Incentive-Compatible Multirate Opportunistic Routing in Non-Cooperative Wireless Mesh Networks

Kai Gong Tianrong Zhang Fan Wu Guihai Chen
Department of Computer Science and Engineering
Shanghai Jiao Tong University, China
{wayngong, tzr1211, wu-fan, gchen}@sjtu.edu.cn

Chunming Qiao
Department of Computer Science and Engineering
The State University of New York at Buffalo, USA
qiao@buffalo.edu

***Abstract*—Wireless mesh networks have emerged as an efficient alternative to deploy broadband network infrastructures in local communities at low cost. To overcome the problem caused by the lossy and dynamic wireless links, opportunistic routing was proposed to achieve high throughput by exploiting multi-user diversity. Since wireless channels exhibit different packet loss probabilities at different transmission bit rates, carefully selecting bit rate at each hop can significantly improve system performance. However, the performance of multirate opportunistic routing still cannot be guaranteed when participating mesh nodes are contributed by different parties and thus have selfish behaviors. In this paper, we present the first incentive protocol for multirate opportunistic routing, under which it is to the best interest of each mesh node to faithfully follow the multirate opportunistic routing protocol. We not only rigorously prove the properties of our protocols but also thoroughly evaluate our incentive protocol on ORBIT wireless testbed. Experiment results show that our protocol can prevent participating nodes' selfish behaviors and guarantee high performance of the multirate opportunistic routing protocol.**

I. Introduction

Wireless mesh networks have emerged as an efficient alternative to deploy broadband network infrastructures in local communities at low cost [1], [2]. A major challenge, which restricts the wireless mesh network from being widely deployed, is throughput scalability. The high loss probability and dynamic quality of wireless links make traditional routing perform badly in wireless mesh networks, especially in urban environments with many interference sources [3]. To overcome the problem caused by the lossy and dynamic wireless links, opportunistic routing [4]–[7] was proposed to achieve high throughput by exploiting multi-user diversity. Different from traditional routing, which deterministically chooses the next hop before transmitting a data packet, opportunistic routing aggregates the power of multiple lossy wireless links by allowing any node who overheard the packet to participate in packet forwarding. Recently, Laufer *et al.* [8] extended existing opportunistic routing protocols to better utilize wireless channels by exploiting the wireless radios' capability of working on multiple transmission bit rates specified by IEEE 802.11 protocols. Their results show that by incorporating multirate transmissions, the opportunistic routing protocol can exhibit much better performance.

Although opportunistic routing has shown its superior performance against traditional deterministic routing in many cases, its performance still cannot be guaranteed when participating mesh nodes are contributed by different parties and thus have selfish behaviors [9]. Similar with other distributed autonomous systems, wireless mesh networks suffer common incentive problems, such as the free-rider problem, where only a small part of participates contribute their resources [10], and the adverse selection problem, where participants do not truthfully reveal their link states [11]. While the free-rider problem can commonly be solved by introducing compensation for contributing one's resources, overcoming the problem of adverse selection is not trivial, especially in wireless mesh networks.

Most of opportunistic routing protocols need to collect the link loss probabilities to make the efficient routing decision. Since the link loss probabilities are private information of the mesh nodes or need to be measured with the cooperation of the participating nodes, a selfish-behaving node may manipulate its incoming and outgoing links' loss probabilities in order to mislead the routing decision to be the one that is more beneficial to itself. Wu *et al.* [9] studied the problem of selfish behavior in opportunistic routing, and proposed practical solutions to stimulate mesh nodes' incentives to truthfully measure the link loss probabilities and follow MORE [5]-based opportunistic routing protocols. However, Wu *et al.*'s work cannot guarantee the incentive-compatibility of the opportunistic routing protocol, when mesh nodes can employ multiple transmission bit rates to transmit a packet.

In this paper, we present the first incentive protocol for multirate opportunistic routing, under which it is to the best interest of each mesh node to faithfully follow the multirate opportunistic routing protocol. Our contributions are listed as follows.

- First, we are the first to study the incentive problem of multirate opportunistic routing and to provide a practical solution.
- Second, we show that the closest related existing work, proposed by Wu *et al.* [9], cannot prevent the nodes' misbehavior in opportunistic routing when mesh nodes can work on multiple transmission bit rates.
- Third, we present a practical incentive protocol that achieves cooperation-optimality in multirate

opportunistic routing, *i.e.*, when everyone follows the routing and incentive protocol, the system performance gets optimized and each mesh node gets its payoff maximized. Specifically, we incorporate probe messages, which is used to measure the link loss probabilities, with a cryptographic component to prevent the probe message from being forged, and carefully design a payment scheme to guarantee that the mesh nodes cannot benefit from manipulating the link loss probability measuring process or deviating from the routing decision.

- Finally, we have conducted extensive experiments to evaluate the performance of our incentive protocol on the ORBIT wireless testbed [12]. Our evaluation results show that our incentive protocol can prevent participating nodes' misbehavior and guarantee the optimal performance of the system.

The rest of the paper is organized as follows. In Section II, we give technical preliminaries on opportunistic routing, and game theoretic model of multirate opportunistic routing. In Section III, we show the infeasibility of existing works. In Section IV, we present our incentive protocol, and prove its cooperation optimality. In Section V, we report the evaluation results on ORBIT wireless testbed. In Section VI, we review the related works. Finally, we conclude the paper and point out potential future directions to improve the work in Section VII.

II. Technical Preliminaries

In this section, we first review the opportunistic routing protocols we consider. Then, we give a simple example to illustrate that nodes have motivations to cheat in a multirate opportunistic routing protocol. We also present the game theoretic model to the problem, and review relevant game theoretic solution concepts.

A. Basic Opportunistic Routing Protocol

Opportunistic routing is an emerging technique to achieve high throughput despite lossy wireless links. Instead of deterministically choosing the next hop before transmitting a packet, opportunistic routing allows multiple nodes overheard the packet to participate in forwarding.

Similar with [9], we focus on a class of basic opportunistic routing protocols (*e.g.*, [5]). A basic opportunistic routing protocol takes link loss probabilities as input, and outputs the times a node needs to forward a received packet and the transmission bit rate the node should use.

Formally, let N be the set of nodes in the wireless mesh network, E be the set of directed virtual links that are considered by the basic routing protocol for forwarding packets from a source node S to a destination node D, and R be the set of available transmission bit rates. Let ϵ_{ij}^r be the link loss probability of directed virtual link $(i,j) \in E$ at transmission rate $r \in R$; *i.e.*, if a packet is sent from node i to node j at rate r, then with probability ϵ_{ij}^r the packet cannot be decoded. Given a path metric, which specifies the "distance" of each node to the destination node, the basic opportunistic routing protocol specifies a function $\mathcal{F}()$ to compute the expected number of transmissions z_i for each node $i \in N$:

$$\begin{aligned} z_i \;=\; & \mathcal{F}\big(N, S, D, i, \\ & \{\big(j,k,r,\epsilon_{jk}^r\big)\,|j,k \in N, r \in R\}, \\ & \{(j,d_j,r_j)|j \in N\}\big), \end{aligned}$$

where d_j is node j's distance to the destination node under the path metric, and r_j is node j's corresponding transmission bit rate that achieve distance d_j. Since transmitting data packets consumes players' battery power, we assume that the cost of transmitting per second is ρ. Then, the expected transmission cost on node i can be defined as $c_i = z_i L\rho/r_i$, where L is the packet length.

Due to limitation of space, we omit the detail of the basic opportunistic routing protocol. Please refer to [5], [9] for detail.

Path Metric:

The calculation of routing decision relies on the path metric, which captures the "distance" from a node to the destination. De Couto *et al.* [13] proposed the ETX metric, which is defined as the expected number of transmissions necessary to deliver one packet from a node to the destination. Later, an extension to ETX metric was proposed as EATX metric [5], [14], [15], which captures the expected number of anypath transmissions. To support multiple transmission bit rates provided by IEEE 802.11 protocols, Laufer *et al.* [8] introduced the expected anypath transmission time (EATT) metric.

Although most of the instances of the basic opportunistic routing protocol are designed based on ETX/EATX distance, they can be easily adapted to EATT distance. Experiment results [8] show that when multirate is used, EATT always achieves equal or higher performance than ETX/EATX. Therefore, we assume that the basic opportunistic routing protocol incorporates EATT metric.

Laufer *et al.* have presented a Shortest Multirate Anypath algorithm, denoted by $\mathcal{M}()$, to compute the nodes' transmission bit rates that minimize the nodes' overall distance to reach a destination [8]:

$$(d_i, r_i) = \mathcal{M}\big(N, D, i, \{(k,l,r,\epsilon_{kl}^r)\,|k,l \in N, r \in R\}\big).$$

With the above defined distance, we say $i < j$, if i is closer to the destination than j under the EATT metric.

Then we can derive $\mathcal{F}()$ to be

$$\begin{aligned} z_i \;=\; & \mathcal{F}\big(N, S, D, i, \\ & \{\big(j,k,r,\epsilon_{jk}^r\big)\,|j,k \in N, r \in R\}, \\ & \{\big(j, \mathcal{M}\big(N, D, i, \{(k,l,r,\epsilon_{kl}^r)\,|k,l \in N, r \in R\}\big)\big) \\ & \quad |j \in N\}\big). \end{aligned}$$

Since we model each communication session as an independent strategic game, for ease of presentation, we rewrite the above function $\mathcal{F}()$ in a concise form in the rest of the paper:

$$z_i = \mathcal{F}\left(N, i, \left(\epsilon_{jk}^r\right)_{j,k \in N, r \in R}\right).$$

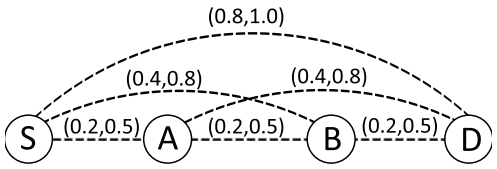

Fig. 1. An example to illustrate the impact of misbehavior in basic opportunistic routing. There is a session from source S to destination D, with two intermediate nodes A and B. True link loss probabilities are shown near the links. The available transmission bit rates are r and $2r$. Here $(0.2, 0.5)$ means that the link's loss probability is 0.2 at transmission bit rate r and 0.5 at rate $2r$. Node A can lower its cost by 43.9% by manipulating the loss probabilities on link (A, B) and (A, D) at transmission bit rate $2r$ to be 0.3 and 0.6, respectively.

B. Motivating Example

We assume that the basic opportunistic routing protocol incorporates the EATT metric to make the routing decision. The efficiency of the routing decision relies on the assumption that every node follows the protocol. However, a node may deviate from the specified protocol in order to lower its cost.

Let's consider the scenario shown in Figure 1. There is a session from source S to destination D, with two intermediate nodes A and B. True link loss probabilities are shown near the links. The available transmission bit rates are r and $2r$. Here $(0.2, 0.5)$ means that the link's loss probability is 0.2 at transmission bit rate r and 0.5 at rate $2r$. We assume that the MORE protocol, which is an instance of the basic opportunistic routing protocol, is used with EATT metric. Using the truthful link loss probabilities, node A's expected transmission cost is $0.2973L\rho/r$. However, by manipulating the loss probabilities on link (A, B) and (A, D) at transmission bit rate $2r$ to be 0.3 and 0.6, respectively, node A can reduce its expected transmission cost to $0.1668L\rho/r$, which is a reduction of 43.9%. Consequently, node A is prone to misbehaving. Unfortunately, such misbehavior may lead to system performance degradation. Therefore, it is highly needed to design incentive protocols to prevent the nodes from misbehaving.

C. Game Theoretic Model

We model the problem of multirate opportunistic routing as a *strategic game*, and study how to guarantee optimal end-to-end throughput when selfish nodes/players exist. The players of this game are the intermediate nodes, denoted by $N \setminus \{S, D\}$, that are supposed to forward packets.

Each player $i \in N$ takes a strategy s_i. The strategy of a player is to determine the number of probe messages to send, and to choose which received probe messages to report. We assume that the source node and the destination node are trustworthy. The source node computes the routing decision, and pays the forwarders for their service.

To enable nodes to pay each other, just as in [16]–[22], we assume that there is some kind of virtual currency in the system. In the system, there is a Credit Clearance Center (CCC). Each node has an account in the CCC and each transaction has to be processed by the CCC. The CCC is a server connected to the Internet. So the node can access the CCC whenever they have connections to the Internet.

Generally, the utility can be written as a function of the profile of all players' strategies

$$u_i = u_i((s_j)_{j \in N}).$$

In this paper, we introduce a carefully designed payment scheme to stimulate the players' incentives to correctly broadcast right number of probe messages, truthfully report the received probe messages, and faithfully follow the computed routing decision. Specifically, in our strategic game model of multi-rate opportunistic routing, the utility u_i is expressed as the difference between payment p_i and cost c_i for forwarding data packets:

$$\begin{aligned} u_i &= p_i - c_i \\ &= p_i - \frac{z_i L \rho}{r_i}. \end{aligned}$$

We assume that the players are rational and their objectives are to maximize their own utilities.

To study the rational behaviors of the nodes in the strategic game of multi-rate opportunistic routing, we now recall a well-known solution concept, namely *Nash equilibrium* (NE), in game theory.

Definition 1 (Nash equilibrium [23]): A profile $s^\star$ of all players' strategies is a Nash equilibrium, if for all $i \in N$, for all strategy $s_i \neq s_i^\star$ of player i, we have

$$u_i(s_i^\star, s_{-i}^\star) \geq u_i(s_i, s_{-i}^\star).$$

Conventionally, s_{-i} denotes the strategy profile of the players other than player i. Intuitively, in a NE, no player can benefit by unilaterally deviating from her equilibrium strategy. However, a NE solution is usually inefficient from the system point of view. We induce *strong Pareto optimality* to characterize the efficiency of the solution.

Definition 2 (strong Pareto optimality [23]): A strategy profile $s^\triangle$ of all players is strongly Pareto efficient, if there does not exist a strategy profile $s' \neq s^\triangle$, such that

$$u_i(s') \geq u_i(s^\triangle), \forall i \in N,$$

with strict inequality for at least one player i.
In other words, in a strongly Pareto efficient strategy profile, no one can improve her utility without decreasing the utility of at least one other player. Strong Pareto optimality provides us a way to identify the desired Nash equilibrium in a strategic game.

In reality, any practical incentive protocol for multirate opportunistic routing should also guarantee high performance of the system. Therefore, we introduce *social efficiency*, which means that the end-to-end throughput should be maximized.

We now define the solution concept, namely *cooperation-optimal protocol*, to the strategic game of multirate opportunistic routing.

Definition 3: A protocol is a cooperation-optimal protocol to the strategic game of multirate opportunistic routing, if it is a socially efficient and strongly Pareto efficient Nash equilibrium, when every player faithfully follows the protocol.

III. Infeasibility of Existing Work

As far as we know, the closest related work to this paper is the incentive-compatible opportunistic routing protocol proposed by Wu *et al.* [9]. Their incentive scheme stimulates nodes' incentive to report/measure link loss probabilities truthfully. Their scheme works well when each node only has a single bit rate to do the transmission. However, in the case of multiple transmission bit rates, since the lowest bit rate normally achieves the smallest loss probability, Wu *et al.*'s scheme will always selects the lowest transmission bit rate on each node to do the transmission in order to reduce packet loss. Unfortunately, selfish nodes can deviate from the protocol to get more payoff. Furthermore, always selecting the lowest transmission bit rate may not the most efficient routing decision.

Without losing generality, we assume

$$r^j < r^k, \forall j < k, 1 \leq j, k \leq |R|.$$

According to Wu *et al.*'s scheme, we have

$$\begin{aligned} r_i^* &= r^1, \\ z_i^{r_i^*} &= \mathcal{F}(N, i, \{(j, k, \epsilon_{j,k}^{r_i^*}) | j, k \in N\}), \\ z_{i,j}^{\star} &= \frac{\alpha(1-\epsilon_{i,j}^{r_i^*})^2}{2}, \end{aligned}$$

and

$$p_i = \frac{\rho}{r_i^*}\left(z_i^{r_i^*} L + \sum_{(i,j)\in E} \alpha(1-\epsilon_{i,j}^{r_i^*})\right),$$

where $\alpha > 0$ is a parameter chosen by the system administrator, and L is the length of the packet.

It was shown in Wu *et al.*'s work that each player gets her utility maximized when reporting loss probabilities truthfully, regardless what others do, in the case of single transmission bit rate. And the utility for node i is

$$\begin{aligned} u_i(s_i^*, s_{-i}) &= p_i - c_i \\ &= \frac{\alpha\rho}{2r_i^*} \sum_{(i,j)\in E} (1-\epsilon_{i,j}^{r_i^*}) \\ &= \frac{\alpha\rho}{2r^1} \sum_{(i,j)\in E} (1-\epsilon_{i,j}^{r^1}). \end{aligned}$$

However, in case of multiple transmission bit rates, a node i may use bit rate r^b (where $b > 1$) to transmit data packets. Assume that

$$\exists i \in N, \exists r^b > r^1, \forall j \in N\backslash\{i\}, r^b\cdot(1-\epsilon_{ij}^{r^b}) > r^1\cdot(1-\epsilon_{ij}^{r^1}).$$

Thus the utility of node i becomes:

$$\begin{aligned} & u_i'(s', s_{-i}) \\ = \; & p_i - c_i' \\ = \; & p_i - \frac{\rho}{r^b}\left(z_i^{r^1} L + \sum_{j\in N\backslash\{i\}} \frac{\alpha(1-\epsilon_{i,j}^{r^1})^2}{2(1-\epsilon_{i,j}^{r^p})}\right) \\ = \; & p_i - \frac{\rho z_i^{r^1} L}{r^b} - \frac{\alpha\rho}{2} \sum_{j\in N\backslash\{i\}} \frac{(1-\epsilon_{i,j}^{r^1})^2}{r^p(1-\epsilon_{i,j}^{r^b})} \\ > \; & p_i - \frac{\rho z_i^{r^1} L}{r^1} - \frac{\alpha\rho}{2} \sum_{j\in N\backslash\{i\}} \frac{(1-\epsilon_{i,j}^{r^1})^2}{r^1(1-\epsilon_{i,j}^{r^1})} \\ = \; & p_i - \frac{\rho}{r^1}\left(z_i^{r^1} L + \sum_{j\in N\backslash\{i\}} \frac{\alpha(1-\epsilon_{i,j}^{r^1})^2}{2(1-\epsilon_{i,j}^{r^1})}\right) \\ = \; & p_i - c_i \\ = \; & u_i(s_i^*, s_{-i}) \end{aligned}$$

So the node i can get higher utility by switching to a higher bit rate to transmit data packets. This shows that Wu *et al.*'s scheme can not prevent selfish behaviors in case of multiple transmission bit rate. Consequently, it is important to find an incentive-compatible routing scheme that stimulates nodes' incentive to honestly participate in the routing despite multirate opportunistic transmissions.

IV. Incentive Protocol

In this section, we present our practical incentive protocol that achieves cooperation-optimality in multirate opportunistic routing, i.e., each participating mesh node can always make its payoff maximized when performing truthfully. Specifically, we incorporate probe messages, which is used to measure the link loss probabilities, with a cryptographic component to prevent the probe message from being forged, and carefully design a payment scheme to guarantee that the mesh nodes cannot benefit by deviating from the protocol.

A. Protocol Detail

Link Loss Probability Measurement:

Both the correctness of EATT metric and the efficiency of the basic opportunistic routing protocol rely on correct measuring of link loss probabilities. Our previous example shows that incorrect link loss probabilities can mislead the basic opportunistic routing protocol, and thus result in inefficient routing decision.

We assume that there exists a key distribution scheme (*i.e.*, [24], [25]) in the wireless mesh network, such that there is a secret key $key(S, i)$ established between the source node S and every intermediate forwarding node $i \in N\backslash\{S, D\}$ before or during the routing initialization phase.

When a session from source node S to destination node D initialize, each intermediate node $i \in N\backslash\{S, D\}$ and the source node S sends m probe messages at each rate $r \in R$ in turn. Then each intermediate node $i \in N \setminus \{S, D\}$ and the destination node D reports the received probe messages to the source node using one of the traditional reliable routing protocols.

We design the format of the probe message sent from node $i \in N \setminus \{D\}$ as followed:

$$< PROBE, i, r, q, MAC_{key(S,i)}(PROBE, i, r, q) >,$$

where q is a unique sequence number, and MAC is a keyed cryptographic Message Authentication Code function (*e.g.*, VMAC [26]). $MAC_{key(S,i)}()$ outputs a digital tag given the secret key between the source S and node i, ensuring that no other node can forge such a probe message.

After collecting the reported probe messages, the source node can compute the link loss probabilities. Suppose the source node collects m_{ij}^r probe messages sent from node i and reported by node j at transmission rate r. The measured loss probability on virtual link (i, j) can be computed as

$$\epsilon_{ij}^{\prime r} = 1 - \frac{m_{ij}^r}{m}.$$

Here, we use $\epsilon_{ij}^{\prime r}$ instead of ϵ_{ij}^r, because the measured link loss probability is not guaranteed to be correct considering the selfish behavior of the player nodes. Therefore, we introduce the following payment scheme to guarantee that truthfully measuring the link loss probability is to the best interest of each player node.

Payment Cap:

If not getting properly compensated, a selfish player node may simply do not participate in packet forwarding at all, or manipulate its incoming and outgoing links' loss probabilities in order to mislead the routing decision to be the one that is more beneficial to itself. Such selfish behaviors will inevitably lead to system performance degradation. To stimulate the selfish player nodes' incentives to faithfully participate in the process of opportunistic routing, we introduce *payment cap*, which is the limit of compensation a player node can get.

Based on measured link loss probabilities, the source node S computes the shortest multirate anypath to the destination node D via intermediate player nodes $N \setminus \{S, D\}$, and each node's workload z_i and best transmission bit rate r_i. To determine the payment cap to each intermediate player node $i \in N$, S also computes the shortest multirate anypath if node i is absent from the forwarder set. Then the payment cap of node $i \in N \setminus \{S, D\}$ is defined as

$$\begin{aligned}\hat{p}_i &= L\rho \sum_{j \in N \setminus \{i\}} \frac{\mathcal{F}\left(N \setminus \{i\}, j, \left(\epsilon_{jk}^{\prime r}\right)_{j,k \in N \setminus \{i\}, r \in R}\right)}{r_j} \\ &\quad - L\rho \sum_{j \in N \setminus \{i\}} \frac{\mathcal{F}\left(N, j, \left(\epsilon_{jk}^{\prime r}\right)_{j,k \in N, r \in R}\right)}{r_j}.\end{aligned}$$

Intuitively, the payment cap of a node i is the difference between the total cost of the shortest multirate anypath if it does not participate in packet forwarding, and the total cost of the shortest multirate anypath without the cost incurred by itself.

Payment:

If we simply give each node the payment equaling to the previously defined payment cap, the node may deposit the virtual money without actually forwarding the packet. Therefore, to enforce the forwarding process, we need to design a payment scheme to connect the nodes' forwarding behaviors with their final payments.

We require each node i to attach a cryptographic tag to each data packets it forward. The format of cryptographic tag is similar to that of the probe message, except the transmission bit rate field r:

$$< DATA, i, q, MAC_{key(S,i)}(DATA, i, q) > .$$

Then every intermediate node $i \in N \setminus \{S, D\}$ and the destination node D reports the cryptographic tags to the source node using one of the traditional reliable routing protocols.

After gathering the cryptographic tags, the source node determines the final payment to each node. Let f_{ij} be the number of cryptographic tags sent from node i and reported by node j. Then, the payment formula is designed as follows:

$$p_i = \eta_i^{\triangle} \eta_i^{\nabla} \hat{p}_i,$$

where

$$\begin{aligned}\eta_i^{\triangle} &= \frac{\sum_{j>i} \min\left(f_{ji}, z_j\left(1 - \epsilon_{ji}^{\prime r_j}\right)\right)}{\sum_{j>i} z_j (1 - \epsilon_{ji}^{\prime r_j})}, \\ \eta_i^{\nabla} &= \left(\min\left(\min_{j<i}\left(\frac{f_{ij}}{z_i(1 - \epsilon_{ij}^{\prime r_i})}\right), 1\right) = 1\right)?1 : 0.\end{aligned}$$

Here, $\eta_i^{\triangle}$ calculates the sum of the normalized ratio of packets received by node i from its upstream nodes. Since only when a node receives sufficient number of coded packets from its upstream nodes, it can generate right number of innovative coded packets for forwarding. It is waste of energy to forwarding too many meaningless coded packets generated with a few received packets. Therefore, the final payment should be proportional to one's number of received packets. Considering that a node may cheat in the link loss probability measuring process to get higher payment cap, we introduce η_i^{∇} to ensure that the node has to do the required number of transmissions to get her compensation.

B. Analysis

In this section, we prove that our incentive protocol is cooperation-optimal to the strategic game of multirate opportunistic routing. To be cooperation-optimal, an incentive protocol needs to satisfy three requirements: 1) It is a Nash equilibrium that every node truthfully measures the link loss probabilities and faithfully follows the computed routing decision; 2) The above Nash equilibrium is strongly Pareto efficient; 3) In the above Nash equilibrium, optimal system performance is achieved.

We note that our incentive protocol satisfies the first requirement. In the Nash equilibrium specified in re-

quirement 1, the utility of a node i is

$$\begin{aligned} u_i^\star &= L\rho \sum_{j\in N\setminus\{i\}} \frac{\mathcal{F}\left(N\setminus\{i\}, j, \left(\epsilon_{jk}^r\right)_{j,k\in N\setminus\{i\}, r\in R}\right)}{r_j} \\ &\quad -L\rho \sum_{j\in N} \frac{\mathcal{F}\left(N, j, \left(\epsilon_{jk}^r\right)_{j,k\in N, r\in R}\right)}{r_j}. \end{aligned}$$

Lemma 1: When our incentive protocol is used, it is a Nash equilibrium that every node truthfully measures the link loss probabilities and faithfully follows the computed routing decision made by the basic opportunistic routing protocol.

Proof: Let's consider a node i. Suppose the other nodes correctly send the right number of probe messages and truthfully report the received probe messages from i to the source S. Suppose the node i send $h_i^r \geq 0$ times required probe messages at transmission bit rate r, then the measured loss probability on link (i,j) at transmission bit rate r is

$$\epsilon_{ij}^{\prime r} = 1 - h_i^r(1-\epsilon_{ij}^r), \forall j \in N\setminus\{i\}.$$

Suppose the node i reports a ratio $g_{ji}^r \leq 1$ of received probe messages from node j at transmission rate r, then the measured loss probability on link (j,i) is

$$\epsilon_{ji}^{\prime r} = 1 - g_{ji}^r(1-\epsilon_{ji}), \forall j \in N\setminus\{i\}.$$

Then node i's payment cap is

$$\begin{aligned} \hat{p}_i' &= L\rho \sum_{j\in N\setminus\{i\}} \frac{\mathcal{F}\left(N\setminus\{i\}, j, \left(\epsilon_{jk}^r\right)_{j,k\in N\setminus\{i\}, r\in R}\right)}{r_j} \\ &\quad -L\rho \sum_{j\in N\setminus\{i\}} \frac{\mathcal{F}\left(N, j, \left(\epsilon_{jk}^{\prime r}\right)_{j,k\in N, r\in R}\right)}{r_j}. \end{aligned}$$

where $\epsilon_{jk}' = \epsilon_{jk}$, when $j \neq i \wedge k \neq i$. This equivalence also holds in the following analysis.

Suppose node i reports a ratio $b_{ji} \leq 1$ of cryptographic tags, and forwards $\bar{z}_i$ coded packets using transmission rate $\bar{r}_i$. Then its payment got is

$$p_i' = \eta_i'^{\triangle}\eta_i'^{\nabla}\hat{p}_i'.$$

The node i's utility is

$$\begin{aligned} u_i' &= p_i' - c_i' \\ &= \eta_i'^{\triangle}\eta_i'^{\nabla}\hat{p}_i' - \frac{\bar{z}_i L\rho}{\bar{r}_i}. \end{aligned}$$

Considering that

$$\begin{aligned} \eta_i'^{\triangle} &= \frac{\sum_{j>i}\min\left(f_{ji}', z_j'(1-\epsilon_{ji}^{\prime r_j'})\right)}{\sum_{j>i} z_j'(1-\epsilon_{ji}^{\prime r_j'})} \\ &= \frac{\sum_{j>i}\min\left(z_j'(1-\epsilon_{ji})b_{ji}, z_j'(1-\epsilon_{ji}^{\prime r_j'})\right)}{\sum_{j>i} z_j'(1-\epsilon_{ji}^{\prime r_j'})} \\ &= \frac{\sum_{j>i}\min\left(z_j'(1-\epsilon_{ji})b_{ji}, z_j'(1-\epsilon_{ji})g_{ji}\right)}{\sum_{j>i} z_j'(1-\epsilon_{ji})g_{ji}} \\ &\leq \frac{\sum_{j>i}\min\left(z_j'(1-\epsilon_{ji}), z_j'(1-\epsilon_{ji})g_{ji}\right)}{\sum_{j>i} z_j'(1-\epsilon_{ji})g_{ji}} \\ &= 1, \end{aligned}$$

it is best for the node i to report all the cryptographic tags it received. Consequently, we have

$$u_i' \leq \eta_i'^{\nabla}\hat{p}_i' - \frac{\bar{z}_i L\rho}{\bar{r}_i}.$$

Since only when

$$\bar{z}_i(1-\epsilon_{ij}^{\bar{r}_i}) \geq z_i'(1-\epsilon_{ij}^{r_i'})h_i^{r_i'}, \forall j < i,$$

node i can get her payment, we consider the case where

$$\bar{z}_i = \max_{j<i}\left(\frac{z_i'(1-\epsilon_{ij}^{r_i'})h_i^{r_i'}}{1-\epsilon_{ij}^{\bar{r}_i}}\right).$$

If in this case, the utility of node i is positive, we have

$$\begin{aligned} u_i' &= L\rho \sum_{j\in N\setminus\{i\}} \frac{\mathcal{F}\left(N\setminus\{i\}, j, \left(\epsilon_{jk}^r\right)_{j,k\in N\setminus\{i\}, r\in R}\right)}{r_j} \\ &\quad -L\rho \sum_{j\in N\setminus\{i\}} \frac{\mathcal{F}\left(N, j, \left(\epsilon_{jk}^{\prime r}\right)_{j,k\in N, r\in R}\right)}{r_j} \\ &\quad -\frac{\bar{z}_i L\rho}{\bar{r}_i}. \end{aligned}$$

Since the shortest multirate anypath algorithm computes the transmission bit rate that minimizes the overall distance to reach the destination [8], we have

$$\begin{aligned} &L\rho\sum_{j\in N} \frac{\mathcal{F}\left(N, j, \left(\epsilon_{jk}^r\right)_{j,k\in N, r\in R}\right)}{r_j} \\ \geq\ & L\rho \sum_{j\in N\setminus\{i\}} \frac{\mathcal{F}\left(N, j, \left(\epsilon_{jk}^{\prime r}\right)_{j,k\in N, r\in R}\right)}{r_j} + \frac{\bar{z}_i L\rho}{\bar{r}_i}. \end{aligned}$$

Finally, we have

$$\begin{aligned} u_i' &\leq L\rho \sum_{j\in N\setminus\{i\}} \frac{\mathcal{F}\left(N\setminus\{i\}, j, \left(\epsilon_{jk}^r\right)_{j,k\in N\setminus\{i\}, r\in R}\right)}{r_j} \\ &\quad -L\rho \sum_{j\in N} \frac{\mathcal{F}\left(N, j, \left(\epsilon_{jk}^r\right)_{j,k\in N, r\in R}\right)}{r_j} \\ &= u_i^\star. \end{aligned}$$

This completes our proof. ∎

Then, we prove that our incentive protocol satisfies the second requirement.

Lemma 2: When our incentive protocol is used, it is strongly Pareto efficient when every node truthfully measures the link loss probabilities and faithfully follows the computed routing decision made by the basic opportunistic routing protocol.

Proof: We prove this lemma by contradiction. Suppose there is another strategy profile $s' \neq s^{\triangle}$, that can achieve a Pareto improvement over strategy profile $s^{\triangle}$ that every node truthfully measures the link loss probabilities and faithfully follows the computed routing decision made by the basic opportunistic routing protocol:

$$u_i(s') \geq u_i(s^{\triangle}) \geq 0, \forall i \in N \setminus \{S, D\},$$

with strict inequality for at least one player i. Consequently, the nodes have to truthfully report their received cryptographic tags to ensure that their neighbors can get payments in the forwarding process.

Given the other nodes' strategy profile s'_{-i}, a node i's utility is

$$\begin{aligned} u_i' &= L\rho \sum_{j\in N\setminus\{i\}} \frac{\mathcal{F}\left(N\setminus\{i\}, j, \left(\epsilon_{jk}'^r\right)_{j,k\in N\setminus\{i\}, r\in R}\right)}{r_j} \\ &\quad -L\rho \sum_{j\in N\setminus\{i\}} \frac{\mathcal{F}\left(N, j, \left(\epsilon_{jk}'^r\right)_{j,k\in N, r\in R}\right)}{r_j} \\ &\quad -\frac{\hat{z}_i L\rho}{\bar{r}_i}, \end{aligned}$$

where $\hat{z}_i$ is the expected number of transmissions needed to make each node $j < i$ receive $z_i'(1-\epsilon_{ij}^{\hat{r}_i})$ coded packets from i. Since the shortest multirate anypath algorithm computes the transmission bit rate that minimizes the overall distance to reach the destination [8], u_i' get maximized when the node i truthfully measures the link loss probabilities and faithfully follows the computed routing decision, *i.e.*, $s_i' = s_i^{\triangle}$. Similarly, we can get that given other nodes' strategy profile, every node i's best strategy is $s_i^{\triangle}$. Therefore, we have $s' = s^{\triangle}$. Here comes the contradiction. ∎

Next, the system performance optimality of the previous strongly Pareto efficient Nash equilibrium can be derived directly from the optimality of the the shortest multirate anypath algorithm.

Lemma 3: When our incentive protocol is used, optimal end-to-end throughput can be achieved in the strongly Pareto efficient Nash equilibrium that every node truthfully measures the link loss probabilities and faithfully follows the computed routing decision made by the basic opportunistic routing protocol.

Finally, we can conclude that:

Theorem 1: Our incentive protocol is a cooperation-optimal protocol.

V. Evaluations

We implement our incentive protocol based on MORE and carry out extensive experiments on the ORBIT wireless testbed [12].

A. Methodology

We randomly select 25 nodes from the ORBIT testbed. Figure 2 shows the locations of the nodes. Each node in the testbed is a PC equipped with Atheros AR5002X Mini PCI 802.11a/b/g wireless card. We allow the wireless interface card to operate in 802.11b/g ad hoc mode, which give 12 different transmission bit rates in total (*i.e.*, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps). We set MORE batch size at 32 packets, packet size at 1.5 kilobytes, and transmission cost at 1 unit cost per second.

Before running the experiments, we measure pair-wise loss probabilities at different transmission bit rates. The loss probabilities between nodes in the testbed at the transmission bit rates are set to values between 0.0 and 1.0.

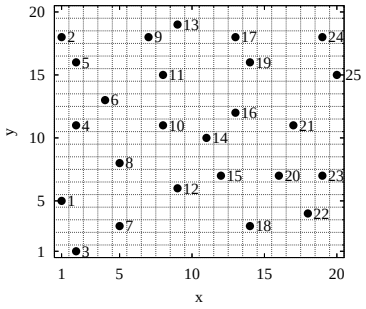

Fig. 2. Node topology.

Source-Destination Pairs: To evaluate the effects of node locations, we randomly select source-destination pairs in our experiments. After choosing a source-destination pair, we run a session between the pair of nodes for 30 seconds. The source is always backlogged.

Node Behavior: In our experiments, we compare two types of node behaviors:

- Following: Each node follows the protocol faithfully.
- Deviating: Selfish nodes may send incorrect numbers of probe messages, or report only parts of their received probe messages in the link loss probability measuring process; they may also deviate from the computed routing decision by transmitting incorrect

numbers of data packets, working on a transmission bit rate other than the optimal one, or reporting only parts of received cryptographic tags.

Metrics: We evaluate two metrics:

- Node utility: This metric reflects the impacts of a node's behavior on her own.
- End-to-end throughput: This metric reflects the impacts of our protocol on the performance of a wireless mesh network with selfish nodes.

B. Cheating Behavior and Node Utility

In our first set of experiments we demonstrate that, if a node deviates from our protocol, then its own utility cannot be increased. For this purpose, we randomly sample several nodes and record the utilities they obtain by following the protocols and by deviating randomly, respectively. The experiment is repeated 100 times with randomly selected source-destination pairs.

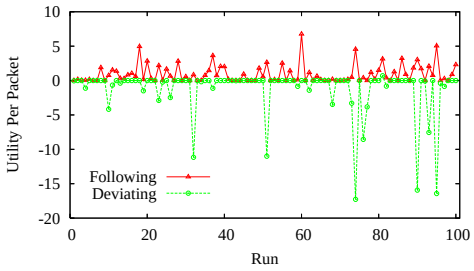

Fig. 3. Utilities obtained by an arbitrarily selected intermediate node when following and deviating. The figure demonstrates that the node can never benefit from cheating.

Figure 3 shows the utilities per packet of a randomly selected node if our protocol is used, when the other nodes follow the protocol faithfully. We can observe that the utility obtained by deviating is non-positive at most of times. More importantly, regardless of which cheating strategy is selected, the utility obtained by cheating is always no more than the utility obtained by following the protocol.

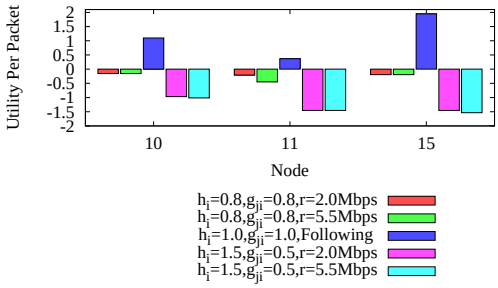

Fig. 4. Utilities of five nodes using five strategies. The transmission is from node 3 to node 24. The strategy of following is always the best.

Furthermore, results of utility comparison are shown in Figure 4. This figure shows three nodes' utilities when each of them uses one of five different strategies as shown in the figure. Here, h_i is the ratio between the number of probe messages node i sent and the number m of probe messages node i is expected to send, g_{ji} is the ratio of probe messages node i reports, and r is the transmission bit rate used by node i to forward packet. In the figure, by "Following" we mean that node i use its best rate computed by the basic opportunistic routing protocol. We can observe that the highest utility is always achieved by the following strategy only.

C. Impacts on End-to-End Throughput

Our second set of experiments are to demonstrate that our protocol can improve the end-to-end throughput of opportunistic routing when selfish nodes exist.

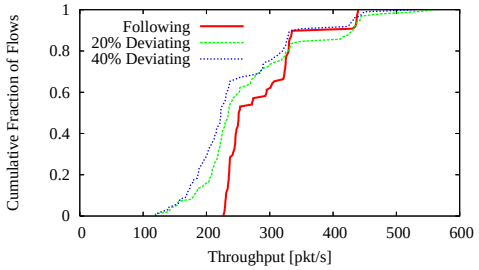

Fig. 5. CDF of the end-to-end throughput achieved with vs. without our protocol on 100 source-destination pairs. When the basic opportunistic routing protocol is used, 20% or 40% of the nodes cheat in the process of link loss probability measurement and deviate from the computed routing decision.

Figure 5 shows the cumulative distribution function (CDF) of the achieved throughput on 100 randomly selected source-destination pairs in the testbed. The figure shows the results when nodes faithfully follow the opportunistic routing and incentive protocol, or randomly deviate from the protocol. In the latter case, we consider two scenarios, in which 20% and 40% of the nodes deviate. We observe that the throughput of our protocol is significantly higher than those of the basic opportunistic routing protocol. Specifically, for the median case, our protocol achieves 7.0% (resp., 12.8%) higher throughput than the basic opportunistic routing protocol when 20% (resp., 40%) of the nodes deviate.

VI. Related Work

In this section, we briefly review related works on opportunistic routing and cooperation in wireless networks.

A. Opportunistic Routing in Wireless Networks

The concept of opportunistic routing was first developed by Biswas and Morris in the context of wireless mesh networks. They claimed that opportunistic routing can potentially increase the throughput and proposed an integrated routing and MAC protocol, named ExOR, to achieve the throughput gain [4]. To improve the system throughput, Chachulski *et al.* designed MORE [5], which combines random network coding and opportunistic routing to avoid transmission duplication. Lin *et al.* [6], [27] further improved the performance of opportunistic routing by transmitting a window of multiple batches simultaneously. Rozer *et al.* proposed an opportunistic adaptive routing protocol SOAR [7] to support multiple simultaneous flows in wireless mesh networks.

Laufer *et al.* [8] extended existing opportunistic routing protocols to better utilize wireless channels by exploiting the wireless radios' capability of working on multiple transmission bit rates specified by IEEE 802.11 protocols. Their results show that by incorporating multirate transmissions, the opportunistic routing protocol can exhibit much higher performance. Our protocol is an incentive-compatible extension for an multirate opportunistic routing protocol, such that the system performance can be guaranteed with the existence of selfish nodes.

B. Cooperation in Wireless Networks

Buttyan and Hubaux proposed the first credit-based system [28] in wireless ad-hoc networks in the Terminodes project. In [18], Zhong *et al.* proposed Sprite, which uses a central authority to collect receipts from forwarding nodes and determines charges and rewards based on the receipts. In [20], Ben Salem *et al.*proposed a charging and rewarding scheme based on symmetric cryptography to make selfish nodes to collaborate with each other. In [29], Jakobsson *et al.* proposed a micro-payment scheme to encourage collaboration in packet forwarding for multi-hop cellular networks.

In [30], Anderegg and Eidenbenz studied the problem of cooperation in the traditional routing. They applied the VCG mechanism to design a routing protocol for a wireless network with selfish nodes. Then, Zhong *et al.* [17] proposed Corsac to integrate VCG and cryptographic technique to solve the combined problem of routing and packet forwarding. Later, OURS was proposed by Wang *et al.* [19]. It has much smaller over-payments than VCG-based solutions. Recently, Wu *et al.* [9] designed protocols to stimulate mesh nodes' incentives to truthfully measure the link loss probabilities and follow MORE-based opportunistic routing protocols. However, Wu *et al.*'s work cannot guarantee the incentive-compatibility when multiple transmission bit rates are available for transmitting a packet.

VII. Conclusion and Future Work

In this paper, we present a practical incentive protocol to solve the problem of selfish behavior in multirate opportunistic routing. Our protocol achieve cooperation-optimality in multirate opportunistic routing, *i.e.*, when everyone follows the routing and incentive protocol, the system performance gets optimized and each mesh node gets its payoff maximized. We integrate our incentive protocol with MORE in a Linux implementation and demonstrate on the ORBIT wireless testbed that (a) cheating decreases a node's utility under our protocol and (b) incentive can substantially improve overall network throughput when selfish nodes exist.

References

[1] D. Aguayo, J. Bicket, S. Biswas, G. Judd, and R. Morris, "Link-level measurements from an 802.11b mesh network," in *SIGCOMM'04*, Portlan, Oregon, Aug. 2004.

[2] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Communications Magazine*, vol. 43, no. 9, 2005.

[3] M. Campista, P. Esposito, I. Moraes, L. H. Costa, O. C. Duarte, D. Passos, C. V. de Albuquerque D. C. Saade, and M. Rubinstein, "Routing metrics and protocols for wireless mesh networks," *IEEE Network*, no. 1, pp. 6–12, Jan.-Feb. 2008.

[4] S. Biswas and R. Morris, "Opportunistic routing in multi-hop wireless networks," in *SIGCOMM'05*, Philadelphia, PA, Aug. 2005.

[5] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading structure for randomness in wireless opportunistic routing," in *SIGCOMM'07*, Kyoto, Japan, Aug. 2007.

[6] Y. Lin, B. Li, and B. Liang, "CodeOR: Opportunistic routing in wireless mesh networks with segmented network coding," in *ICNP'08*, Orlando, FL, Oct. 2008.

[7] E. Rozner, J. Seshadri, Y. A. Mehta, and L. Qiu, "Soar: Simple opportunistic adaptive routing protocol for wireless mesh networks," *IEEE Transactions on Mobile Computing*, vol. 8, pp. 1622–1635, 2009.

[8] R. Laufer, H. Dubois-Ferri'ere, and L. Kleinrock, "Multirate anypath routing in wireless mesh networks," in *INFOCOM'09*, Apr. 2009.

[9] F. Wu, T. Chen, S. Zhong, L. E. Li, and Y. R. Yang, "Incentive-compatible opportunistic routing for wireless networks," in *MobiCom'08*, Sep. 2008.

[10] E. Adar and B. A. Huberman, "Free riding on gnutella," *First Monday*, no. 10, Oct. 2000.

[11] W. E. Bluhm, *Society of Actuaries 50th Anniversary Monograph*. Schaumburg, Ill., Society of Actuaries, etc., 1999, ch. V: Cumulative Anti-Selection Theory.

[12] Rutgers ORBIT project team, "http://www.orbit-lab.org."

[13] D. S. J. D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *MobiCom'03*, Sep. 2003.

[14] Z. Zhong, J. Wang, S. Nelakuditi, and G.-H. Lu, "On selection of candidates for opportunistic anypath forwarding," *ACM SIGMOBILE Mobile Comp. and Comm. Review*, vol. 10, no. 4, pp. 1–2, Oct. 2006.

[15] Dubois-Ferriere, "Anypath routing," Ph.D. dissertation, Ecole Polytechnique Federale de Lausanne, Lausanne, Switzerland, Nov. 2006.

[16] W. Wang, X.-Y. Li, and Y. Wang, "Truthful multicast in selfish wireless networks," in *MobiCom'04*, Sep. 2004.

[17] S. Zhong, L. E. Li, Y. G. Liu, and Y. R. Yang, "On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks–an integrated approach using game theoretical and cryptographic techniques," in *MobiCom'05*, Sep. 2005.

[18] S. Zhong, J. Chen, and Y. R. Yang, "Sprite, a simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *INFOCOM'03*, Apr. 2003.

[19] W. Wang, S. Eidenbez, Y. Wang, and X.-Y. Li, "Ours–optimal unicast routing systems in non-cooperative wireless networks," in *MobiCom'06*, Sep. 2006.

[20] N. Ben Salem, L. Buttyan, J. P. Hubaux, and M. Jakobsson, "A charging and rewarding scheme for packet forwarding in multi-hop cellular networks," in *MobiHoc'03*, Jun. 2003.

[21] S. Eidenbenz, G. Resta, and P. Santi, "Commit: A sender-centric truthful and energy-efficient routing protocol for ad hoc networks with selfish nodes," in *IPDPS'05*, Apr. 2005.

[22] S. Zhong and F. Wu, "On designing collusion-resistant routing schemes for non-cooperative wireless ad hoc networks," in *MobiCom'07*, Sep. 2007.

[23] M. J. Osborne and A. Rubenstein, *A Course in Game Theory*. MIT Press, 1994.

[24] W. Du, J. Deng, Y. S. Han, and P. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in *CCS'03*, 2003.

[25] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *CCS'03*, 2003.

[26] VMAC, "Vmac: Message authentication code using universal hashing," *http://www.fastcrypto.org/vmac/draft-krovetz-vmac-01.txt*, Mar. 2010.

[27] Y. Lin, B. Liang, and B. Li, "SlideOR: oline opportunistic network coding in wireless mesh networks," in *INFOCOM'10*, Mar. 2010.

[28] L. Buttyan and J. P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in *MobiHoc'00*, Boston, Massachusetts, Aug. 2000.

[29] M. Jakobsson, J. P. Hubaux, and L. Buttyan, "A micro-payment scheme encouraging collaboration in multi-hop cellular networks," in *FC'03*, Gosier, Guadeloupe, Jan. 2003.

[30] L. Anderegg and S. Eidenbenz, "Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," in *MobiCom'03*, Sep. 2003.