Cooperation in Wireless Networks with Unreliable Channels

Wenjing Wang, Mainak Chatterjee, and Kevin Kwiat

***Abstract*—In a distributed wireless system, multiple network nodes behave cooperatively towards a common goal. An important challenge in such a scenario is to attain mutual cooperation. This paper provides a non-cooperative game theoretic solution to enforce cooperation in wireless networks in the presence of channel noise. We focus on one-hop information exchange and model the packet forwarding process as a hidden action game with imperfect private monitoring. We propose a state machine based strategy to reach Nash Equilibrium. The equilibrium is proved to be a sequential one with carefully designed system parameters. Furthermore, we extend our discussion to a general wireless network scenario by considering how cooperation can prevail over collusion using evolutionary game theory. The simulation results are provided to back our analysis. In particular, network throughput performance is measured with respect to parameters like channel loss probability, route hop count, and mobility. Results suggest that the performance due to our proposed strategy is in close agreement with that of unconditionally cooperative nodes. Simulation results also reveal how the convergence of cooperation enforcement is affected by initial population share and channel unreliability.**

***Index Terms*—Wireless networks, cooperation enforcement, evolutionary game theory, sequential equilibrium, imperfect observation, collusion resistance.**

I. Introduction

In a distributed wireless system where multiple network entities (also called nodes) work towards individual or common goals, cooperative behavior among the nodes (such as controlling the transmit power level, reducing interference for each other, revealing private information, adhering to network policies) is highly desired for increasing system capacity. For example, when data transfer is required between any pair of non-adjacent nodes, the node pair *relies* on the nodes between them to relay the data packets. However, this assumption may be too strong in some scenarios when nodes do not belong to the same authority or work towards different goals [2], [3], [22], [27]. As a result, nodes may prefer not to participate in packet forwarding, since the notion of cooperation might not be rational to them. Therefore, in order to ensure proper functioning of the network, it is important to stimulate or enforce cooperation among the nodes.

Over the past years, mechanisms have been devised that either stimulate nodes to forward each others' packets [7], [9], [11] or punish nodes for misbehaving [4], [8], [21], [27]. Majority of the proposed methods can be broadly categorized into two types: incentive-based [10], [12], [28] and reputation-based [15], [23], [24]. Most incentive-based protocols assume the network with rational nodes/agents and adopt the concept of virtual currency (e.g., "nuglets") [9] which is a method to reward nodes participating in packet forwarding. It has been well established that pricing schemes (in terms of reward and penalty) [3], [12] and security of payment systems [10], [11] are closely associated with the incentive-based approaches. On the contrary, in a reputation-based system, a node's behavior is monitored and measured by its neighbors. Based on the observed past behaviors, a node receives a certain level of service or gets isolated for being non-cooperative [8], [21]. An example of reputation-based scheme is CORE [23], where each node maintains a reputation table for the other nodes. The reputation value is updated based on the node's own observations and the information provided by the other nodes.

Meanwhile, there have been some interesting developments that use game theory to analyze how cooperation can be achieved [13], [24], [28], [32]. In [13], Félegyházi *et al.* formally define the packet forwarding game in ad hoc networks and derive the conditions under which cooperation yields Nash Equilibrium. Michiardi *et al.* apply game theory in [24] to analyze several strategies in the repeated prisoner's dilemma. They also show that in order to foster coalition among cooperative nodes, enough incentives should be granted. Zhong *et al.* [32] show that there is no dominant strategy in a forwarding subgame and cryptographic techniques can be employed for the required tamper-proof hardware support. A more general framework on cooperation in ad hoc networks is presented in [28], where Srinivasan *et al.* focus on the energy efficiency through cooperation.

However, the aforementioned efforts are not sufficient to completely understand and model cooperation in wireless network in the presence of noise. The noisy nature of the wireless channels makes the analysis very challenging. More recent work [15], [16], [25], [29], [31] confirm that the effect of noise makes the observation *imperfect*. In [15], Jaramillo *et al.* propose a distributed reputation monitoring based strategy to enforce cooperation when the channel is lossy. Their strategy is proved to be subgame perfect even if the channel estimation is not accurate. Non-cooperative game theory has been used

Paper approved by M. Chiang, the Editor for Optimization and Games in Networks of the IEEE Communications Society. Manuscript received February 12, 2010; revised October 9, 2010 and January 25, 2011.

W. Wang and M. Chatterjee are with department of EECS, University of Central Florida, Orlando, FL (e-mail: {wenjing, mainak}@eecs.ucf.edu).

K. Kwiat is with the Air Force Research Laboratory, Rome, NY (e-mail: kevin.kwiat@rl.af.mil).

A preliminary version of this manuscript appeared in the 6th IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2009.

This research was supported by the Air Force Office of Scientific Research (AFOSR) under the federal grant no. FA9550-07-1-0023, and the National Science Foundation under award no. CCF-0950342. Approved for Public Release; Distribution Unlimited: 88ABW-2011-0555 dated 15 February 2011.

Digital Object Identifier 10.1109/TCOMM.2011.081111.100085

to enforce cooperation when channel collision exists [25], [29]. In [31], statistical methods are used to filter noise from observation so that attacks can be identified. Ji *et al.* [16] calculate the belief of nodes on others' actions and propose a belief-based multi-node multihop packet forwarding scheme. Li *et al.* [20] further generalize noise and imperfect monitoring as hidden information and hidden action games, and study truthful routing issues from a mechanism design perspective. Related investigations are also shown by Feldman *et al.* in [14].

The research presented in this paper addresses the problem of cooperation enforcement with noisy channel. Although our research is inspired by [15] and [16], our modeling and methodology are quite different from existing work and should not be considered as a simple variant. In [15], the implicit assumptions are that the channels and environment are identical around the receiver and the observer, so that the sender can observe the forwarding actions directly. However, in our model, we do not assume the channels to be identical. [16] proposes a viable way to achieve equilibrium based on beliefs. In their approach, a complex belief model is employed which requires the nodes to calculate their beliefs about what actions the opponents have taken. However, as the game evolves, the computation complexity of updating beliefs is high. Furthermore, the difficulties in hidden action game with imperfect private monitoring games are generally two-fold. First, when the noisy channel makes action history unknown to the public, the games do not possess the recursive structure on the equilibrium [1]. Second, players (nodes) are not sure about what the opponents are going to do because they cannot perfectly monitor their actions. In that case, a player must take the best strategy based on her belief about her opponents' actions at every move, which is the essence of the strategies proposed in [16]. The first difficulty implies that the modeling and analysis of node interactions should apply the theory of dynamic games, while the second difficulty demands an effective and efficient approach to achieve equilibrium. This research is motivated by the aforementioned challenges, and we attempt to find a less complex alternative approach to enforce cooperation in unreliable wireless networks.

Our main focus in this research stems from the state-of-the-art advances in game theory on repeated games under private monitoring and strategies [6], [17], [18]. We focus on one-hop information exchange in a wireless network setting and model the non-cooperative packet forwarding game in the presence of noise. We show that although nodes' actions are hidden due to the channel, they can nevertheless monitor their own payoffs. Based on the private observation of their payoffs, we construct a forwarding approach using a two-state machine. We demonstrate that careful design of the state transition parameters achieves *sequential equilibria* that enforces cooperation. Furthermore, to address how to enforce cooperation when collusion exists, we focus on the collusion resistance using both repeated and evolutionary games. Our findings indicate that a subgame perfect cooperation enforcement strategy ensures cooperation as a prevailing action if the strategy is evolutionary stable or the initial non-cooperative population is bounded.

The main contributions in this paper can be summarized as follows.

- We model the packet forwarding process with channel noise as a hidden action game with imperfect monitoring and propose a strategy profile for the game. The strategy is shown to give a sequential equilibrium solution. Extensive simulations show that the cooperation enforcement strategy is more efficient (Pareto superior) over non-cooperative ones.
- We adopt evolutionary game theory in capturing the population dynamics. Analysis indicates that if nodes are patient enough and value future payoffs, collusion resistance and cooperation enforcement are equivalent.

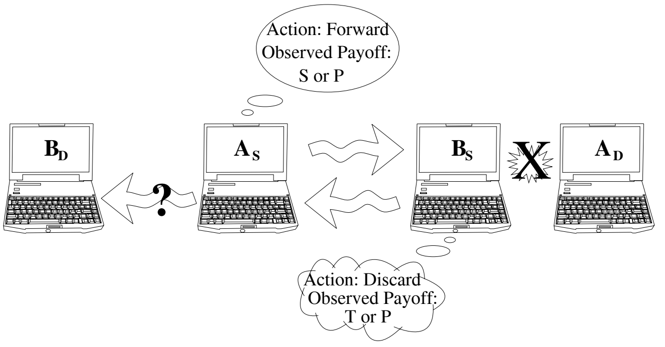

Fig. 1. Two player packet forwarding game model.

The rest of the paper is organized as follows. In Section II, we introduce the packet forwarding game considering noise. In Section III, we explain how to build a strategy profile with a two-state machine and analyze its equilibrium properties. In Section IV, we use evolutionary game theory to show how cooperation can be enforced despite collusion. Section V provides the simulation model and results to illustrate the properties of the proposed strategies as well as our analysis. The last section concludes the paper.

II. The Packet Forwarding Game under Noise

We begin our analysis with a review of the classical two-player packet forwarding problem [13], [15]. As shown in Figure 1, we consider two data sessions: (i) A_S to A_D through B_S and (ii) B_S to B_D through A_S. If the channel is perfect (loss free), based on the actions A_S and B_S take, they will obtain different payoffs as listed in Table I. The entries in the matrix, i.e., R, S, T, P, not only determine the payoffs players can obtain, but also indicate the type of the game. For example, the well-known Prisoner's Dilemma [26] characterizes the scenario of packet forwarding when $T > R > P > S$. It is noted that, depending on how the system is configured, the values in the matrix might be different. In this research, instead of using a specific payoff matrix, we assume the matrix has a general form as shown in Table I. Later, we will show how the values in the matrix affect the equilibrium properties of our strategy. Given the payoff matrix, it is clear that for an action $\boldsymbol{a} = (a_{A_S}, a_{B_S}) = (Forward, Discard)$, the payoff vector would definitely be $\boldsymbol{u} = (u_{A_S}, u_{B_S}) = (S, T)$.

However, when we bring in the channel loss, even if both nodes take the same action as above, the payoff vector is not likely to remain the same. For node A_S, it forwards B_S's

TABLE I
PAYOFF MATRIX OF TWO PLAYER PACKET FORWARDING GAME. R=REWARD, S=SUCKER, T=TEMPTATION, P=PENALTY.

		Node A_S			
		Forward		Discard	
Node B_S	Forward	R	R	S	T
	Discard	T	S	P	P

TABLE II
PAYOFF PROBABILITIES FOR GIVEN ACTION PROFILES. F=FORWARD, D=DISCARD.

		Node i's payoffs			
		R	S	T	P
Actions	(F, F)	$(1-p_e)^2$	$p_e(1-p_e)$	$p_e(1-p_e)$	p_e^2
	(D, F)	0	0	$1-p_e$	p_e
	(F, D)	0	$1-p_e$	0	p_e
	(D, D)	0	0	0	1

packet to B_D, but the forwarding action might fail due to the channel noise, and B_D does not receive the packet. Since B_S's payoff is determined by whether B_D receives the packet, from node B_S's perspective, A_S is playing *Discard* even though its action was *Forward*. Thus, the payoff vector now is $\boldsymbol{u} = (P, P)$. Nonetheless, node B_S cannot directly observe A_S's action. This is because what B_S can observe relies only on the channel between it and A_S and this channel is different from that between A_S and B_D due to interference. Also, we do not assume that B_D can, through some mechanism, inform B_S about whether the packet is received or not. Hence, what the nodes can do is to monitor their own payoffs (*realized payoff*), and indirectly, form a *belief* on what others have done. Based on the same payoff matrix in Table I, if the noise is presented as a channel loss probability p_e,[1] we can calculate the probabilities associated with actions and payoffs. In Table II, we list the probabilities as node i plays the first action and its opponent plays the second action in the action profiles. With these probabilities, we can further calculate the expected payoff of a node. For example, when $\boldsymbol{a} = (Forward, Discard)$, the expected payoff vector is $\boldsymbol{u} = ((1-p_e)S + p_e P, (1-p_e)T + p_e P)$.

Let us now formally define the packet forwarding game under noise.

DEFINITION 1: A *packet forwarding game* (Γ) *under noise* is a quadruple (I, A, Ω, u), where

- $I = 1, 2, ..., n$ denotes the set of nodes.
- A is a space of actions (a_i) a node (i) can take.
- Ω is a space of observed signals. For every action $a_i \in A_i$ node i takes, it observes a signal $\omega_i \in \Omega_i$. Both action a_i and signal ω_i are node i's private information. The probability distribution of private signal $\omega = (\omega_1, ..., \omega_n)$ depends on the action profile $a = (a_1, ..., a_n)$ and the noise in the channel. It is denoted as $p(\omega|a)$.
- u presents the realized payoffs. For node i, its expected payoff is given by $g_i(a) = \Sigma_\omega p(\omega|a) u_i(a_i, \omega_i)$.

Often times, this game is played repeatedly as nodes have a number of packets to be forwarded. From a discounted repeated game [26] perspective, the discounted payoff for node i is $U_i = \Sigma_{t=0}^{\infty} \delta^t g_i(a(t))$, where $a(t)$ is the action taken at time t and $\delta \in (0, 1)$ is the discount factor. The discount factor infers the preference of time or patience. A large δ shows a node's patience in the game and good valuation of payoffs it gets in future stages, while a small δ means that the node is more eager for immediate payoffs and has higher probability of leaving the game after each stage.

The above definition differs from most existing game models in the sense that a node cannot directly observe others' actions, rather, it observes through a *private* signal[2] associated with the action profiles played. As a matter fact, existing models can be regarded as a special case when $\omega = a$ for all nodes (all nodes have perfect public observation of others' actions), or $\omega_1 = \omega_2 = ... = \omega_n \neq a$ (all nodes have imperfect public observation of others' actions). While the existing models either ignore the noisy nature of the wireless channel or need some sort of communications among nodes to exchange the observations, our model eliminates such pre-assumptions and hence most appropriately abstracts an wireless network scenario.

The outcome of a single stage (static) game can be characterized by the well-known *Nash Equilibrium* [26]. In a Nash equilibrium, no player can unilaterally deviate from the equilibrium strategy to gain more payoff; or in other words, every player is playing the best response to others. When the same game is played repeatedly for finite or infinite number of times, the notion of *subgame* is used so that the game can be viewed as a subset of the original game starting at a certain stage, with perfectly or imperfectly monitored history. The repeated game can be analyzed by finding the *Subgame-Perfect Nash Equilibrium* (SPNE), which consists of a series of Nash Equilibria at every subgame of the original game [26]. From our modeling of the packet forwarding game, in order for each node to make best response to others' actions that are hidden, a node first needs to form a belief on what the others have done. A profile of strategies and beliefs makes an *assessment*. To further refine the SPNE given the assessment, *sequential equilibrium* [19] is introduced.

DEFINITION 2: Sequential Equilibrium[3] is an assessment of strategy π and belief μ, which satisfies the following properties:

- *Strategy Sensibility*: When the beliefs are fixed, no player prefers at any point to change her part of strategy in π given the information set, i.e., π maximizes the expected payoffs.
- *Belief Sensibility*: Those information sets can be reached with positive probabilities (μ) given π.
- *Consistency*: The assessment should be a limit point of a sequence of the mixed strategies and associated sensible beliefs, i.e., $(\pi, \mu) = \lim_{n\to\infty}(\pi_n, \mu_n)$.

Thus, in order to enforce cooperation in wireless networks with noisy channel, it is highly desirable that any adopted

[1] It is noted here that our assumption of non-identical channel is not comprised, because the channel between A_S and B_S can have different lossy properties, so that direct observation of actions is impossible.

[2] It is noted that the signal here does not necessarily mean the physical signal in the communication channel, but rather, it refers to all the possible observations a node can make, e.g., the payoffs.

[3] Please refer to [19] for a more formal definition.

strategies and their associated beliefs constitute the sequential equilibrium. Also, this sequential equilibrium is attainable by carefully designing the parameters that aid the calculation of the beliefs. To further clarify the concept of sequential equilibrium in the packet forwarding game, we assume that although nodes cannot perfectly observe the actions of others, they have beliefs about what the opponents have done. Based on the beliefs, they take corresponding actions in future games. The sequential equilibrium requires that the nodes form their beliefs in such a way (e.g., following Bayesian rules) that the states associated with the beliefs can be reached with positive probabilities. In addition, the consequent actions taken given the beliefs are the best response to the current state. A possible solution to attain the equilibrium is proposed in [16], where one node plays the Grim Trigger strategy and the other one plays the defection strategy, and the beliefs are updated at every stage of the game. However, the belief-based approach requires extensive computations, and moreover, their modeling on the effect of the channel is not thoroughly investigated, as the *Discard* action can never be observed as *Forward*. Our goal is to design a more efficient way to attain sequential equilibrium under the noisy channel. Our approach is different from [16] in both design notion and methodology.

III. STATE MACHINE BASED FORWARDING

In this section, we demonstrate how to construct a sequential equilibrium using state machine based forwarding. It is noted that a larger space of other cooperation enforcement strategies, as well as the associated equilibria with noisy channels have been analyzed in [25], [29]. For the sake of clarity, we consider the packet forwarding game between two nodes. The payoff matrix is shown in Table I, where the parameters follow the basic configuration of Prisoner's Dilemma, i.e., $T > R > P > S$.

First, we define two types of observable signals ω: *Punishment* signal and *Reward* signal. We define that a *Punishment* signal is observed when the node's realized payoff is P, otherwise a *Reward* signal is observed. It is noted that a punishment signal can be observed even if node is playing cooperatively. Table II can be used to calculate $p(\omega|a)$ given the action profiles. However, the observations are private.

Further, let us consider a strategy with two states, C (Cooperative) and N (Non-Cooperative). The strategy begins with state C and operates with the following transition probabilities.

- When the node is in State C, play $Discard$ with a small probability q_C. If $Discard$ is taken and *Punishment* is observed, transit to N with probability ρ_C. Stay in C, otherwise.
- When the node is in State N, play $Discard$ with a large probability q_N. If $Discard$ is taken and *Reward* is observed, transit to C with probability ρ_N. Stay in N, otherwise.

The state machine based forwarding approach is illustrated in Figure 2. In this approach, there is always an uncertainty about the state the opponent node is in, and hence the beliefs are updated all the time. In order for this design to reach sequential equilibria, it is important that, with any history, the state machine is a best response to itself, regardless of the beliefs. In other words, the problem is to find whether there is a set of the system parameters (transition probabilities), such that node i does not gain different payoffs by choosing either actions, i.e., *Forward* (*F*) or *Discard* (*D*), no matter what state its opponent node $-i$ is in.

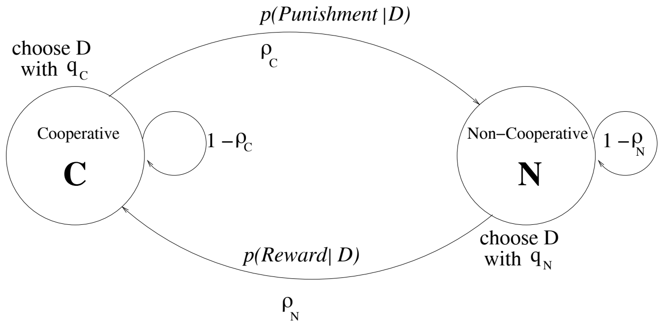

Fig. 2. Forwarding state machine.

The design problem is hence reduced to finding the system parameters (q_C, q_N, ρ_C, ρ_N) that make the strategy itself a best response to the state machine. We denote V_C and V_N as the average repeated game payoffs for node i when node $-i$ is in state C and N respectively. From Bellman equations [5], we can write the following equations.

When node i plays F,

$$V_C = (1-\delta)[(1-q_C)R + q_C S] + \delta[(1-q_C p_e \rho_C)V_C + q_C p_e \rho_C V_N] \tag{1}$$

$$V_N = (1-\delta)[(1-q_N)R + q_N S] + \delta\{(1-p_e)\rho_N q_N V_C + [1-(1-p_e)\rho_N q_N]V_N\} \tag{2}$$

Similarly, if node i plays D,

$$V_C = (1-\delta)[(1-q_C)T + q_C P] + \delta[(1-q_C\rho_C)V_C + q_C\rho_C V_N] \tag{3}$$

$$V_N = (1-\delta)[(1-q_N)T + q_N P] + \delta V_N \tag{4}$$

For node i to be indifferent between F and D, equations (1) and (3) should be equal when node $-i$ is in state C, or equations (2) and (4) should be equal when node $-i$ is in state N. Thus, the solutions for above equations represent the equilibria of the state machine. The following theorem provides one of the solutions.

THEOREM 1: *For the state machine based forwarding approach, there is a sequential equilibrium for large* δ, *when* $p_e < \frac{R-P}{T-P}$ *and* $T > R$.

Proof: From equations (1) and (3) we have

$$(1-\delta)[(1-q_C)(T-R)+\rho_C(P-S)] = \delta q_C \rho_C (1-p_e)(V_C - V_N) \tag{5}$$

Thus, from equation (1), we can further derive

$$V_C = (1-q_C)R + q_C S + \frac{p_e}{1-p_e}[(1-q_C)(R-T) + q_C(S-P)] \tag{6}$$

Similarly, from equations (2) and (4) we have

$$(1-\delta)[(1-q_N)(T-R)+\rho_N(P-S)] = \delta q_N \rho_N (1-p_e)(V_C - V_N) \tag{7}$$

and

$$V_N = (1 - q_N)T + q_N P \tag{8}$$

From the observation of equations (5)-(8), we are left with four variables and two equations, which implies there are two free variables. To find a possible solution to the equations, we consider ρ_C as a free variable and set $\rho_C = 1$. The reasoning is as follows. If there is a solution of the above equations with $\rho_C < 1$, we can always decrease q_C in equation (6) to increase V_C as long as the following condition is met.

$$p_e < \frac{R - S}{T - P} \tag{9}$$

However, this will lead to further increasing ρ_C to balance equation (5). Thus, ρ_C can be increased to 1 but never exceed 1 as it is a probability. For the variables in equations (7) and (8) we let $q_N = 1$, which will further reduces the analysis above as[4]

$$V_N = P \tag{10}$$

and

$$\rho_N = \frac{q_C(P - S)}{(1 - q_C)(T - R) + q_C(P - S)}. \tag{11}$$

It is not hard to see that $\rho_N \in [0, 1]$. Therefore $q_N = 1$ is a valid setting.

Putting equations (11) and (6) back to equation (7), we obtain a quadratic equation of q_C as

$$\begin{aligned}
&\{\delta(1 - p_e)[R - S - \frac{p_e}{1 - p_e}(T - R + S - P)]\}q_C^2 \\
&+\{\delta(1 - p_e)[P - R - \frac{p_e}{1 - p_e}(T - R)] \\
&+(1 - \delta)(P - S - T + R)\}q_C + (1 - \delta)(T - R) = 0(12)
\end{aligned}$$

It is easy to see that one root of equation (12) is $q_C = 0$ when $\delta = 1$. To find the relationship between q_C and δ, we check the existence of implicit function (F) around (q_C, δ)=(0, 1) as

$$\frac{\partial F}{\partial q_C}|_{(q_C,\delta)=(0,1)} = (1 - p_e)[P - R - \frac{p_e}{1 - p_e}(T - R)]. \tag{13}$$

Since $p_e < \frac{R-P}{T-P}$, equation (13)$\neq$ 0, and thus the Implicit Function Theorem can be applied around $\delta = 1$ such that

$$\begin{aligned}
\frac{dq_C}{d\delta} &= -\frac{\frac{\partial F}{\partial \delta}|_{(q_C,\delta)=(0,1)}}{\frac{\partial F}{\partial q_C}|_{(q_C,\delta)=(0,1)}} \\
&= \frac{T - R}{(1 - p_e)[P - R - \frac{p_e}{1-p_e}(T - R)]}
\end{aligned} \tag{14}$$

From the assumptions, we know that equation (14)$<$ 0, which essentially states that there exists a value $q_C \in (0, 1)$, for a large enough δ such that $q_C \to 0$ as $\delta \to 1$. Hence, a set of parameters satisfying the system requirement is obtained around $\delta = 1$.

Further, with the set of parameters, the average payoff is updated as

$$\begin{aligned}
V_C &= \lim_{q_C \to 0}\{(1 - q_C)R + q_C S \\
&\quad + \frac{p_e}{1 - p_e}[(1 - q_C)(R - T) + q_C(S - P)]\} \\
&= R + \frac{p_e}{1 - p_e}(R - T) > P.
\end{aligned} \tag{15}$$

Thus, state C is always more efficient than state N. In addition, when the nodes are updating their beliefs on the opponent, it will always assume that the opponent has never deviated because no deviation is observable. The consistency requirement is satisfied as neither node tries to update its beliefs about others; instead, the nodes play the best response strategies. Hence, we have proved that the state machine based forwarding approach has a sequential equilibrium for large δ, when $p_e < \frac{R-P}{T-P}$ and $T > R$. ■

In the proof, we showed that with the system parameters (state transition probabilities) in [0,1], q_C can be arbitrarily close to 0 as δ goes to 1; and the cooperative state is always strictly Pareto superior to the non-cooperative state. Moreover, the average payoff of the cooperative state is arbitrarily close to $R - \frac{p_e}{1-p_e}(T - R)$.

By further manipulating the constraints in Theorem 1, we have the properties as follows.

COROLLARY 1: In order to reach sequential equilibrium, $R < T < \frac{1-p_e}{p_e}(R - P)$.

COROLLARY 2: In a sequential equilibrium, the average payoff of the cooperative state is lower bounded by P and upper bounded by $R - \frac{p_e}{1-p_e}(T - R)$.

Corollaries 1 and 2 infer that the values of the elements in the payoff matrix can help to reach the sequential equilibrium, and at the same time pushing the average payoff to the Pareto frontiers. In particular, we can find a small enough ϵ such that $T = R + \epsilon$ to relax the constraint on channel loss in Theorem 1.

COROLLARY 3: If $T = R + \epsilon$, when $\epsilon \to 0^+$, a sequential equilibrium can be reached regardless of the noise in the channel, and the average payoff of the cooperative state $V_C \to R$.

Proof: Since $T = R + \epsilon$, in Theorem 1, in order to reach sequential equilibrium $p_e < \frac{R-P}{T-P} = \frac{T-\epsilon-P}{T-P}$. Also, $\lim_{\epsilon\to 0^+} \frac{T-\epsilon-P}{T-P} = 1$. Since $p_e \in (0, 1)$, for $\epsilon \to 0^+$, it essentially relaxes the constraint on p_e; thus p_e can take any value in (0,1). From Corollary 1, $T < \frac{1-p_e}{p_e}(R - P)$, which derives $\frac{p_e}{1-p_e} < \frac{R-P}{R+\epsilon}$. Hence, $V_C(\epsilon) = \lim_{\epsilon\to 0^+} R - \frac{\epsilon(R-P)}{R+\epsilon} = R$. ■

IV. COLLUSION RESISTANCE AND COALITION FORMATION

Our discussion so far provides a method to enforce cooperation in a two player game, however, we are more interested in how cooperation can be enforced among *all* the nodes in the network. In this section, we analyze cooperation from the perspective of non-cooperative collusion. In particular, we address two aspects: (i) how to resist collusion among

[4] It is also correct to select ρ_N as the free variable, however, if we were to set $\rho_N = 1$, further analysis would have been much less elegant. The derived closed form expressions of the results will have limited implications.

nodes that deviate from the cooperation strategy, and (ii) how the population of cooperative nodes grows and cooperation prevails? We still consider the forwarding game, although the game now is played between a colluding node and a cooperative node.

A. Collusion Resistance

We consider nodes belonging to two different groups playing the packet forwarding game as defined in Definition 1. Based on what group a node belongs to, the strategies it plays are either colluding (s_c) or not colluding (s_a). Collusion is hence defined with the amount of utility derived from the games.

DEFINITION 3: Collusion is a group of players working together to maximize their own payoffs regardless of the social optimum. A strategy s^c is a colluding strategy if and only if

$$U_i(s^c, s^c) \geq U_i(s^a, s^c),$$

where U_i is the observed average discounted payoff for node i, s^a is any strategy other than s^c. It is called a *strict colluding strategy* if the inequality holds.

We consider a pure strategy profile s^* which is subgame perfect and enforce cooperation on the equilibrium point (e.g., our proposed state machine based forwarding). Let x_c be the population share of a strict colluding pure strategy profile s^c. The following lemma gives an upper bound on x_c.

LEMMA 1: A cooperation enforcement strategy s^* is collusion resistant if and only if

$$x_c < \frac{U_i(s^*, s^*) - U_i(s^c, s^*)}{U_i(s^c, s^c) + U_i(s^*, s^*) - U_i(s^c, s^*) - U_i(s^*, s^c)}. \tag{16}$$

Proof: We assume that the number of nodes in the game is n. For the group of cooperating nodes, the group's total payoff is

$$U^* = n(1 - x_c)U_i(s^*, s^*) + nx_cU_i(s^*, s^c). \tag{17}$$

The total payoff for the group of colluding nodes is

$$U^c = n(1 - x_c)U_i(s^c, s^*) + nx_cU_i(s^c, s^c). \tag{18}$$

Collusion resistance requires that $U^* > U^c$. Therefore, $x_c[U_i(s^*, s^c) - U_i(s^*, s^*) + U_i(s^c, s^*) - U_i(s^c, s^c)] > U_i(s^c, s^*) - U_i(s^*, s^*)$.
Since subgame perfect Nash equilibrium requires $U_i(s^*, s^*) \geq U_i(s^c, s^*)$ and strict colluding infers $U_i(s^c, s^c) > U_i(s^*, s^c)$, we get equation (16). ■

B. Coalition Formation

Lemma 1 shows that in order to resist collusion, the colluding node population should be kept under a threshold. However, when the games are played over time, the population of different groups (i.e., cooperative or colluding) is highly dynamic. We apply evolutionary game theory [30] in our following analysis to capture the dynamics on population.

DEFINITION 4: Let Δ be a strategy set, where strategies $s_x, s_y \in \Delta$. s_x is an *evolutionarily stable strategy* (ESS) if for every strategy $s_y \neq s_x$ there exists some $\bar{\epsilon}_y \in (0, 1)$ such that

$$u[s_x, \epsilon s_y + (1 - \epsilon)s_y] > u[s_y, \epsilon s_y + (1 - \epsilon)s_x]$$

for all $\epsilon \in (0, \bar{\epsilon}_y)$.

PROPOSITION 1: $\Delta^{ESS} = \{s_x \in \Delta^{NE} : u(s_x, s_y) > u(s_y, s_y),\ \forall\ s_y \in \beta(s_x), s_y \neq s_x\}$, where Δ^{NE} denotes the set of Nash Equilibrium strategies, and $\beta(s_x)$ is the set of best response strategies against s_x.
We consider the same s^* and assume it is ESS. We denote x_* as the population share of nodes adopting s^*, i.e., group of cooperative nodes. Obviously, $x_* + x_c = 1$.

According to evolution theory, one of the ways to characterize the population dynamics is through replicator. For the sake of the discussion, we assume the nodes in the network are smart enough to learn their payoffs and the dynamics for the population of x_* is given as

$$\dot{x}_* = [u(s^*, s^c) - u(s^c, s^c)]x_* \tag{19}$$

Let $\mathbf{M_a}$ represent the payoff matrix when s^* plays s^c.

$$\mathbf{M_a} = \begin{pmatrix} u(s^*, s^*) & u(s^*, s^c) \\ u(s^c, s^*) & u(s^c, s^c) \end{pmatrix}$$

This matrix also holds true for the player playing s^c. Applying $\mathbf{M_a}$ to equation (19), we get

$$\begin{aligned} \dot{x}_* &= [(u(s^*, s^*) - u(s^c, s^*))x_*x_c]x_* \\ &\quad +[(u(s^*, s^c) - u(s^c, s^c))x_*x_c]x_c \\ &= (a_1x_* - a_2x_c)x_*x_c \end{aligned} \tag{20}$$

where $a_1 = u(s^*, s^*) - u(s^c, s^*)$, $a_2 = u(s^c, s^c) - u(s^*, s^c)$.

LEMMA 2: The cooperation enforcement strategy s^* leads to +1 evolutionarily stable state on population share if and only if s^* is ESS or the initial population share $x_c^0 < a_1/(a_1 + a_2)$.

Proof: For any $x_* < 1$, the +1 state can only be reached if $\dot{x}_* > 0$. Since $x_c, x_* > 0$, it requires $a_1x_* - a_2x_c > 0$. If $a_1a_2 < 0$. The only possibility is $a_1 > 0,\ a_2 < 0$, and indicates s_* is ESS (Proposition 1). If $a_1a_2 > 0$. $x_c^0 < \frac{a_1}{a_1+a_2}$. ■

It can be noted that in case s^* is not ESS, $x_c^0 = \frac{a_1}{a_1+a_2}$ and $x_*^0 = \frac{a_2}{a_1+a_2}$ are the mixed strategy Nash Equilibrium values. It suggests that when no ESS exists, the strategy with the initial population greater than the equilibrium value prevails.

Summarizing the discussions above, we have the following theorem on a general cooperation enforcement strategy.

THEOREM 2: A cooperation enforcement strategy s^* enforces the prevalence of cooperation if and only if it satisfies either of the following two conditions:

- s^* is ESS,
- $x_c^0 < \min(\frac{U_i(s^*,s^*)-U_i(s^c,s^*)}{U_i(s^c,s^c)+U_i(s^*,s^*)-U_i(s^c,s^*)-U_i(s^*,s^c)}, \frac{a_1}{a_1+a_2})$.

Remarks: In the second condition, both terms in the minimization function are the same if $\delta = 1$ for the repeated game. It also suggests that when all the players in the game stick to continuous participation, the colluding nodes will be enforced to be cooperative with time. Thus collusion resistant is bona fide cooperation coalition formation. The sensitivity of the convergence of the formation (i.e., $\dot{x}_*$) will be determined by the payoff matrix entries.

V. Simulations and Evaluation

In this section, we evaluate our cooperation enforcement packet forwarding strategies through simulation. We also show how the dynamics of the population evolve and how collusion can be resisted in the forwarding games.

A. Simulation Setup

We consider 50 nodes that are randomly scattered in an area of $1000m \times 1000m$. The physical communication range is set to be $250m$. During the simulation, log-distance path loss with exponent of 3 is adopted as the propagation model, and IEEE 802.11 is the underlying MAC protocol with a bandwidth of 2 Mbps. In particular, we simulate CSMA/CA with exponential backoff where the contention window grows exponentially from a minimum value of 31. The unit slot time is 20 μs. DIFS and SIFS are 50 μs and 10 μs, respectively. The size of an ACK packet is 38 bytes. Each data packet size is 64 bytes and is generated as a constant bit rate (CBR) traffic with 2 packets per second, unless specially mentioned. We allow only one data session at a time. The data sessions originate and terminate at randomly selected source and destination nodes.

To simulate the repeated nature of the packet forwarding games, any node pair engaged in packet forwarding plays a number of games with respect to the discount factor δ defined as a system parameter. For a given δ, the average number of subgames is $1/(1-\delta)$. Therefore, a data session has at least $1/(1-\delta)$ packets with one packet being forwarded in a subgame. The simulation runs for 1000 seconds with different channel loss probabilities.

B. Performance Evaluation

Our investigation starts with the one hop packet forwarding (i.e., two-player packet forwarding game). We set the game payoff matrix as $T = 0.8$, $R = 0.7$, $P = 0.1$ and $\delta = 0.99$. Figure 3 shows the average payoff for each of the nodes using our state machine based forwarding strategy. For comparison, we plot the payoff for "Full Cooperation" strategy as well. Full cooperation implies that a node will always forward others' packet unconditionally. The theoretical bounds for our proposed strategy are also presented. The plot shows that the payoffs of the proposed strategy are within the theoretical limits developed in Corollary 2. Also, it is observed that the payoffs are very close to the unconditional "Full Cooperation" strategy. The average payoffs are much closer to the upper bound than the lower bound because when the games reach sequential equilibria, mutual cooperation is enforced.

Figure 4 presents the average node payoffs with different channel loss probabilities (Packet Error Rate, PER) p_e and discount factor δ. Note that $\delta = 0.999$ implies 1000 subgames played while $\delta = 0.99$ implies 100 subgames. The plots provide two insights: (i) as the channel becomes more unreliable, the average payoff drops and (ii) the more games are played, the more average payoff is generated. These observations also suggest that it is more desirable to have more packets in one continuous data session before switching for another relaying node.

We show the equilibrium nature of the proposed state machine based forwarding strategy in Figure 5. The payoffs of deviation strategies are plotted. In the deviation strategies, when the node is in state C, it always plays $Discard$ with probability $q_C = 0.1$ or $q_C = 0.15$ (Recall that in our equilibrium strategy, q_C is very small.). In this setting, $\delta = 0.999$ and $p_e = 0.01$. Figure 5 clearly shows that the payoffs with our proposed strategy are strictly greater that the deviation strategies.

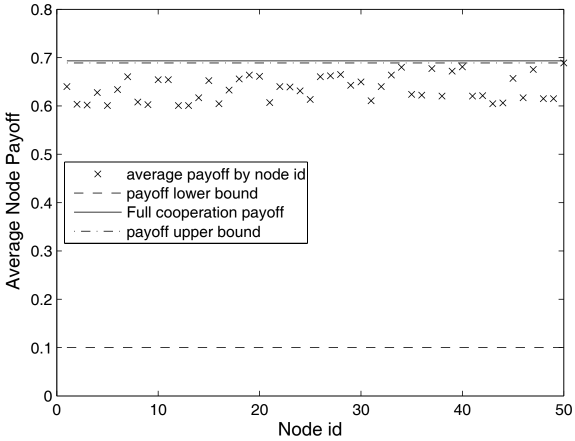

Fig. 3. Average node payoff for state machine based forwarding strategy.

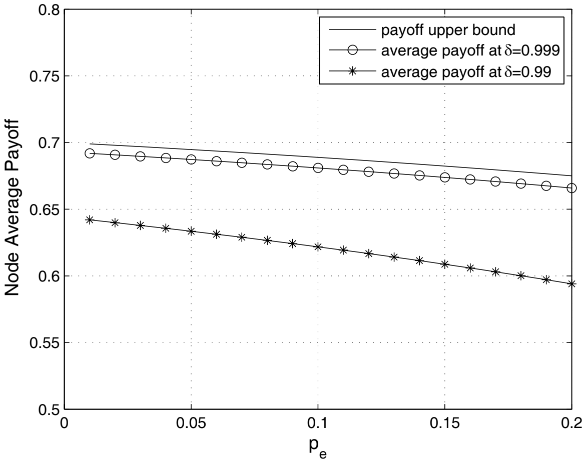

Fig. 4. Average node payoff with different channel loss probability and discount factor.

To further evaluate our proposed strategies, we consider the network performance by assuming every hop on a data route is independent. In Figure 6, we present the normalized network throughput at $\delta = 0.99$. We denote 1 as the state that all the generated packets are successfully delivered from source to destination. It is shown that with a small channel loss probability ($p_e = 0.01$), our proposed State Machine based Forwarding strategy (SMF) reaches almost the same throughput as the fully cooperative strategy. With a larger p_e, the throughput difference between SMF and the unconditional cooperation case is larger.

In addition, we analyze the effects of hop count and channel unreliability on the throughput. The results are shown in Figure 7 with $\delta = 0.999$. It can be noted that throughput drops

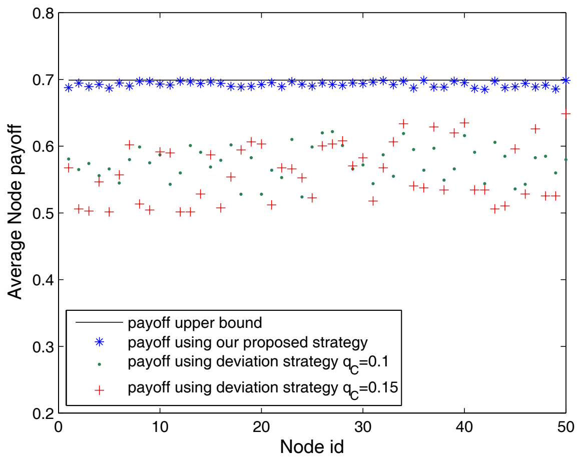

Fig. 5. Average node payoff comparison with deviation strategies.

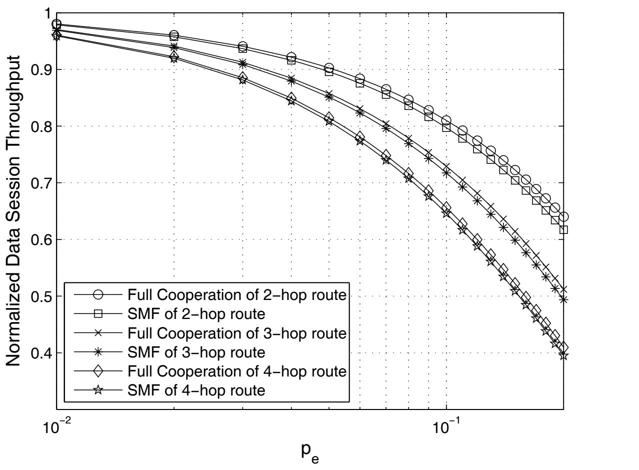

Fig. 7. Normalized data session throughput vs. hop count and channel loss probability.

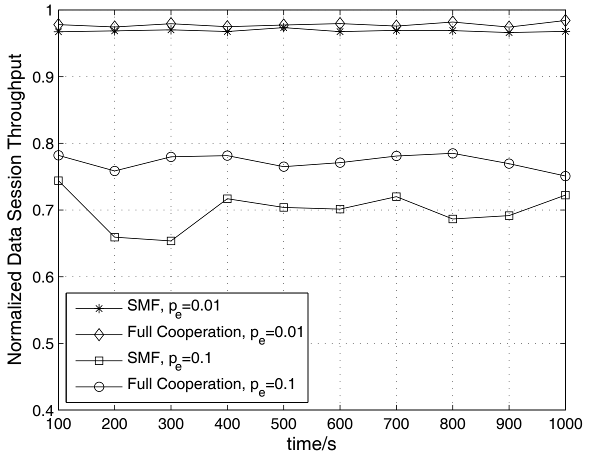

Fig. 6. Normalized data session throughput for different channel loss probability and strategies.

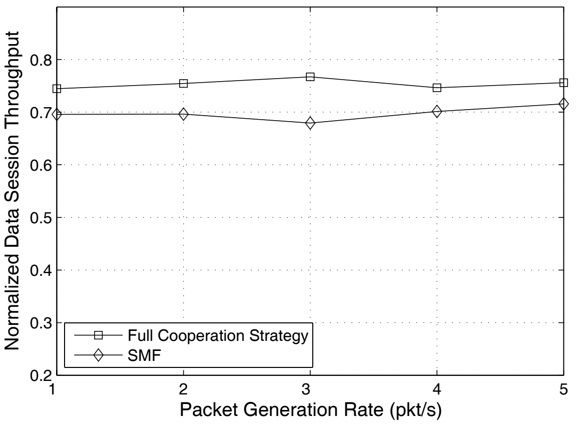

Fig. 8. Normalized data session throughput vs. packet generation rates.

when channel becomes more unreliable or hop count increases. Also, our proposed SMF yields throughput performance very close to the situation where all the nodes are unconditionally cooperative.

The relationship of packet generation rate and throughput is presented in Figure 8. In this setting, channel loss rate (PER) p_e for each link is non-identical and set to a random value in [0.005, 0.015]. δ is set to 0.99. The plots do not show much difference for different packet rates and the throughput remains almost constant. It is noted that although our simulation data rate does not fully utilize the link capacity, the result will not change in a saturated network. The reason is because the game is in an extensive game form, which does not require that all players move (take actions) at the same time. Therefore, even if there are collisions and/or delays when nodes try to access the channel, our modeling of the game is still valid.

Last but not least, we study the effect of mobility. In this setting, $p_e = 0.01$, $\delta = 0.999$. We use Random WayPoint (RWP) mobility profile with 5 seconds of pause in between two consecutive moves. Figure 9 plots the throughput performance for two different speeds. The results suggest that mobility introduces link break probability and decreases the throughput for our proposed forwarding strategy.

C. Population Dynamics

To illustrate how the dynamics of the population evolves and how collusion can be resisted in the forwarding games, we take the average population share over five simulation runs and plot how the population changes as the games are played. The strategies adopted by the nodes are our proposed State Machine based Forwarding (SMF) and a naive collusion strategy (CS) defined as follows:

DEFINITION 5: Naive Collusion Strategy (CS): Forward all packets from the colluding group, discard all packets from outside the group.

In Figure 10, we show the population dynamics with different initial population share and channel loss rates. It is very clear from the plots that the population adopting SMF overtakes that adopting CS and the games eventually converge to a point where the entire population adheres to

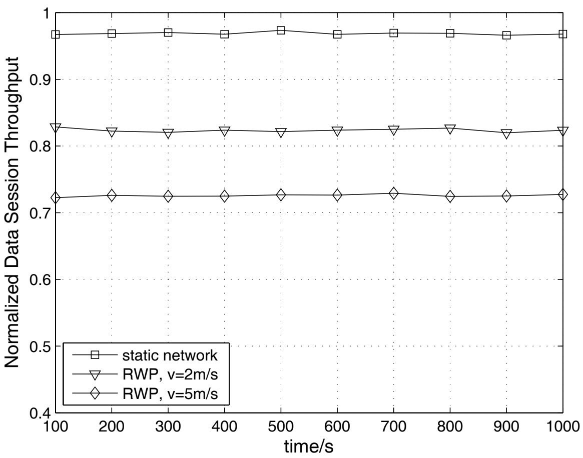

Fig. 9. Normalized data session throughput for mobile nodes.

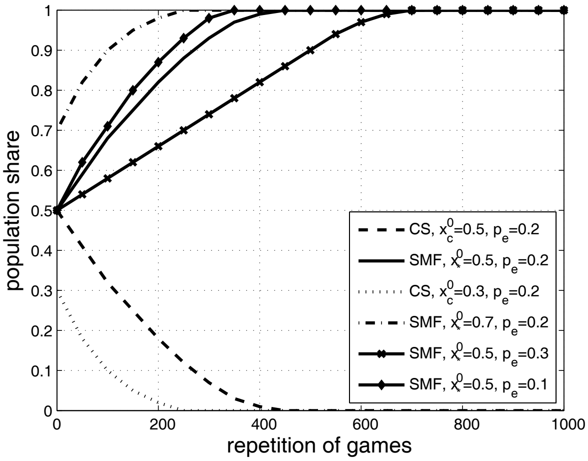

Fig. 10. The effect of initial population share and channel unreliability.

SMF, i.e., all the nodes are cooperative. It is also suggested that a larger initial cooperative population ($x_*^0 = 0.7$) leads to a faster convergence of the population evolution. The plots also clearly imply that the more reliable the channel is, the faster cooperation can be enforced.

VI. Conclusions

In this paper, we investigate strategies that attain cooperation in wireless networks with noisy channel. We consider packet forwarding in unreliable channel as the core problem and abstract it into a game theoretic model. The heterogeneous and unreliable nature of the channel only allow the game to be played with imperfect private information. To solve the game, we propose a state machine based forwarding strategy which brings a sequential equilibrium to the game. We also show that through carefully designing the system parameters, the equilibrium points are attainable. To address how cooperation can be achieved in the presence of collusion, we apply evolutionary game theory and show collusion resistance and cooperation enforcement are equivalent. Our research is backed by extensive simulation results. In particular, we show how the proposed forwarding strategy outperforms other non-cooperative strategies. Moreover, we provide the network throughput performance under the proposed strategy with respect to hop count, channel loss probability, and mobility. In addition, the convergence of cooperation is also shown to be related with initial cooperative population share and channel unreliability.

References

[1] D. Abreu, D. Pearce, and E. Stacchetti, “Towards a theory of discounted repeated games with imperfect monitoring," *Econometrica*, vol. 58, pp. 1041-1064, 1990.

[2] E. Altman, V. S. Borkar, A. Kherani, P. Michiardi, and R. Molva, “Some game-theoretic problems in wireless ad-hoc networks," in *Proc. EuroNGI Workshop 2004*, pp. 82-104.

[3] L. Anderegg and S. Eidenbenz, “Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," in *Proc. ACM Mobicom 2003*, pp. 245-259.

[4] S. Bansal and M. Baker, “Observation-based cooperation enforcement in ad hoc networks," Technical Report, Standford University, 2003.

[5] D. Bertsekas, *Dynamic Programming and Optimal Control*. Athena Scientific, 2001.

[6] V. Bhaskar and I. Obara, “Belief-based equilibria in repeated prisoners' dilemma with private monitoring," *J. Economic Theory*, vol. 102, pp. 40-69, 2002.

[7] L. Blazevic, L. Buttyán, S. Capkun, S. Giordiano, J. P. Hubaux, and J. Y. Le Boudec, “Self-organization in mobile ad-hoc networks: the approach of terminodes," *IEEE Commun. Mag.*, vol. 39, no. 6, pp. 166-174.

[8] S. Buchegger and J. L. Boudec, “Performance analysis of the confidant protocol: cooperation of nodes—fairness in dynamic ad-hoc networks," in *Proc. ACM MobiHoc 2002*, pp. 226-236.

[9] L. Buttyán and J. P. Hubaux, “Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks," Technical Report EPFL, DSC, 2001.

[10] L. Buttyán and J. P. Hubaux, “Enforcing service availability in mobile ad-hoc WANs," in *Proc. ACM Mobihoc 2000*, pp. 87-96.

[11] L. Buttyán and J. P. Hubaux, “Stimulating cooperation in self-organizing mobile ad-hoc networks," *ACM/Kluwer Mobile Netw. Appl.*, vol. 8, no. 5, pp. 579-592.

[12] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, “Modelling incentives for collaboration in mobile ad hoc networks," *Performance Evaluation*, vol. 57, no. 4, pp. 427-439.

[13] M. Félegyházi, J.-P. Hubaux, and L. Buttyan, “Nash equilibria of packet forwarding strategies in wireless ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 5, no. 5, pp. 463-476.

[14] M. Feldman, J. Chuang, I. Stoica, and S. Shenker, “Hidden-action in multi-hop routing," in *Proc. ACM E-Commerce 2005*, pp. 117-126.

[15] J. J. Jaramillo and R. Srikant, “DARWIN: distributed and adaptive reputation mechanism for wireless ad-hoc networks," in *Proc. ACM MobiCom 2007*, pp. 87-97.

[16] Z. Ji, W. Yu, and K. J. R. Liu, “Cooperation enforcement in autonomous MANETs under noise and imperfect observation," in *Proc. IEEE SECON 2006*, pp. 460-468.

[17] M. Kandori, “Introduction to repeated games with private monitoring," *J. Economic Theory*, vol. 102, pp. 1-15, 2002.

[18] M. Kandori and I. Obara, “Efficiency in repeated games revisited: the role of private strategies," *Econometrica*, vol. 74, no. 2, pp. 499-519, 2006.

[19] D. M. Kreps and R. Wilson, “Sequential equilibria," *Econometrica*, vol. 50, no. 4, pp. 863-894, 1982.

[20] X.-Y. Li, Y. Wu, P. Xu, G. Chen, and M. Li, “Hidden information and actions in multi-hop wireless ad hoc networks," in *Proc. ACM Mobihoc 2008*, pp. 283-292.

[21] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, “Sustaining cooperation in multi-hop wireless networks," in *Proc. NSDI 2005*, pp. 231-244.

[22] A. B. Mackenzie and S. B. Wicker, “Game theory and the design of self-configuring, adaptive wireless networks," *IEEE Commun. Mag.*, Nov. 2001, pp. 126-131.

[23] P. Michiardi and R. Molva, “Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proc. Commun. Multimedia Security Conf. 2002*, pp. 107-121.

[24] P. Michiardi and R. Molva, “Analysis of coalition formation and cooperation strategies in mobile ad hoc networks," *Ad Hoc Networks*, vol. 3, 2005, pp. 193-219.

[25] F. Milan, J. J. Jaramillo, and R. Srikant, “Achieving cooperation in multihop wireless networks of selfish nodes," in *Proc. GameNets Workshop 2006*.

[26] M. J. Osborne, *An Introduction to Game Theory*. Oxford University Press, 2004.

[27] M. T. Refaei, V. Srivastava, L. DaSilva, and M. Eltoweissy, “A reputation-based mechanism for isolating selfish nodes in ad hoc networks," in *Proc. Mobiquitous 2005*, pp. 3-1-1.

[28] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, “Cooperation in wireless ad hoc networks," in *Proc. IEEE Infocom 2003*, pp. 807-817.

[29] W. Wang, M. Chatterjee, and K. Kwiat, “Cooperation enforcement in ad hoc networks under unreliable channel," in *Proc. IEEE MASS 2008*, pp. 456-462.

[30] J. W. Weibull, *Evolutionary Game Theory*. MIT Press, 1995.

[31] W. Yu and J. K. R. Liu, “Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks," *IEEE Trans. Mobile Comput.* vol. 6, no. 5, pp. 507-521, 2007.

[32] S. Zhong, L. Li, Y. Liu, and Y. Yang, “On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks—an integrated approach using game theoretical and cryptographic techniques," in *Proc. ACM Mobicom 2005*, pp. 117-131.

Wenjing Wang obtained Ph.D. in Electrical Engineering from School of Electrical Engineering and Computer Science at the University of Central Florida in 2010. He received his B.Sc. from the University of Science and Technology of China (USTC) in 2005 and M.S. from the University of Central Florida in 2007, both in Electrical Engineering. His research interests include applied game theory, wireless access networks, ad hoc networks, vehicular inter-networking and transport layer protocols. He is a recipient of the AT&T graduate fellowship. He is currently affiliated with Attila Technologies LLC, as a scientist.

Mainak Chatterjee received his Ph.D. from the Department of Computer Science and Engineering at The University of Texas at Arlington in 2002. Prior to that, he completed his B.Sc. with Physics (Hons) from the University of Calcutta in 1994 and M.E. in Electrical Communication Engineering from the Indian Institute of Science, Bangalore, in 1998. He is currently an Associate Professor in the school of Electrical Engineering and Computer Science at the University of Central Florida. His research interests include economic issues in wireless networks, applied game theory, resource management and quality-of-service provisioning, ad hoc and sensor networks, CDMA data networking, and link layer protocols. He serves on the executive and technical program committee of several international conferences. Email: mainak@eecs.ucf.edu.

Kevin A. Kwiat has been a civilian employee with the U.S. Air Force Research Laboratory (AFRL) in Rome, New York for over 28 years. He received the BS in Computer Science and the BA in Mathematics from Utica College of Syracuse University, and the MS in Computer Engineering and the Ph.D. in Computer Engineering from Syracuse University. He holds 4 patents. In addition to his duties with the Air Force, he is an adjunct professor of Computer Science at the State University of New York at Utica/Rome, an adjunct instructor of Computer Engineering at Syracuse University, and a Research Associate Professor with the University at Buffalo. He completed assignments as an adjunct professor at Utica College of Syracuse University, a lecturer at Hamilton College, a visiting scientist at Cornell University, and as a visiting researcher at the University of Edinburgh as part of the Air Force Office of Scientific Research “Window on Europe” program. He has been recognized by the AFRL Information Directorate with awards for best paper, excellence in technology teaming, and for outstanding individual basic research. His main research interest is dependable computer design.