This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.

Design and Analysis of Defection-Proof MAC Protocols Using a Repeated Game Framework

Khoa T. Phan, Jaeok Park, and Mihaela van der Schaar
Electrical Engineering Department, University of California, Los Angeles (UCLA)
Email: {kphan, jaeok, mihaela}@ee.ucla.edu

***Abstract*—It is well-known that medium access control (MAC) protocols are vulnerable to the selfish behavior of nodes, which often results in inefficient use of resources. In this work, we aim to overcome this inefficiency by constructing a class of defection-proof MAC protocols in the context of slotted multiple access communications. The operation of the proposed protocols can be divided into a review phase and a reciprocation phase. In a review phase, nodes cooperate and collect signals on the behavior of other nodes. At the end of a review phase, nodes perform a statistical test independently to determine whether there has been a defecting node in the system. In a reciprocation phase, a node cooperates if it concludes that no defection has occurred and carries out a punishment otherwise. We provide sufficient conditions for protocols to be defection-proof against a constant defection strategy and to achieve an arbitrarily small efficiency loss. We analyze an example of a statistical test based on which we can build protocols that satisfy the sufficient conditions.**

***Index Terms*—Defection-proof protocols, game theory, MAC protocols, repeated games.**

I. Introduction

In wireless communication networks, multiple nodes often share a common channel and contend for access. To resolve the contention problem, many different distributed medium access control (MAC) protocols have been devised and are currently used in international standards (e.g., IEEE 802.11a/b/g MAC protocols) [1], [2]. Recently, the game theory framework has been used to analyze the variations of the slotted Aloha protocol [3], [4]. Most MAC protocols are designed with the assumption that nodes will comply with the rules imposed by the protocol. However, this assumption cannot be taken for granted when nodes are selfish and able to manipulate a given protocol. The literature has shown that the selfish behavior of nodes can degrade the performance of other nodes as well as that of the system (see for example, [5]). Therefore, the design of distributed MAC protocols that are robust to selfish manipulation is important to provide a reliable and efficient network performance.

In this paper, we propose and analyze a class of Aloha-type protocols that can preclude undue channel access by selfish nodes. The proposed protocols are fully distributed in that they require neither a central controller nor coordination messages. Nodes cannot communicate with each other and make their decisions independently based on their local information. The design of protocols in the presence of network manager was studied in pricing based networks [6], noncooperative Stackelberg equilibrium based networks [7], or correlated equilibrium based networks [8]. Our design methodology is based on a repeated game framework [9], where nodes can condition their transmission decisions on their past observations. We use the notion of review strategies [10], [11] in which each node reviews the behavior of other nodes based on its signals. A potential punishment triggered by a node that obtained a dissatisfactory performance can provide incentives for nodes to adhere to the prescribed protocol.

Sustaining cooperation using the repeated game approach has been studied in communications and networking [12], [13]. These works consider a scenario where a deviation can be detected without errors, in which case it is relatively easy to deter any deviation by triggering punishment when a deviation is observed. On the contrary, we consider a scenario where the choice of a node, a transmission probability, cannot be observed directly and nodes can detect a deviation only statistically. We also allow that the observations of nodes are different across nodes, in which case it is difficult to coordinate the behavior of nodes. Our main contributions can be summarized as follows.

- We formalize a slotted multiple access communications scenario as a repeated game. This approach allows us to formally express distributed defection-proof protocols and our design problem.
- We propose a general design framework for protocols that are defection-proof against a certain type of selfish behavior. We provide necessary and sufficient conditions for a protocol to be defection-proof and sufficient conditions for obtaining a defection-proof protocol that achieves an arbitrarily small efficiency loss.
- We study defection-proof protocols in a specific scenario where nodes obtain signals on the results of their transmission attempts and the statistical test is based on the empirical success frequency of a node.

The paper is organized as follows. In Section II, we formulate a slotted multiple access communications scenario as a repeated game and state our design problem. In Section III, we propose a class of protocols based on a statistical test and study their properties in terms of defection-proofness and performance. In Section IV, we provide analytical and numerical results on the defection-proof protocols in a specific scenario. In Section V, we conclude.

978-1-4244-5638-3/10/$26.00 ©2010 IEEE

II. Repeated Game Framework for Slotted Multiple Access Communications

A. Random Access Game

We consider a wireless communication network with a fixed set $\mathcal{N} = \{1, 2, \ldots, N\}$ of N nodes interacting over time. Time is divided into slots, and in each slot, every node has a packet to transmit (i.e., saturated arrival) and can send the packet or wait. Due to interference in the shared communication channel, a packet is transmitted successfully only if there is no other packet transmitted in the same slot. If more than one transmission takes place in a slot, a collision occurs and no packet is transmitted successfully. We model the interaction of nodes in a single slot as a non-cooperative game in normal form, called the *random access game*.

The set of pure actions available to node i in a slot is $A_i \triangleq \{T, W\},\ i \in \mathcal{N}$, where T stands for "transmit" and W for "wait." We denote the pure action of node i by $a_i \in A_i$ and a pure action profile by $\mathbf{a} \triangleq (a_1, \ldots, a_N) \in \mathcal{A} \triangleq \prod_{i\in\mathcal{N}} A_i$. The mixed action of node i is a probability distribution on A_i. Since there are only two pure actions, a mixed action can be represented by a transmission probability p_i while the set of mixed actions for node i can be written as $P_i \triangleq [0, 1]$. A mixed action profile is denoted by $\mathbf{p} \triangleq (p_1, \ldots, p_N) \in \mathcal{P} \triangleq \prod_{i\in\mathcal{N}} P_i$. We define the payoff function of node i by $u_i : \mathcal{A} \to \mathbb{R}$, where $u_i(\mathbf{a}) = 1$ if $a_i = T$ and $a_j = W$ for all $j \neq i$ and $u_i(\mathbf{a}) = 0$ otherwise. Then the expected payoff of a node is given by the probability that it has a successful transmission, and with a slight abuse of notation, the payoff of node i when mixed action profile $\mathbf{p}$ is chosen can be expressed as

$$u_i(\mathbf{p}) = p_i \prod_{j\in\mathcal{N}\setminus\{i\}} (1 - p_j).$$

The random access game is defined by the tuple $\Gamma = \langle \mathcal{N}, (A_i)_{i\in\mathcal{N}}, (u_i)_{i\in\mathcal{N}} \rangle$. It is well-known from the static analysis of the random access game that there is at least one node i such that $p_i = 1$ at any Nash equilibrium (NE) [5], [7]. That is, when nodes myopically maximize their own payoffs, there is at least one node always transmitting its packet, and thus at most one node can obtain a positive payoff. In this paper, we investigate whether the better utilization of the channel (i.e., a positive payoff for every node) can be achieved by analyzing the random access game as a repeated game.

B. Repeated Game Model

We now formulate the repeated game model of the random access game, where nodes can condition their actions on their past observations, or their information history. We assume that at the end of each slot nodes can obtain signals on the pure action profile chosen in the slot. Let Z_i be the finite set of signals that node i can receive. Then a signal structure of the random access game is specified by $(\mathcal{Z}, Q)$, where $\mathcal{Z} \triangleq \prod_{i\in\mathcal{N}} Z_i$ and Q is a mapping from $\mathcal{A}$ to $\Delta(\mathcal{Z})$. $Q(\mathbf{a})$ represents the distribution of signals when pure action profile $\mathbf{a}$ is chosen. For example, in the slotted Aloha protocol [1], a node receives an ACK signal when it transmits and succeeds. In this example, the signal space can be written as $Z_i = \{S, F\}$, for all $i \in \mathcal{N}$, where S means that the node receives an ACK signal and F means that it does not. If there is no error in the transmission and reception of ACK signals, the signal distribution Q is such that $Q(\mathbf{a})$ puts probability mass 1 on $\mathbf{z} \in \mathcal{Z}$ with $z_i = S$ and $z_j = F$ for all $j \neq i$ if $a_i = T$ and $a_j = W$ for all $j \neq i$, for each $i \in \mathcal{N}$, and probability mass 1 on $z_i = F$ for all i otherwise. Note that this signal structure corresponds to private monitoring [9] in that it is possible for nodes to receive different signals.

The history of node i in slot t contains the signals that node i has received by the end of slot $t-1$, i.e., $h_i^t = (z_i^0, \ldots, z_i^{t-1})$, for $t = 1, 2, \ldots$, where z_i^t represents the signal that node i receives in slot t and z_i^0 is set as an arbitrary element of Z_i.[1] The set of the slot t histories of node i is written as H_i^t, and the set of all histories of node i is defined by $H_i \triangleq \cup_{t=1}^{\infty} H_i^t$. The (behavior) strategy of node i specifies a mixed action for node i given any history it can obtain. Thus, it can be represented by a mapping $\sigma_i : H_i \to P_i$. We use Σ_i to denote the set of the strategies of node i. We define a *protocol* as a strategy profile $\sigma \triangleq (\sigma_1, \ldots, \sigma_N) \in \Sigma \triangleq \prod_{i\in\mathcal{N}} \Sigma_i$. We sometimes write $\sigma = (\sigma_i, \sigma_{-i})$, where σ_{-i} denotes the strategies of the nodes other than node i.

To evaluate payoffs in the repeated game model, we use the limit of means criterion since the length of a slot is typically short. A protocol σ induces a probability distribution on the sequences of mixed action profiles $\{\mathbf{p}^t\}_{t=1}^{\infty}$. The (expected) payoff of node i under protocol σ can be expressed as

$$U_i(\sigma) = \liminf_{J\to\infty} E\left[\frac{1}{J}\sum_{t=1}^{J} u_i(\mathbf{p}^t)\middle|\sigma\right]. \tag{1}$$

C. Design Problem

Definition 1: A protocol $\sigma \in \Sigma$ is *defection-proof* (DP) against a strategy $\sigma_i' \in \Sigma_i$ of node i if

$$U_i(\sigma_i, \sigma_{-i}) \geq U_i(\sigma_i', \sigma_{-i}).$$

Definition 1 says that when σ that is DP against σ_i' is prescribed, node i cannot gain by deviating to σ_i'. Note that σ constitutes a NE of the repeated random access game if σ is DP against σ_i', for all $\sigma_i' \in \Sigma_i$, for all $i \in \mathcal{N}$. Hence, NE is more robust than defection-proofness. However, as pointed out in [14], it is difficult, if not impossible, to construct a NE with strategies that are simple and easy to compute. Thus, we focus on a simpler problem of constructing an DP protocol against a particular deviation strategy, and our result will lay a foundation for finding a NE protocol in future research. We fix two transmission probabilities: the cooperation probability, $p_c \in (0, 1)$, and the defection probability, $p_d \in (p_c, 1]$. Our problem is to design a protocol that induces selfish nodes to choose p_c as frequently as possible when they have an option to always choose p_d. In other words, we look for a protocol

[1] In slot t, node i also knows its past mixed actions $(p_i^1, \ldots, p_i^{t-1})$ and the realizations $(a_i^1, \ldots, a_i^{t-1})$ of its mixed actions. However, since we focus on protocols using only past signals, we do not include these in our history specification.

that is DP against a constant defection strategy $\sigma^d \in \Sigma_i$, which specifies $\sigma^d(h_i^t) = p_d$ for all $h_i^t \in H_i$, for all $i \in \mathcal{N}$.

III. Design and Analysis of defection-proof Protocols

A. Defection-proof Protocols Based on a Statistical Test

For simplicity, we consider a scenario where the signal structure is symmetric and focus on symmetric protocols, i.e., σ with $\sigma_1 = \cdots = \sigma_N$. We consider a class of strategies called *review strategies* [10]. When a node uses a review strategy, it starts from a *review phase*, for which it collects its signals. When the review phase ends, the node performs a statistical test based on the signals whose null hypothesis is that every node transmitted with cooperation probability p_c during the review phase. Then the node moves to a *reciprocation phase* where it transmits with probability p_c if the test is passed and with probability 1 if the test fails. When the reciprocation phase ends, a new review phase begins. A review strategy, denoted by σ^r, can be characterized by three elements, (R, L, M), where R is a statistical test, and L and M are natural numbers that represent the length of a review phase and a reciprocation phase, respectively. Thus, we sometimes write σ^r as $\sigma^r(R, L, M)$.

Given a symmetric protocol that prescribes a review strategy, we can compute two probabilities of errors.

- False punishment probability $P_f(R, L)$: the probability that there is at least one node whose test fails after a review phase when nodes follow a protocol $\sigma_r \triangleq (\sigma^r, \ldots, \sigma^r)$.
- Miss detection probability $P_m(R, L)$: the probability that there is no node among those following σ^r whose test fails after a review phase when there is exactly one node deviating to σ^d from σ^r.

Since we focus on symmetric protocols, we use $U(\sigma^1; \sigma^2)$ to denote the payoff of a node when it follows σ^1 while every other node follows σ^2. Define $\tau_c(x) = xp_c(1-p_c)^{N-1}$, $\tau_p(x) = x(1-p_c)^{N-1}$, and $\tau_d(x) = xp_d(1-p_c)^{N-1}$, for $x = 1, 2, \ldots$. Then the payoff of a node when every node follows a review strategy σ^r is given by

$$U(\sigma^r; \sigma^r) = \frac{1}{L+M}\Bigg(\tau_c(L) + (1-P_f)\,\tau_c(M) + \left\{(1-P_f)^{\frac{N-1}{N}}\left[1-(1-P_f)^{\frac{1}{N}}\right]\right\}\tau_p(M)\Bigg). \quad (2)$$

The payoff of a node choosing defection strategy σ^d while other nodes follow σ^r is given by

$$U(\sigma^d; \sigma^r) = \frac{1}{L+M}\left[\tau_d(L) + P_m\tau_d(M)\right]. \quad (3)$$

By Definition 1, σ_r is DP against σ^d if and only if

$$U(\sigma^r; \sigma^r) \geq U(\sigma^d; \sigma^r). \quad (4)$$

The following theorem provides the necessary and sufficient conditions for a review strategy to be DP against σ^d.

Theorem 1: Given $p_c \in (0, 1)$ and $p_d \in (p_c, 1]$, protocol σ_r specifying a review strategy $\sigma^r(R, L, M)$ is DP against σ^d if and only if $g(R, L) > 0$ and $M \geq \tilde{M}(R, L)$, where

$$g(R, L) \triangleq [1 - P_f(R, L)]^{\frac{N-1}{N}} - [1 - P_f(R, L)](1 - p_c) - P_m(R, L)p_d \quad (5)$$

and

$$\tilde{M}(R, L) \triangleq \frac{L(p_d - p_c)}{g(R, L)}. \quad (6)$$

Proof: Let

$$\tilde{g}(R, L, M) \triangleq U(\sigma^r; \sigma^r) - U(\sigma^d; \sigma^r) = \frac{1}{L+M}\left[M(1-p_c)^{N-1}g(R, L) + \tau_c(L) - \tau_d(L)\right].$$

By (4), protocol σ_r is DP against σ^d if and only if $\tilde{g}(R, L, M) \geq 0$. It is easy to check that $g(R, L) > 0$ and $M \geq \tilde{M}(R, L)$ imply $\tilde{g}(R, L, M) \geq 0$. Suppose $\tilde{g}(R, L, M) \geq 0$. Since $\tau_c(L) - \tau_d(L) = L(p_c - p_d)(1-p_c)^{N-1} < 0$, it follows that $g(R, L) > 0$, and we obtain $M \geq \tilde{M}(R, L)$. ■

We should mention that Theorem 1 can also be seen as providing sufficient and necessary conditions for the **existence** of protocols DP against a given σ^d which is stronger than providing conditions for a review to be DP against σ^d.

B. Price of Selfishness

Theorem 1 characterizes the set of protocols based on a review strategy that are DP against σ^d. We propose a measure of inefficiency due to the selfishness of nodes, which can be used to evaluate an DP protocol. We define the system payoff as the sum of the payoffs of all the nodes. When nodes are obedient, we can make nodes choose p_c, which yields the system payoff

$$V_c = Np_c(1-p_c)^{N-1}.$$

When an DP protocol σ_r is used to deal with selfish nodes, we obtain the system payoff

$$V(\sigma_r) = NU(\sigma^r; \sigma^r).$$

Since signals provide only imperfect information about the transmission probabilities of other nodes, a punishment can be triggered even when all nodes follow an DP protocol σ_r. This results in an efficiency loss, which we measure by the *price of selfishness* (PoS) defined by

$$\mathcal{P}_s(\sigma_r) = V_c - V(\sigma_r). \quad (7)$$

Theorem 2: Let $p_c = 1/N$. Then $\mathcal{P}_s(\sigma_r) \geq 0$ for all σ_r DP against σ^d (with equality if and only if $P_f = 0$).

Proof: Fix an DP protocol σ_t. Using (2) and (7), we can express the PoS as

$$\mathcal{P}_s(\sigma_r) = \frac{NM}{L+M}(1-p_c)^{N-1}[p_cP_f - (1-P_f)^{\frac{N-1}{N}} + (1-P_f)]. \quad (8)$$

Since $(1-P_f)^{\frac{N-1}{N}}$ is concave, we have $(1-P_f)^{\frac{N-1}{N}} \leq 1 - \frac{N-1}{N}P_f$ for $P_f \in [0, 1]$, with equality if and only if $P_f = 0$. Using $p_c = 1/N$, we obtain the result. ■

Note that $p_c = 1/N$ maximizes V_c [15]. Theorem 2 says that when p_c is chosen to maximize the system payoff, there is always a positive efficiency loss unless we can construct a perfect statistical test in a sense that punishment is never triggered when every node cooperates. From (8), we can obtain the following result immediately.

Corollary 1: Let $p_c = 1/N$. Suppose that two protocols $\sigma_r(R, L, M)$ and $\sigma'_r(R, L, M')$ are DP against σ^d. Then $\mathcal{P}_s(\sigma_r) \geq \mathcal{P}_s(\sigma'_r)$ if and only if $M \geq M'$.

Corollary 1 implies that for given (R, L) such that $g(R, L) > 0$, choosing $M = \lceil \tilde{M}(R, L) \rceil$ minimizes the PoS while having $\sigma_r(R, L, M)$ DP against σ^d, where $\lceil \cdot \rceil$ denotes the ceiling function. When p_c is chosen to maximize the system payoff and the statistical test is imperfect, it is optimal to set the length of a reciprocation phase just enough to deter potential deviations since punishment is detrimental to the system payoff. This observation allows us to reduce the design choice to (R, L). The following theorem provides a sufficient condition on the statistical test for constructing an DP protocol that achieves an arbitrarily small PoS.

Theorem 3: Let $p_c = 1/N$. Suppose that R satisfies $\lim_{L\to\infty} P_f(R, L) = 0$ and $\lim_{L\to\infty} P_m(R, L) = 0$. Then for any $\delta > 0$, there exist L and M such that $\sigma_r(R, L, M)$ is DP against σ^d and $\mathcal{P}_s(\sigma_r) < \delta$.

Proof: $\lim_{L\to\infty} P_f(R, L) = 0$ and $\lim_{L\to\infty} P_m(R, L) = 0$ imply that $\lim_{L\to\infty} g(R, L) = p_c > 0$. By Theorem 1, we can construct an DP protocol by choosing L sufficiently large and M as $\lceil \tilde{M}(R, L) \rceil$. By Corollary 1, $\mathcal{P}_s(\sigma_r)$ is increasing in M, and thus we have

$$0 \leq \mathcal{P}_s(\sigma_r) \leq \frac{N(\tilde{M}+1)}{L + (\tilde{M}+1)}(1-p_c)^{N-1} [p_c P_f - (1-P_f)^{\frac{N-1}{N}} + (1-P_f)]. \quad (9)$$

Note that $\lim_{L\to\infty} \tilde{M}(R, L)/L = (p_d - p_c)/p_c$, and thus the right-hand side of (9) converges to zero as L goes to infinity, which implies $\lim_{L\to\infty} \mathcal{P}_s(\sigma_r) = 0$. ■

Theorem 3 states that the efficiency loss due to selfishness can be made arbitrarily small when there is an "asymptotically perfect" statistical test in that the probabilities of errors vanish as more signals are accumulated. In Section IV, we will propose and analyze such a statistical test. However, we should emphasize that the vanishing condition on the probabilities of the statistical test R in Theorem 3 is **sufficient** condition only. Thus, the result on arbitrarily small PoS of DP protocols may also hold for tests that are not asymptotically perfect.

We conclude this section with a couple of remarks. First, the constructed DP protocols are DP against multiple nodes deviating to σ^d because the gain from deviation decreases with the number of deviating nodes. Hence, if a protocol can deter a single node from deviating to σ^d, it can also deter multiple nodes from doing so. Second, the constructed DP protocols are DP against a more general class of deviation strategies with which a deviation to p_d starts in an arbitrary slot (determined deterministically or randomly). This is because we do not consider discounting in the payoff of the repeated game.

IV. Defection-proof Protocols Based on the ACK Ratio Test

A. Description of the Statistical Test

We consider the signal structure using ACK signals as discussed in Section II.B. We propose a particular statistical test called the ACK ratio test. The test statistic is the ratio of the total number of ACK signals to the length of a review phase, i.e., $\sum_{k=1}^{L} \chi_{\{z_i^k = S\}}/L$, where χ is an indicator function and $(z_i^1, \ldots, z_i^L)$ are the signals that node i collected in a review phase. The test is passed if the statistic exceeds a threshold value, $p-\epsilon$, where $p = p_c(1-p_c)^{N-1}$ and $\epsilon \in (0, p)$, and fails otherwise. Note that p is the expected value of the ACK ratio when every node transmits with probability p_c. If there is a deviating node, the ACK ratio tends to be smaller because its expected value is reduced to $\tilde{p} \triangleq p_c(1-p_c)^{N-2}(1-p_d)$. The ACK ratio test is designed to differentiate these two events while having ϵ as a "margin of error." Since the ACK ratio test can be identified with ϵ, we use ϵ instead of R to represent the ACK ratio test.

B. Analytical Results

Let $F(y; n, p)$ be the cumulative distribution function of a binomial random variable with total number of trials n and probability of success p, i.e.,

$$F(y; n, p) = \sum_{m=0}^{\lfloor y \rfloor} \binom{n}{m} p^m (1-p)^{n-m},$$

where $\lfloor \cdot \rfloor$ denotes the floor function. Suppose that every node transmits with probability p_c in a review phase. Then the number of ACK signals that a node receives in the review phase follows a binomial distribution with parameters L and p. Thus, the probability that a punishment is triggered by node i is given by

$$Pr\left\{ \sum_{k=1}^{L} \chi_{\{z_i^k = S\}}/L \leq p - \epsilon \right\} = F(L(p-\epsilon); L, p),$$

and the false punishment probability is given by

$$P_f(\epsilon, L) = 1 - [1 - F(L(p-\epsilon); L, p)]^N.$$

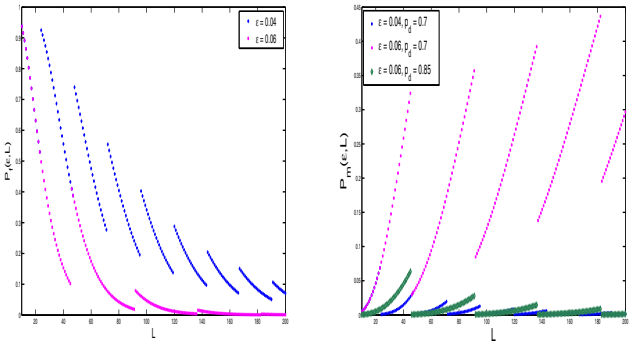
Suppose that there is exactly one deviating node transmitting with probability p_d in a review phase. Then, the success probability in a binomial distribution changes to $\tilde{p}$, and thus the miss detection probability is given by

$$P_m(\epsilon, L) = [1 - F(L(p-\epsilon); L, \tilde{p})]^{N-1}. \quad (10)$$

The following lemma regards the monotonicity of P_f and P_m w.r.t. the statistical test parameter ϵ.

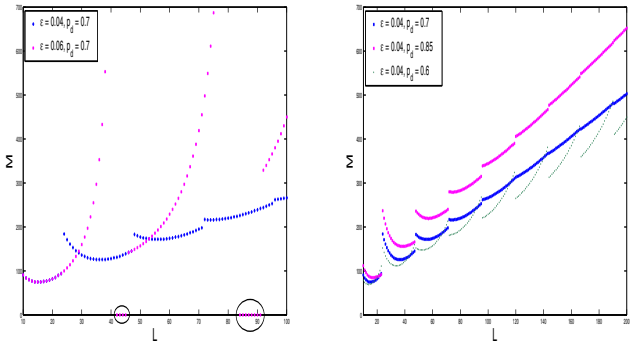
Lemma 1: Given $p_c \in (0, 1)$, $p_d \in (p_c, 1]$, and L, $P_f(\epsilon, L)$ and $P_m(\epsilon, L)$ are non-increasing and non-decreasing as $\epsilon \in (0, p)$ increases, respectively.

Proof: The proof is straightforward by noting that $F(L(p-\epsilon); L, p)$ and $F(L(p-\epsilon); L, \tilde{p})$ is non-increasing with ϵ, $0 < \epsilon < p$. ■



(a) (b)

Fig. 1: $P_f(\epsilon, L)$ and $P_m(\epsilon, L)$ versus length of a review phase L.



(a) (b)

Fig. 2: The minimum length of a reciprocation phase $\lceil \tilde{M}(R, L) \rceil$ versus length of a review phase L.

The next lemma examines the asymptotic properties of P_f and P_m as L becomes large.

Lemma 2: Given $p_c \in (0, 1)$ and $p_d \in (p_c, 1]$, $\lim_{L\to\infty} P_f(\epsilon, L) = 0$ for all $\epsilon \in (0, p)$ and $\lim_{L\to\infty} P_m(\epsilon, L) = 0$ for all $\epsilon \in (0, p - \tilde{p})$. Moreover, $\lim_{L\to\infty} P_m(\epsilon, L) = 1$ for all $\epsilon \in (p - \tilde{p}, p)$.

Proof: We use the normal approximation of a binomial distribution and apply the strong law of large numbers [16]. When every node transmits with probability p_c, the ACK ratio converges almost surely to p as L goes to infinity, which implies that the false punishment probability goes to zero for all $\epsilon > 0$. When there is exactly one node transmitting with probability p_d, the ACK ratio of a node transmitting with probability p_c converges almost surely to $\tilde{p}$ as L goes to infinity. Hence, if $\tilde{p} < p - \epsilon$, the miss detection probability goes to zero. ■

Lemma 2 gives a sufficient condition on the ACK ratio test to apply the results of Theorem 3.

Theorem 4: Let $p_c = 1/N$. If $\epsilon \in (0, p - \tilde{p})$, then for any $\delta > 0$, there exist L and M such that $\sigma_r(\epsilon, L, M)$ is DP against σ^d and $\mathcal{P}_s(\sigma_r) < \delta$.

Proof: Theorem 4 follows from Lemma 2 and Theorem 3. ■

Theorem 4 states that for given $p_c = 1/N$ and p_d, we can make the ACK ratio test based protocol σ_r be DP against σ^d and achieve an arbitrarily small PoS by choosing ϵ such that $0 < \epsilon < p - \tilde{p} = p_c(1 - p_c)^{N-2}(p_d - p_c)$. Note that as p_d is larger, it is easier to detect a deviation, and thus we have a wider range of ϵ that renders defection-proofness.

C. Numerical Results

As an example, we consider a network with 5 nodes (i.e., $N = 5$) and fix $p_c = 1/N = 0.2$.

Fig. 1 plots the false punishment probability $P_f(\epsilon, L)$ and the miss detection probability $P_m(\epsilon, L)$ as the length of a review phase L varies. Fig. 1(a) shows that $P_f(\epsilon, L)$ exhibits a decreasing tendency as L increases, with discontinuities occurring at the points where the floor function of $L(p-\epsilon)$ has a jump. Moreover, P_f is smaller for larger ϵ which confirms Lemma 1.

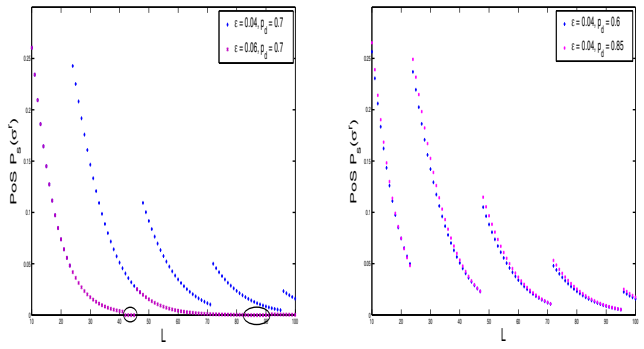
The upper threshold for the parameter ϵ in Lemma 2 is $p - \tilde{p} = 0.0512$ for $p_d = 0.7$. We can see that when ϵ is smaller than this threshold, $P_m(\epsilon, L)$ tends to decrease with L and approaches 0 for large L as shown in Fig. 1(b). Otherwise, $P_m(\epsilon, L)$ tends to increase and converges to 1. Also, for fixed ϵ, Fig. 1(b) shows that $P_m(\epsilon, L)$ is smaller for larger p_d, i.e., as the defection becomes greedier, the deviating node is more likely to get punished.

Fig. 2 plots the relationship between the length of a review phase L and the minimum length of a reciprocation phase $\lceil \tilde{M}(R, L) \rceil$ for different parameters ϵ and p_d.

In Fig. 2(a), we fix $p_d = 0.7$ and $\epsilon = 0.04, 0.06$. Since the vertical axis is truncated, some combinations of L and $\epsilon = 0.06$ result in (very) large values of M which are not shown, and $M = 0$ means that there exists no DP protocols for given ϵ, L, and p_d. For example, there exist no DP protocols for $42 \le L \le 45$ or $84 \le L \le 91$ when $\epsilon = 0.06$. We can see that when ϵ is small, there are more L values such that we can design DP protocols using the proposed ACK ratio test, i.e., $g(\epsilon, L) > 0$ is satisfied. Note that for small values of ϵ, both $P_f(\epsilon, L)$ and $P_m(\epsilon, L)$ tend to decrease as L increases which is a desirable property.

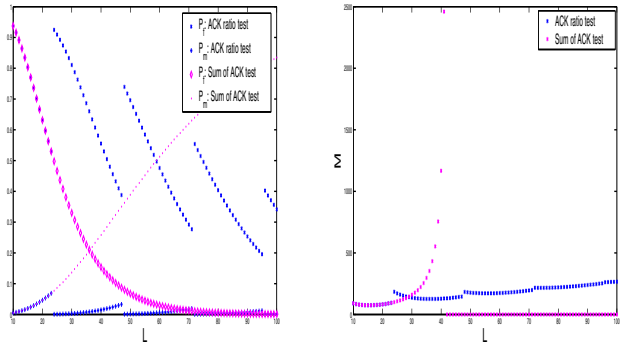
In Fig. 2(b), we fix $\epsilon = 0.04$ and vary the defection probability p_d. For the considered simulated values, we can observe that the minimum length of a reciprocation phase is larger for smaller values of p_d and some values L. Also, for some values of L, especially when L is small, shorter reciprocation phase is needed for longer review phase. However, in general, a longer review phase requires a longer reciprocation phase for fixed p_d.

Fig. 3 shows the PoS $\mathcal{P}_s(\sigma^r)$ versus the length of a review phase L of the defection-proof protocols with minimum length of reciprocation phase for different parameters ϵ and p_d. The points where the prices are shown as 0 in Fig. 3(a) are where no DP protocols exist for the given parameters. We can observe that as L increases, the PoS tends to decrease to 0, which is



(a) (b)

Fig. 3: PoS $P_s(\sigma^r)$ versus length of a review phase L.



(a) (b)

Fig. 4: Performance comparisons of σ^r and $\bar{\sigma}^r$.

consistent with Theorem 4. Fig. 3(a) shows that for a fixed $p_d = 0.7$, the PoS is much smaller for $\epsilon = 0.06$ than for $\epsilon = 0.04$. This is because the false alarm of the former case is smaller than of the latter case as shown in Fig. 1(a). Moreover, the PoS is almost the same for different defection probabilities p_d for fixed $\epsilon = 0.04$ as revealed in Fig. 3(b).

Next, to better understand the advantages (and disadvantages) of the proposed ACK ratio test, we study briefly the class of review strategies $\bar{\sigma}^r(\bar{R}, L, M)$ whose test $\bar{R}$ is based on the statistics of the sum of ACK signals for a node i. When playing $\bar{\sigma}^r$ and receiving less than k, $k \geq 1$, ACK signals in the review phase, a node punishes in the reciprocation phase. Otherwise, it continues to cooperate. We can derive analytical formulas for $P_f(\bar{R}, L)$ and $P_m(\bar{R}, L)$, but we omit here due to lack of space.

Fig. 4 shows comparative results for the protocols σ^r with $\epsilon = 0.04$ and $\bar{\sigma}^r$ with $k = 1$ for $p_d = 0.7$. When $k = 1$, it can be observed that the implementation complexity of $\bar{\sigma}^r$ is less than that of σ^r, except when $0 < L(p - \epsilon) \leq 1$. It can be seen (and shown analytically) that $P_f(\bar{R}, L)$ smoothly decreases to 0 while $P_m(\bar{R}, L)$ increases to 1 as L increases and becomes large. Moreover, for some values L, $\bar{\sigma}_r$ performs 'better' than σ_r in the sense that shorter reciprocation phase is needed for the same length of review phase. However, for larger values of L, $\bar{\sigma}_r$ has much longer reciprocation phase. Furthermore, when $L \geq 42$, there do not exist DP $\bar{\sigma}_r$ protocols. So, the results of Theorem 3 do not hold for review strategies employing the test $\bar{R}$ with $k = 1$.

V. Conclusion

The decentralized operation of Aloha systems with selfish nodes often leads to inefficient use of resources. In order to overcome this problem, we have designed Aloha-type protocols that are defection-proof against a certain type of deviations and have analyzed their performance. The design is based on a statistical test performed periodically and potential punishment triggered conditional on the result of the statistical test. In the proposed protocols, nodes statistically decide in an independent manner whether deviations took place in the system and, if necessary, impose punishments. Our design methodology to construct defection-proof protocols can be applied in other multi-user communication or networking interactions with private monitoring.

References

[1] L. G. Roberts, "Aloha packet system with and without slots and capture," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 5, no. 2, pp. 28–42, Apr. 1975.

[2] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535–547, Mar. 2000.

[3] E. Altman, R. El Azouzi, and T. Jiménez, "Slotted Aloha as a game with partial information," *Comput. Networks*, vol. 45, no. 6, pp. 701–713, Aug. 2004.

[4] R. T. Ma, V. Misra, and D. Rubenstein, "An analysis of generalized slotted-Aloha protocols," *IEEE/ACM Trans. Netw.*, vol. 17, no. 3, pp. 936–949, Jun. 2009.

[5] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux, "On selfish behavior in CSMA/CA networks," in *Proc. IEEE Infocom*, Miami, FL, 2005.

[6] Y. Jin, and G. Kesidis, "A pricing strategy for an Aloha network of heterogeneous users with inelastic bandwidth requirements," in *Proc. Conf. on Information Sciences and Systems (CISS)*, New Jersey, USA, Mar. 2002.

[7] J. Park and M. van der Schaar, "Stackelberg contention games in multiuser networks," *EURASIP J. Advances Signal Process.*, vol. 2009, Article ID 305978, 15 pages, 2009.

[8] E. Altman, N. Bonneau, and M. Debbah, "Correlated equilibrium in access control for wireless communications," *Lecture Notes in Computer Science*, pp. 173–183, Apr. 2006.

[9] G. Mailath and L. Samuelson, *Repeated Games and Reputations: Long-run Relationships*. Oxford, U.K.: Oxford Univ. Press, 2006.

[10] R. Radner, "Repeated principal-agent games with discounting," *Econometrica*, vol. 53, no. 5, pp. 1173–1198, Sep. 1985.

[11] O. Gossner, "The Folk theorem for finitely repeated games with mixed strategies," *Int. J. Game Theory*, vol. 24, no. 1, pp. 95–107, Mar. 1995.

[12] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, "Repeated open spectrum sharing game with cheat-proof strategies," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1922–1933, Apr. 2009.

[13] R. J. La and V. Anantharam, "Optimal routing control: repeated game approach," *IEEE Trans. Autom. Control*, vol. 47, no. 3, pp. 437–450, Mar. 2002.

[14] M. Kandori, "Introduction to repeated games with private monitoring," *J. Econ. Theory*, vol. 102, no. 1, pp. 1–15, Jan. 2002.

[15] J. L. Massey and P. Mathys, "The collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 31, no. 2, pp. 192–204, Mar. 1985.

[16] P. Billingsley, *Probability and Measure*. New York: Wiley, 1995.