_\eta$.

By defining the class $\mathcal{F}_\eta$, we imply that the detection scheme should focus on attacks with larger impact to system performance and not on small-scale or short-term attacks. We define the severity of the attack by changing the gain factor η. Values of η larger but close to 1 are equivalent to low-impact attacks whereas values significantly larger than 1 are equivalent to DoS attacks.

4. ATTACK DETECTION MODEL: SEQUENTIAL PROBABILITY RATIO TEST (SPRT)

We assume the network employs a monitoring mechanism for detection of potential malicious activities. The monitoring mechanism consists of: (i) determination of the subset of monitoring nodes $\mathcal{M}$ that act as network monitors and (ii) employment of a detection algorithm at each detector node. In this work we assume that an efficient mechanism for determination of the subset of monitoring nodes already exists and put emphasis on the detection part of the monitoring mechanism.

Due to the nature of the IEEE 802.11 MAC, the back-off measurements are enhanced by an additional sample each time a node attempts to access the channel. Intuitively, this gives rise to the employment of a sequential detection scheme in the observed problem. The objective of the detection test is to derive a decision as to whether or not misbehavior occurs with the least number of observations. A sequential detection test is therefore a procedure which decides whether or not to receive more samples with every new information it obtains. If sufficient information for deriving a decision has been made (i.e. the desired levels of the probability of false alarm and probability of miss are satisfied), the test proceeds to the phase of making a decision.

It is now clear that two quantities are involved in decision making: a stopping time N and a decision rule d_N which at the time of stopping decides between hypotheses H_0 (legitimate behavior) and H_1 (misbehavior). We denote the above combination with $D{=}(N, d_N)$.

In order to proceed with our analysis we first define the properties of an efficient detector. Intuitively, the starting point in defining a detector should be minimization of the probability of false alarms $\mathbb{P}_0[d_N = 1]$. Additionally, each detector should be able to derive the decision as soon as possible (minimize the number of samples it collects from a misbehaving station) before calling the decision function $\mathbb{E}_1[N]$. Finally, it is also necessary to minimize the probability of deciding that a misbehaving node is acting normally $\mathbb{P}_1[d_N = 0]$. It is now easy to observe that $\mathbb{E}_1[N]$, $\mathbb{P}_0[d_N = 1]$, $\mathbb{P}_1[d_N = 0]$ form a multi-criteria optimization problem. However, not all of the above quantities can be optimized at the same time. Therefore, a natural approach is to define the accuracy of each decision a priori and minimize the number of samples collected:

$$\inf_{D \in \mathcal{T}_{a,b}} \quad \mathbb{E}_1[N] \qquad (3)$$

where

$$\mathcal{T}_{a,b} = \{(N, d_N) : \mathbb{P}_0[d_N = 1] \le a \text{ and } \mathbb{P}_1[d_N = 0] \le b\}$$

The solution D^* (optimality is assured when the data is i.i.d. in both classes) to the above problem is the SPRT [11]. The SPRT test is defined in terms of the log-likelihood ratio S_n

$$S_n = \ln \frac{f_1(x_1, \ldots, x_n)}{f_0(x_1, \ldots, x_n)}, \qquad (4)$$

of the two joint probability density functions $f_i(x_1, \ldots, x_n)$ of the data $\{x_1, \ldots, x_n\}$ under hypothesis $\mathbf{H}_i$, $i = 0, 1$. The corresponding stopping time N and decision rule d_N are then given by

$$N = \inf_n \{n : S_n \notin [L, U]\} \qquad (5)$$

$$d_N = \begin{cases} 1 & \text{if } S_N \ge U \\ 0 & \text{if } S_N \le L, \end{cases} \qquad (6)$$

where $L \approx \ln \frac{b}{1-a}$ and $U \approx \ln \frac{1-b}{a}$. We can see that the SPRT test continues sampling as long as the log-likelihood ratio takes values within the interval (L, U) and stops taking more samples the first time it exceeds it. Once stopped, the decision function d_N decides in favor of hypothesis $\mathbf{H}_1$ when S_N exceeds the largest threshold and in favor of $\mathbf{H}_0$ when S_N is below the smallest threshold. If in particular the data are independent and identically distributed (i.i.d.) under both hypotheses then the log-likelihood ratio S_n takes the following simple form

$$S_n = \sum_{k=1}^{n} \ln \frac{f_1(x_k)}{f_0(x_k)} = S_{n-1} + \ln \frac{f_1(x_n)}{f_0(x_n)}, \; S_0 = 0. \qquad (7)$$

Here $f_i(x)$ is the common probability density function (pdf) of the samples under hypothesis $\mathbf{H}_i$, $i = 0, 1$. Notice that the recurrent relation in the right hand side of (7) allows for an efficient computation of the statistics S_n which requires only constant number of operations per time step and finite memory (we only need to store S_n as opposed to the whole sequence $\{x_n, \ldots, x_1\}$).

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4367
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4367

Furthermore, by Wald's identity:

$$\mathbb{E}_j[N] = \frac{\mathbb{E}_j[S_N]}{\mathbb{E}_j\left[\ln\frac{f_1(x)}{f_0(x)}\right]} = \frac{\mathbb{E}_j[S_N]}{\int_0^W f_j(x)\ln\frac{f_1(x)}{f_0(x)}} \qquad (8)$$

with $\mathbb{E}_1[S_N] = Lb + U(1-b)$ and $\mathbb{E}_0[S_N] = L(1-a) + Ua$. The coefficients $j = 0, 1$ in Eq.(8) correspond to legitimate and adversarial behavior respectively.

Before proceeding towards further analysis, we note that the denominator in Eq. 8 represents the denotes the Kullback-Leibler divergence between two distributions.

5. DERIVATION OF THE WORST-CASE ATTACK IN THE PRESENCE OF INTERFERENCE

As it has already been mentioned in Sect. 2, it is of essential importance to investigate how interference affects the performance of the quickest detection system. In this work we assume that interference arises due to concurrent transmissions of nodes that are not in each other's range, but are in the range of the observer node. Consequently, this results in lossy observations at the detector side. We now present the assumed interference model and derive the worst-case attack in the presence of interference.

5.1 Interference model

In this work, we assume that interference at the detector side results in lossy observations. As a consequence, the detector fails to detect new control messages sent by an attacker with probability p_2. Due to the inability to observe the actual back-off sequence, the detector is no longer able to derive the original attacker's strategy $f_1^\star(x)$. Instead, it will observe the new back-off distribution, $\tilde{f_1^\star}(x)$ which is generated according to the following set of rules:

1. the real back-off x_1 is observed with probability $1-p_2$;
2. back-off x_1+x_2 is observed with probability $p_2(1-p_2)$ (one transmission of the attacker is not observed);
3. back-off $x_1+x_2+x_3$ is observed with probability $p_2^2(1-p_2)$ (2 transmissions of the attacker are not observed);
4. ...
5. back-off $x_1+\ldots+x_i$ is observed with probability $p_2^{i-1}(1-p_2)$ (i-1 transmissions of the attacker are not observed);

where each back-off x_i is generated according to the original pdf $f_1^\star(x)$. For example, the new pdf generated by missing one transmission, can be calculated as $P(X_1 + X_2 \leq Y)$, which is nothing else but the convolution of $f_1^\star(x) * f_1^\star(x)$(since each X_i is generated according to $f_1^\star(x)$). In order to illustrate this, we present a simple scenario in Fig. 1. We assume the malicious node M attempts to access the channel using the optimal pdf $f_1^\star(x)$, generating corresponding back-off values b_i. When no interference is present, an observer (detector) that is measuring back-off values of neighboring stations measures time periods between successive RTS messages T_i, and calculates the corresponding back-off values b_i (an example of such calculation is provided in [9]). However, if the observer misses the second control message, it measures back-off $b_1 + b_2$ at a time instance t_2 instead of registering two successive back-off values b_1 and b_2 at time instances t_1 and t_2 respectively. Depending on the strength and duration of interference, the observer retrieves a corrupted back-off sequence, which results in detection delay.

Before proceeding towards derivation of the worst-case attack in the presence of interference we first briefly present the proposed detection scheme that minimizes detection delay.

5.2 Worst-case attack

We now derive the expression for the least favorable distribution of an adversary in the presence of interference following the framework from [9] and evaluate the performance loss of the detector in such scenarios. We assume that the adversary generates the back-off sequence using an optimal pdf $f_1^\star(x)$, which results in achieving maximal detection delay. We mentioned in Sect. 2 that as a consequence of interference, the detector observes a different back-off sequence and a different pdf of both the adversary and legitimate participant: $\tilde{f_1^\star}(x)$ and $\tilde{f}_0(x)$ respectively. Following the approach from [9], we know that the detection delay is inversely proportional to $\int \tilde{f_1^\star}(x)\log\frac{\tilde{f_1^\star}(x)}{\tilde{f}_0(x)}dx$. However, $\tilde{f}_0(x)$ is no longer uniform and now the problem of finding the attack that maximizes the required number of observations needed for detection reduces to the problem:

$$\min_{\tilde{f_1^\star}} \int \tilde{f_1^\star}(x)\log\frac{\tilde{f_1^\star}(x)}{\tilde{f}_0(x)}dx \qquad (9)$$

subject to the constraints,

$$\int x f_1^\star(x)dx \leq \eta \text{ and } \int x f_1^\star(x)\,dx = 1 \qquad (10)$$

where η has the same meaning as in Sect. 3. We now observe that the constraints from Eq. 10 are with respect to $f_1^\star(x)$ and the original expression in Eq. 9 that needs to be minimized is with respect to $\tilde{f_1^\star}(x)$. In order to derive an expression for the optimal pdf we first prove the following claim:

Claim 2. *Imposing constraints on $f_1^\star(x)$ is equivalent to imposing constraints on $\tilde{f_1^\star}(x)$, i.e. there exists a linear relation between the constraints with a known factor.*

Proof. Assuming that the probability of missing a control message sent by an attacker is p_2, the expression for $\tilde{f_1^\star}(x)$ can be written as:

$$\begin{aligned}\tilde{f_1^\star}(x) &= (1-p_2)f_1^\star(x) + p_2(1-p_2)f_1^\star * f_1^\star(x) + \qquad (11)\\ &+ \; p_2^2(1-p_2)f_1^\star * f_1^\star * f_1^\star(x) + \ldots\end{aligned}$$

where "*" denotes convolution. By applying the Laplace transform to Eq.(12) the following expression is obtained:

$$\tilde{F}_1^\star(s) = \sum_{i=1}^{\infty} p_2^{i-1}(1-p_2)^i (F_1^\star)^i(s) = \frac{(1-p_2)F_1^\star(s)}{1-p_2F_1^\star(s)} \qquad (12)$$

After applying the well known properties of the Laplace transform: F(0)=1 and $\frac{\partial F(s)}{\partial s}_{|s=0} = -\int xf(x)dx$ to Eq. (12), the following expression is obtained:

$$\frac{\partial \tilde{F}_1^\star(s)}{\partial s}_{|s=0} = (1-p_2)[1+2p_2+3p_2^2+\ldots]\frac{\partial F_1^\star(s)}{\partial s}_{|s=0} \qquad (13)$$

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4367
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4367

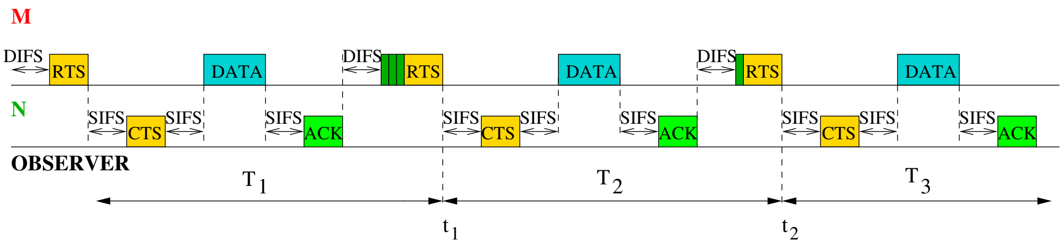

Figure 1: Noise diagram.

By using $\frac{\partial F(s)}{\partial s}_{|s=0}=-\int xf(x)\,dx$ it is now easy to derive from Eq.(13) that

$$\int x\tilde{f}_1^\star(x)\,dx = \frac{1}{1-p_2}\int xf_1^\star(x)\,dx$$

which concludes the proof. □

We now transfer the constraints from $f_1^\star(x)$ to $\tilde{f}_1^\star(x)$ and form the following Lagrangian:

$$\begin{aligned} L(\tilde{f}_1^\star,\lambda,\mu) &= \int \tilde{f}_1^\star(x)\log\frac{\tilde{f}_1^\star(x)}{\tilde{f}_0(x)}\,dx \qquad (14)\\ &+ \lambda\int x\tilde{f}_1^\star(x)\,dx\\ &+ \mu\int \tilde{f}_1^\star(x)\,dx \end{aligned}$$

where μ is the Lagrange multiplier corresponding to equality constraints and λ is the Karush-Kuhn-Tucker (KKT) multiplier corresponding to the inequality constraint. The KKT conditions can be expressed as follows:

1. $\frac{\partial L}{\partial \tilde{f}_1^\star(x)}=0$
2. $\lambda \geq 0$
3. $\lambda(\int x\tilde{f}_1^\star(x)\,dx-\eta)=0$
4. $\int \tilde{f}_1^\star(x)\,dx = 1$
5. $\int x\tilde{f}_1^\star(x)\,dx \leq \eta$

In order to derive a result using the condition (1), we apply the method of variations to Eq.(15). In order to proceed further, we assume that

$$\tilde{f}_\epsilon^\star(x) = (1-\epsilon)\tilde{f}_1^\star(x)+\epsilon\delta(x)$$

which corresponds to perturbation around $\tilde{f}_1^\star(x)$. By replacing $\tilde{f}_1^\star(x)$ with $\tilde{f}_{1\epsilon}^\star(x)$ in Eq. (15), the criterion becomes a function of ϵ. Consequently, if $\tilde{f}_1^\star(x)$ is optimum, then the derivative with respect to ϵ at $\epsilon=0$ must be 0. If we take the derivative and set $\epsilon=0$, we obtain

$$\int(\delta(x)\log\frac{\tilde{f}_1^\star(x)}{\tilde{f}_0(x)}+\delta(x)+\lambda x\delta(x)+\mu\delta(x))dx = \qquad (15a)$$

$$= \int \delta(x)(\log\frac{\tilde{f}_1^\star(x)}{\tilde{f}_0(x)}+1+\lambda x+\mu)dx = 0$$

Since Eq.(15) must be valid for any density $\delta(x)$, the following expression for $\tilde{f}_1^\star(x)$ is obtained:

$$\log\frac{\tilde{f}_1^\star(x)}{\tilde{f}_0(x)}+1+\lambda x+\mu = 0$$

and consequently

$$\tilde{f}_1^\star(x) = \tilde{f}_0(x)e^{-1-\mu}e^{-\lambda x} \qquad (16)$$

By analyzing the second KKT condition, $\lambda \geq 0$, for (i) $\lambda = 0$ and (ii) $\lambda > 0$, we conclude that $\lambda > 0$ at all times, i.e. all constraints are active. We now observe that $\tilde{f}_1^\star(x)$ from Eq. (16) is of exponential nature only if $\tilde{f}_0(x)$ is either exponential nature or constant. Due to the fact that $f_0(x) \sim Unif[0,W]$

$$F_0(s) = \frac{1-e^{-Ws}}{Ws}$$

By applying the same reasoning as in Eq. (12) the following relation between $\tilde{F}_0(s)$ and $F_0(s)$ is obtained:

$$\tilde{F}_0(s) = \frac{(1-p_2)F_0(s)}{1-p_2F_0(s)} \qquad (17)$$

Obviously, $\tilde{f}_0(x)$ is neither constant nor exponential, which results in $\tilde{f}_1^\star(x)$ not being of exponential nature any more. Consequently, the analysis from [8, 4] is no longer valid. Although the adversary still accesses the channel using the pdf $f_1^\star(x)$ (and denies channel access to the legitimate participants for the same amount of time) and the legitimate participants access the channel using the uniform pdf $f_0(x)$, the detector observes different access distributions for both the adversary and legitimate participants, which results in different detection delay.

The question that arises at this point is how observing back-off sequences generated with $\tilde{f}_1^\star(x)$ instead of $f_1^\star(x)$ and $\tilde{f}_0(x)$ instead of $f_0(x)$ affects the performance of both the adversary and the detection system. We answer this question in the following section by representing our system in the form of a Markov Chain.

6. MARKOV CHAIN REPRESENTATION

As it has previously been pointed out, the detector will miss an observation with certain probability, which consequently results in erroneous back-off observations. In this analysis we adopt the approach from [12] and apply it to the case of the IEEE 802.11 noisy environment.

6.1 System model

Let $\mathcal{S} = s_1, s_2, \ldots, s_K$ denote the state space of a Markov chain with K states. Each of the observed K states corresponds to a certain interference level. We assume that each interference level results in a corresponding observation error at the detector's side. More specifically, we assume that each interference level i results in observing back-off $\tilde{x}_i = x_1 + \ldots + x_i$, $i = 2,\ldots,K$, instead of observing separate back-off values $x_1, x_2, \ldots, x_i$. Consequently, we assume

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4367
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4367

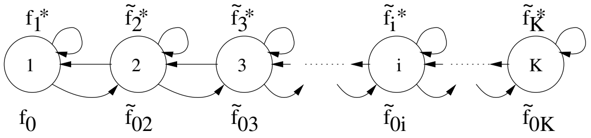

Figure 2: Markov Chain representation of the system. Each state corresponds to a different interference level.

that the detector observes an erroneous back-off generation pdf in each state $i \neq 1$, equal to $\tilde{f}_i^\star(x) = \underbrace{f_1^\star(x) * \ldots * f_1^\star(x)}_{i}$, where "*" denotes convolution. A system is said to be in the state s_i if the corresponding SINR values are in the range $[\Gamma_k, \Gamma_{k+1})$. Consequently, the system can be characterized with the following set of thresholds: $\vec{\Gamma} = [\Gamma_1, \ldots, \Gamma_{K+1}]$. Furthermore, let P_{ij} and π_i represent the state transition probability and the steady state probability respectively. We assume the transitions happen between the adjacent states, resulting in $P_{k,i} = 0$ for $|k-i| > 1$. The actual values of the thresholds and transition probabilities can be obtained by simulation (i.e. in [12]) and the analysis of methods used for such performance evaluation is beyond scope of this paper.

6.2 Performance analysis

In order to evaluate the performance of the proposed detection system in the presence of interference we first return to Fig. 2. It has already been mentioned that in each state of the Markov chain the detector observes a different back-off sequence, i.e. in state i, the observed back-off will be $x_1 + \ldots + x_i$ and the detector will register a single (large) back-off value instead of registering i separate (small) back-off values. We now observe the worst-case scenario, when $i \to \infty$. Since $x_1, x_2, \ldots$ is a sequence of random variables which are defined on the same probability space, they share the same probability distribution and are independent, the distribution of their sum $S_i = x_1 + \ldots + x_i$ approaches the normal distribution $\mathcal{N}(i\mu, \sigma^2 i)$. Hence, for K (from Fig. 2) sufficiently large, the distance between the observed distributions becomes the distance between $\mathcal{N}(K\mu_1, \sigma_1^2 K)$ and $\mathcal{N}(K\mu_0, \sigma_0^2 K)$, where μ_i, σ_i, $i = 0, 1$ represent the mean and variance of legitimate and adversarial distributions.

Due to the fact that the detection delay $\mathbb{E}[N]$ is inversely proportional to the KL-distance between the original and adversarial distributions, the only fact we are interested in at this point is how this distance changes as the interference level increases. For this analysis we again return to the Markov chain in Fig. 2. We now observe states i and $i+1$ of the Markov chain. We observe that the corresponding distributions in states i and $i+1$ are $\tilde{f}_i^\star$, $\tilde{f}_{0i}$ and $\tilde{f}_{i+1}^\star$, $\tilde{f}_{0(i+1)}$ respectively. Using the approach from [5], we form the following theorem:

Theorem 3. *If the distributions at states i and $i+1$ of the Markov chain are $\tilde{f}_i^\star$, $\tilde{f}_{0i}$ and $\tilde{f}_{i+1}^\star$, $\tilde{f}_{0(i+1)}$ respectively, then $D(\tilde{f}_i^\star || \tilde{f}_{0i}) > D(\tilde{f}_{i+1}^\star || \tilde{f}_{0(i+1)})$ for all $i \geq 1$.*

Proof.

$$\begin{aligned} & D(\tilde{f}^\star(x_i, x_{i+1}) || \tilde{f}_0(x_i, x_{i+1})) = \qquad (18) \\ & D(\tilde{f}^\star(x_i) || \tilde{f}_0(x_i)) + D(\tilde{f}^\star(x_{i+1}|x_i) || \tilde{f}_0(x_{i+1}|x_i)) = \\ & D(\tilde{f}^\star(x_{i+1}) || \tilde{f}_0(x_{i+1})) + D(\tilde{f}^\star(x_i|x_{i+1}) || \tilde{f}_0(x_i|x_{i+1})). \end{aligned}$$

□

The above theorem states that the Kullback-Leibler divergence $D(*||*)$ between the original and the adversarial distributions *decreases* as i increases. Knowing that i increases with increase of interference level, we conclude that the KL-distance between the observed distributions decreases with the increase of interference. Since the detection delay $\mathbb{E}[N]$ is inversely proportional to the KL-distance (Eq. 8), it is easy to see that the detection delay increases with increase of interference level in the system. This result was expected even by intuitive analysis, since the detector observes larger back-off sequences than the actual ones, which logically leads to delay in detection (i.e. the detector believes that the adversary is accessing the channel using legitimate back-off function). We now provide experimental evaluation of the result proved in Theorem 3.

7. PERFORMANCE EVALUATION OF THE OPTIMAL DETECTOR

The goal of the simulations is to assess the efficiency of the proposed detection system by identifying the relative impact of uncertain system parameters on it. In this specific scenario we perform detailed analysis of impact of interference on the efficiency of the quickest detection system presented in [8, 9]. In Sect. 6.2 we proved that detection delay increases in the presence of multi-user interference. In this section we extend this analysis and show how interference affects the performance of a detector that was optimized for detection under conditions with no interference. In particular, we evaluate the performance with respect to the False Alarm and Detection Rates for the original scenario from [8] and compare it with the performance in the presence of interference.

In order to illustrate the impact of interference on the performance of a detection scheme, we simulate the interference scenario where the detector observes back-off $x_1 + x_2$ instead of two separate back-off values for the value of absolute gain $\frac{\eta}{n+1} = 0.8$ in the Network Simulator Opnet. It is important to note that, just like in the scenario where no interference is present, the analysis we provide represents the worst-case scenario. The assumed scenario with constant interference levels provides us with the guarantees that the detector will perform either the same or better than this. The results are presented in Fig. 3. We observe that even low, but constant, interference level has significant impact on the performance of the detector and that the detection delay increases up to 3 times. In order to better understand the impact of interference on the performance of the detector, we note that the detection delay in the presence of interference corresponds to the adversarial strategy where the adversary attempts to access the channel for approximately 50% of time (when 33% is legitimate behavior). Assuming that we are dealing with an intelligent attacker, this setting enables him to deploy even more aggressive strategies with larger detection delay. Naturally, this setting favors the adversary. Another interesting, but expected, result can be observed from Fig. 3. We

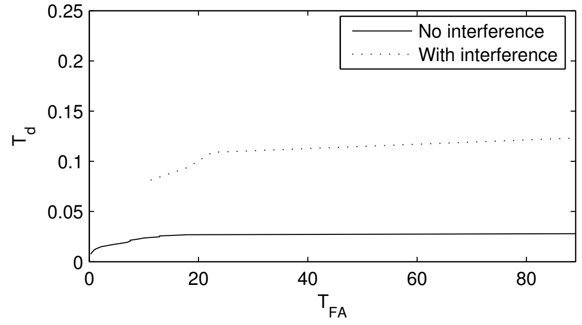

Figure 3: Performance comparison of the detection scheme with and without interference for $\frac{\eta}{n+1} = 0.8$. The resulting detection delay for $\frac{\eta}{n+1} = 0.8$ in the presence of interference corresponds to the adversarial strategy with $\frac{\eta}{n+1} \approx 0.5$.

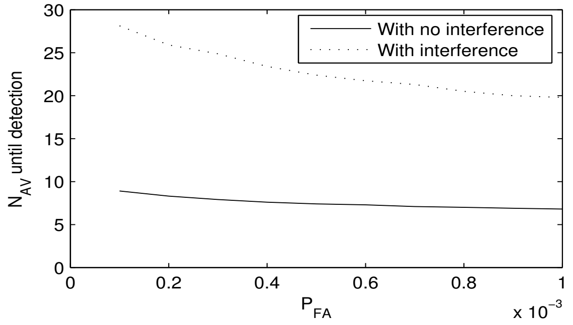

Figure 4: Average number of samples needed for attack detection (N_{AV}) with and without interference.

observe that for high values of P_{fa}, i.e. low sensitivity of the system, there are no detections. This points out that in the presence of interference we need to either adjust the parameters od our detection system or employ a better detection system with higher sensitivity if we want to maintain the same (or similar) detection rate.

To further illustrate the effects of interference on the performance of the proposed quickest detection system, we review the results presented in Fig. 4, which depicts the average number of samples needed for detection as a function of P_{fa}. It is easy to observe that for any sensitivity of a detector (i.e. any value of P_{fa}), the average number of samples needed for detection of an adversary is almost constant and up to 3 times higher than in the setting when no interference is present. Consequently, this result forces us to think whether it is efficient to deploy such detector after a certain interference level is reached. Namely, even when the False Alarm rate is low (no system resources are wasted on issuing alarms for non-existing intrusions), the system still wastes resources for collecting back-off samples, performing the SPRT test at every time instance and issuing alerts when an intrusion is detected. However, in some cases if the time instance when an intrusion is detected happens much later than the time instance of an actual attack, the adversary might have already achieved his goal and left the area or has already caused too much damage to the system, increasing the losses above the acceptable levels.

7.1 Effect of interference on False Alarm Rate

We start our assessment of the performance of the proposed detection system in the presence of interference by analyzing its impact on the number of false alarms (or equivalently False Alarm Rate). We deploy a setting in which the detection system produces 27 False Alarms in the time period of 90s in the setting when no interference is present. This is a sub-optimal setting, which results in approximately 2 False Alarms per second. However, we adopt this setting in order to illustrate the impact of interference. In the presence of interference the number of False Alarms decreases to 0. By observing only the number of False Alarms within the given time period, one could conclude that the deployed detector is optimal under the given conditions. However, knowing that due to the presence of interference the detector's perception of both legitimate and malicious back-offs is distorted, it is easy to conclude that the low number of False Alarms is not due to the efficiency of the detection system, but due to the fact that it operates at a sub-optimal point. At this point, we defer further discussion related to the False Alarm rate until Sect. 7.3 and first analyze the performance of the detection system with respect to the detection rate.

7.2 Effect of interference on Detection Rate

In order to obtain a better insight at the impact of interference on the overall performance of the proposed detection system, let us take a closer look at the impact of interference at the detection rate. One could argue that the most important feature of a detector is the number of False Alarms and if that number is low, the detection system is sufficiently efficient. However, it is important to note that in the wireless environment detection of adversaries is a time-critical activity and if an attack is not detected within a certain time frame, the resulting losses in terms of lost traffic, number of dropped packets etc. become significant and the detection system becomes obsolete since its main purpose has already been defeated. For that reason, we first review Fig. 5 and analyze the impact of interference on average detection delay for a wide range of adversarial strategies, i.e. we vary $\frac{\eta}{n+1} \in [0.6, 0.9]$. We now observe that the detector optimized for functioning in the environment with no (or very low) amount of interference, exhibits sub-optimal performance for all attack strengths, except for DoS attacks, when legitimate participants are not allowed to access channel at all. Hence, although such system has zero False Alarms, its performance with respect to the detection delay is unacceptable for most adversarial strategies.

To further illustrate the effects of interference, we review the results in Fig. 6. We observe that the detection rate significantly decreases and the proposed detection system is not usable in such settings. Looking at Theorem 3, the above results can be easily explained (a more detailed analysis of this issue from a different perspective is provided in [2], where the author proves that P_d decreases as the distance between the observed distribution decreases). Due to the fact that the distance among the observed distributions *decreases* as interference increases, the detection delay increases.

7.3 Receiver Operating Characteristic (ROC) interpretation

The usual practice in performance evaluation of detection systems is to observe the tradeoff between the False Alarm rate and the detection rate (ROC curve). In this section we

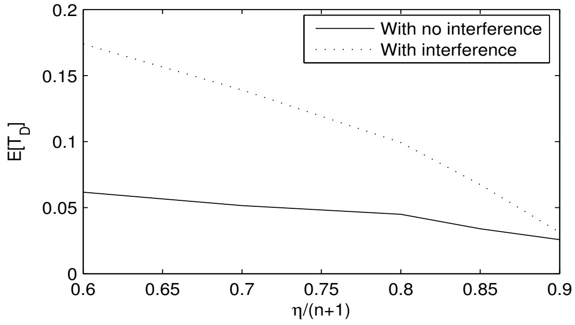

Figure 5: Average detection delay ($E[T_D]$) with and without interference.

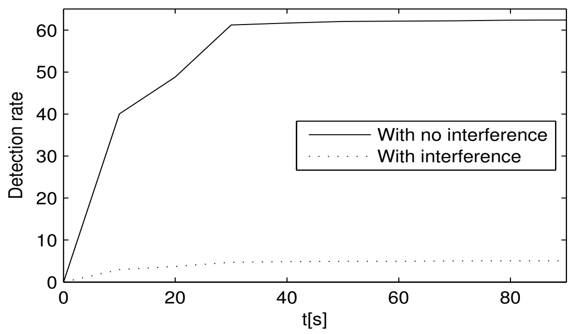

Figure 6: Average detection rate with and without interference.

attempt to interpret the results presented in the previous sections using ROC curves. The results in Sect. 7.1 and 7.2 provide useful insights about the response of the system with respect to attacks of various strengths in the presence of interference. In this section, with the help of Fig. 7, we explain how interference affects efficiency of a detection system optimized for functioning in the scenarios where no or low interference is present. We assume that the parameters of a detection system (i.e. the (P_{fa}, P_d) pair) were chosen to minimize the detection delay with a low False Alarm rate. In this section, using the results from Sect. 7.1 and 7.2, we explain how interference forces a non-adaptive detection system to function using sub-optimal parameter configuration. We will also further illustrate our claim from Sect. 7.1 that low number of False Alarms does not always correspond to an efficient detector.

The performance evaluation metrics usually assume the knowledge of some uncertain parameters such as the likelihood of an attack, interference levels, costs of False Alarms and missed detections. However, the uncertain parameters frequently change in a wireless environment and can significantly hinder the expected performance of a given detection system. Consequently, the evaluation of a detection system configured with erroneous parameters might not be of significant value.

We now observe that the presence of interference can severely affect the detector's performance. The solution to this problem is to have multiple detectors with different sensitivity levels available and depending on the requirements of the detector and environment conditions, decide which ones to use. For example, in systems where timely decision making is of crucial importance, the deployed detectors need to be more robust to interference (and thus more expensive [3]) and it is also advisable to deploy multiple detectors in order to minimize the probability of error in decision making. However, this strategy significantly increases the overall cost and may not be applicable in most scenarios.

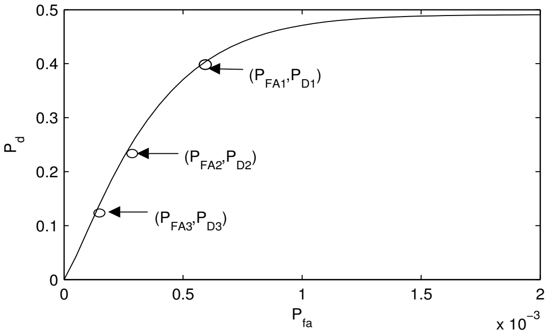

Figure 7: Typical ROC curve. With the increase of interference, the operating point is forced towards the lower values (P_{fa}, P_d). Consequently the observed detection system becomes unusable after a certain level of interference is reached.

Finally, as we have seen, it is important not only to detect misbehavior with a quickest detection system, but the crucial step in designing a precise and robust detector is to evaluate the environment in which it will be operating and be able to provide certain performance guarantees, such as that in environments with interference levels higher than a pre-specified threshold, the system will be able to to guarantee detection delay T_{D_i} with certain P_{FA_i} and P_{D_i}. If the guarantees do not satisfy the needs of the system, either a more expensive detection system needs to be purchased or alternative detection methods need to be deployed.

To illustrate this claim we now look at a typical ROC curve in Fig. 7 (detailed analysis of ROC curves and their performance can be found in [1]). Assume that the detector was configured to function at an optimal point of the ROC curve, that corresponds to the pair (P_{fa1}, P_{d1}). Note that this curve is just an example and that in realistic scenario, the False Alarm rates should be much lower than the ones presented in Fig. 7. If the interference level increases, the number of False Alarms (and consequently the P_{fa}) decreases and the corresponding P_d also decreases. Consequently, the operating point of the detector shifts to a point (P_{fa2}, P_{d2}) (with $P_{d_1} > P_{d_2}$ and $P_{fa_1} > P_{fa_2}$) which increases overall cost, since we assume the cost is inversely proportional to the detection delay. Consequently, the further increase in interference levels forces the detector to operate at the operating point (P_{fa_k}, P_{d_k})=(0,0). The interpretation of this result is that the features of the deployed detector are not good enough for the environment and that either more detectors need to be deployed or another, more robust, detection system needs to be designed.

Alternatively, a user may decide to maintain the same P_d even when the interference is present. In this specific setting, the corresponding P_{fa} needs to be increased (i.e. we compromise with having a larger number of false alarms in order to maintain the same detection rate). This will result in a new ROC curve (a new detection system). Naturally, this approach should be taken in extreme cases as it is expensive and time consuming to deploy a new detection system due to the change of interference levels. A more reasonable approach, applicable due to the random nature of wireless networks, is to deploy an *adaptive* detection system, which will change its settings depending on the perceived interference levels and guarantee certain performance levels as long as interference level remains below the pre-defined critical value.

8. CONCLUSIONS AND FUTURE WORK

This work represents the first step towards providing performance bounds of intelligent adaptive adversaries in wireless networks as well as providing a set of tools for evaluation of performance of detection schemes in the presence of interference. The interpretation of results provided in Sect. 7 points out that it is desirable to have an adaptive detection system that will change its parameters according to the conditions in the network and subject to its own performance parameters (such as P_{fa}, P_d).

As a part of future work,we intend to test the performance of various detection systems (with different ROC curves, i.e. different sensitivity parameters) under a wide range of interference values. In addition to that, we intend to extend the work presented in [4] by comparing the performance of detection schemes in the presence of interference and obtain a more realistic set of performance bounds for parametric (SPRT) and non-parametric (DOMINO, np-CUSUM) detection procedures.

9. REFERENCES

[1] S. Axelsson. The base-rate fallacy and its implications for the difficulty of intrusion detection. In *Proc. of the 6th ACM Conference on Computer and Communications Security (CCS '99)*, pages 1–7, November 1999.

[2] R. E. Blahut. *Principles and Practice of Information Theory.* Addison-Wesley, 1987.

[3] A. A. Cárdenas, J. S. Baras, and K. Seamon. A framework for the evaluation of intrusion detection systems. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, Oakland, CA, May 2006.

[4] A. A. Cárdenas, S. Radosavac, and J. S. Baras. Performance comparison of detection schemes for MAC layer misbehavior. In *IEEE INFOCOM'07: Proceedings of the 26th Annual IEEE Conference on Computer Communications*, pages 1496–1504, 2007.

[5] T. M. Cover and J. A. Thomas. *Elements of Information Theory.* John Wiley & Sons, Inc., N. Y., 1991.

[6] IEEE. IEEE wireless LAN medium access control (MAC) and physical layer (PHY) specifications, 1999.

[7] P. Kyasanur. Selfish MAC layer misbehavior in wireless networks. *IEEE Transactions on Mobile Computing*, 4(5):502–516, 2005. Senior Member-Nitin H. Vaidya.

[8] S. Radosavac, J. S. Baras, and I. Koutsopoulos. A Framework for MAC Protocol Misbehavior Detection in Wireless Networks. In *Proceedings of the 4th ACM workshop on Wireless security*, pages 33–42, Cologne, Germany, September 2005.

[9] S. Radosavac, G. V. Moustakides, J. S. Baras, and I. Koutsopoulos. An analytic framework for modeling and detecting access layer misbehavior in wireless networks. *to appear in ACM Transactions on Information and System Security (TISSEC)*, 11(4), November 2008.

[10] M. Raya, J.-P. Hubaux, and I. Aad. DOMINO: A system to detect greedy behavior in IEEE 802.11 Hotspots. In *Proceedings of MobiSys '04*, pages 84–97, 2004.

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

[12] Q. Zhang and S. A. Kassam. Finite-state Markov model for Rayleigh fading channels. *IEEE Transactions on Communications*, 47(11):1688–1692, November 1999.

Digital Object Identifier: 10.4108/ICST.VALUETOOLS2008.4367
http://dx.doi.org/10.4108/ICST.VALUETOOLS2008.4367