

COMO: A Game-Theoretic Approach for Joint Multirate Opportunistic Routing and Forwarding in Non-Cooperative Wireless Networks

Fan Wu, *Member, IEEE*, Kai Gong, Tianrong Zhang, Guihai Chen, *Member, IEEE*, and Chunming Qiao, *Fellow, IEEE*

Abstract—Multirate opportunistic routing was proposed to achieve high throughput by exploiting multi-user diversity and transmission rate diversity in wireless networks. However, the performance of multirate opportunistic routing still cannot be guaranteed when participating nodes are contributed by different parties and thus have selfish behaviors. In this paper, we present the first Cooperation-Optimal protocol for Multirate Opportunistic routing and forwarding, namely COMO, which guarantee the faithfulness of each player, and thus achieve the social efficiency and strongly Pareto efficient Nash equilibrium with the faithfulness as a given property. Here, social efficiency means that the end-to-end throughput should be maximized, while in a strongly Pareto efficient Nash equilibrium, no one can improve her utility without decreasing the utility of at least one other player. We not only rigorously prove the game-theoretic properties of our incentive protocol, but also extensively evaluate its performance on the 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 with a low communication overhead.

Index Terms—Wireless Network, Opportunistic Routing, Game Theory.

1 INTRODUCTION

Wireless networks have emerged as an efficient alternative to deploy broadband network infrastructures in local communities at low cost [2], [3]. A major challenge, which restricts the wireless 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 networks, especially in urban environments with many interference sources [9]. To overcome the problem caused by the lossy and dynamic wireless links, opportunistic routing [6], [10], [23], [32] 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 allows any node who overheard the packet to participate in packet forwarding. Recently, Laufer *et al.* [22] 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 par-

ticipating mesh nodes are contributed by different parties and thus have selfish behaviors [40]. In this paper, we study the performance of multirate opportunistic routing in wireless networks, where the participating nodes are contributed by different parties. Our objective is to ensure good performance even if the nodes have selfish behaviors. Similar to other distributed autonomous systems, wireless networks suffer common incentive problems, such as the free-rider problem, where only a small part of participants contribute their resources [1], and the adverse selection problem, where participants do not truthfully reveal their link states and thus prevent the routing protocol from finding the optimal routing strategy [7]. 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 networks.

Many existing opportunistic routing protocols need to collect the link loss probabilities to make efficient routing decision. Since the link loss probabilities are private information of the 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.* [40] studied the problem of selfish behavior in opportunistic routing, and proposed practical solutions to stimulate the nodes' incentives to truthfully measure the link loss probabilities and follow MORE [10]-based opportunistic routing protocols. However, as shown in Section 4, Wu *et al.*'s work cannot guarantee the incentive-compatibility of the opportunistic routing protocol, when the nodes can employ multiple transmission bit rates to transmit a packet.

- F. Wu, K. Gong, T. Zhang, and G. Chen are with the Shanghai Key Laboratory of Scalable Computing and Systems, Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. E-mails: {wu-fan, wayngong, tzt1211, gchen}@sjtu.edu.cn
- C. Qiao is with the Department of Computer Science and Engineering, State University of New York at Buffalo, USA. E-mail: qiao@buffalo.edu

In this paper, we present the first Cooperation-Optimal protocol for Multirate Opportunistic routing and forwarding, namely COMO, which guarantee the faithfulness of each player, and thus achieve the social efficiency and strongly Pareto efficient Nash equilibrium with the faithfulness as a given property. Here, social efficiency means that the end-to-end throughput should be maximized, while in a strongly Pareto efficient Nash equilibrium, no one can improve her utility without decreasing the utility of at least one other player. Our contributions are listed as follows.

- We are the first to study the incentive problem of multirate opportunistic routing and to provide a practical solution.
- We show that the closest related existing work by Wu *et al.* [40], cannot prevent the nodes' misbehavior in opportunistic routing when the nodes can work on multiple transmission bit rates.
- We present a practical incentive protocol COMO 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 node gets its payoff maximized. Specifically, we incorporate probe messages, which 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 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 COMO on the ORBIT wireless testbed [33]. Our evaluation results show that our incentive protocol can prevent participating nodes' misbehavior and guarantee the optimal performance of the system with a low communication overhead.

The rest of the paper is organized as follows. In Section 2, we review the related works. In Section 3, we give technical preliminaries on opportunistic routing, and game theoretic model of multirate opportunistic routing. In Section 4, we show the infeasibility of existing works. In Section 5, we present our incentive protocol COMO, and prove its cooperation optimality. In Section 6, we report the evaluation results on ORBIT wireless testbed. Finally, we conclude the paper and point out potential future directions to improve the work in Section 7.

2 RELATED WORKS

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

2.1 Opportunistic Routing in Wireless Networks

Opportunistic routing belongs to cooperative diversity techniques (e.g. [6], [20], [21], [27]) which take advantage of broadcast transmissions to send information through multiple concurrent relays. Nodes can combine information from multiple signals so that they can make best decisions of routing or forwarding. As an example, protocols in [20] fully exploit spatial diversity in the channel by allowing all nodes that

overheard a transmission to simultaneously forward the signal. Another example is the protocol in [6], which optimizes the choice of forwarder from multiple receivers by deferring the decision after the transmission.

A protocol of opportunistic routing was 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 [6]. To improve the system throughput, Chachulski *et al.* designed MORE [10], which combines random network coding and opportunistic routing to avoid transmission duplication. Lin *et al.* [23], [24] further improved the performance of opportunistic routing by transmitting a window of multiple batches simultaneously. Radunovic *et al.* [29] introduced credit to realize flow control. Rozer *et al.* proposed an opportunistic adaptive routing protocol SOAR [32] to support multiple simultaneous flows in wireless networks. Koutsonikolas *et al.* [19] improved network coding based opportunistic routing protocols with a novel cumulative coded acknowledgment scheme. Katti *et al.* [18] make use of physical layer information to exploit symbol level multi-user diversity. They further proposed SourceSync [30] to synchronize senders to achieve combined signals which lowers the packet error rate. Han *et al.* proposed O3 [15], which combines inter-flow coding and rate limiting to improve the end-to-end throughput. Wang *et al.* presented CORMAN [39], which is extended from ExOR and works in mobile ad hoc networks. In [41], [43], the authors extended the opportunistic routing to multi-channel, multi-radio wireless networks. Besides, Rozner *et al.* [31] developed an optimization framework to exploit communication opportunities arising by chance.

Laufer *et al.* [22] 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. Unfortunately, none of the existing works on incentives can be applied to multirate opportunistic routing. Our protocol is an incentive extension for a multirate opportunistic routing protocol, such that the system performance can be guaranteed with the existence of selfish nodes.

2.2 Cooperation in Wireless Networks

Buttayan and Hubaux proposed the first credit-based system [8] in wireless ad-hoc networks in the Terminodes project. In [8], they proposed the usage of nuglets, a virtual currency, to pay nodes for forwarding others' packets. Motivated by the nuglet, several other credit-based systems were proposed to stimulate cooperation in packet forwarding. In [46], 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 [5], Ben Salem *et al.* proposed a charging and rewarding scheme based on symmetric cryptography to make selfish nodes collaborate with each other. In [17], Jakobsson *et al.* proposed a micro-payment scheme

to encourage collaboration in packet forwarding for multi-hop cellular networks. Yao and Zhong showed the first cheat-proof scheme for cooperative relay in cognitive radio networks [42].

In [4], Andereg 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.* [45] 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.* [37]. It has much smaller over-payments than VCG-based solutions. Then Zhong and Wu [47] studied collusion resistance for incentive-compatible routing. Dice [44] considers efficiency and fairness of resource allocation in the network coding based opportunistic routing protocols. Recently, Wu *et al.* [40] designed protocols to stimulate the nodes' incentives to truthfully measure the link loss probabilities and follow MORE-based opportunistic routing protocols. INPAC [11] is complimentary to Wu *et al.*'s work, from the perspective of packet forwarding process. Huang and Krishnamurthy [16] applied the VCG mechanism in opportunistic scheduling. However, their works cannot guarantee the incentive-compatibility when multiple transmission bit rates are available for transmitting packets.

3 TECHNICAL PRELIMINARIES

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

3.1 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 [40], we focus on a class of basic opportunistic routing protocols (*e.g.*, [10]). 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 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 a transmission rate r_i and

the expected number of transmissions z_i for each node $i \in N$:

$$(r_i, z_i) = \mathcal{F}(N, S, D, i, \{(j, k, r, \epsilon_{jk}^r) | j, k \in N, r \in R\}, \{(j, d_j, r_j) | j \in N\}), \quad (1)$$

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 achieves 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 limitations of space, we omit the details of the basic opportunistic routing protocol. Please refer to [10], [40] for details.

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.* [12] 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 EAX metric [48], which captures the expected number of anypath transmissions. To support multiple transmission bit rates provided by IEEE 802.11 protocols, Laufer *et al.* [22] introduced the expected anypath transmission time (EATT) metric.

Although most of the instances of the basic opportunistic routing protocol are designed based on ETX/EAX distance, they can be easily adapted to EATT distance. Experiment results show that when multirate is used, EATT always achieves equal or higher performance than ETX/EAX [22]. 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 [22]:

$$(d_i, r_i) = \mathcal{M}(N, D, i, \{(k, l, r, \epsilon_{kl}^r) | k, l \in N, r \in R\}). \quad (2)$$

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

$$(r_i, z_i) = \mathcal{F}(N, S, D, i, \{(j, k, r, \epsilon_{jk}^r) | j, k \in N, r \in R\}, \{(j, \mathcal{M}(N, D, i, \{(k, l, r, \epsilon_{kl}^r) | k, l \in N, r \in R\})) | j \in N\}). \quad (3)$$

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:

$$(r_i, z_i) = \mathcal{F}(N, i, (\epsilon_{jk}^r)_{j, k \in N, r \in R}). \quad (4)$$

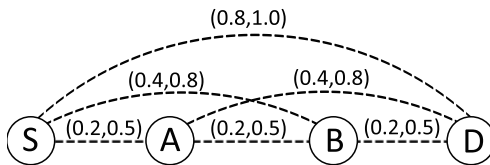


Fig. 1. An example to illustrate the impact of misbehavior in basic opportunistic routing. There is a session from source S to destination D , with two intermediate nodes A and B . True link loss probabilities are shown near the links. The available transmission bit rates are r and $2r$. Here $(0.2, 0.5)$ 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.

3.2 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.

3.3 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 [5], [14], [37], [38], [45]–[47], 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

$$u_i = u_i((s_j)_{j \in N}). \quad (5)$$

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 multirate opportunistic routing, the utility u_i is expressed as the difference between payment p_i and cost c_i for forwarding data packets:

$$u_i = p_i - c_i = p_i - \frac{z_i L \rho}{r_i}. \quad (6)$$

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 multirate opportunistic routing, we now recall a well-known solution concept, namely *Nash equilibrium* (NE), in game theory.

Definition 1 (Nash equilibrium [28]): A profile s^* of all players' strategies is a Nash equilibrium, if for all $i \in N$, for all strategy $s_i \neq s_i^*$ of player i , we have

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*). \quad (7)$$

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

Definition 2 (strong Pareto optimality [28]): A strategy profile s^Δ of all players is strongly Pareto efficient, if there does not exist a strategy profile $s' \neq s^\Delta$, such that

$$u_i(s') \geq u_i(s^\Delta), \forall i \in N, \quad (8)$$

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

can achieve a socially efficient and strongly Pareto efficient Nash equilibrium, when every player faithfully follows the protocol.

We note that Zhong *et al.* [45] proposed a similar concept of forwarding-dominant protocol. Unfortunately, a negative result was shown that there does not exist a forwarding-dominant protocol even with deterministic routing protocols in ad-hoc networks. Then, they turned to an alternative solution concept, which is also called cooperation-optimal protocol. However, our cooperation-optimal protocol defined in this paper differs from that of [45] in two aspects. First, social efficiency considered in these two solution concepts are different. Social efficiency considered in [45] is minimizing the energy consumption on an end-to-end route. However, minimized energy consumption does not necessarily maximize the end-to-end throughput. Therefore, we consider the social efficiency on end-to-end throughput in this manuscript instead. Second, the solution concept of cooperation-optimal protocol in [45] is based on extensive game and subgame perfect equilibrium, while our definition is based on strategic game and strongly Pareto efficient Nash equilibrium. Here strongly Pareto efficient Nash equilibrium is stronger than subgame perfect equilibrium in game theory.

N	set of nodes in the wireless network
E	set of directed virtual links
R	set of available transmission bit rates
S	source node
D	destination node
ϵ_{ij}^r	link loss probability of directed virtual link $(i, j) \in E$ at transmission rate $r \in R$
r_i	transmission rate of player $i \in N$
z_i	expected number of transmissions of player $i \in N$
d_i	node i 's distance to the destination node under the path metric
ρ	cost of transmitting per second
c_i	expected transmission cost on node $i \in N$
L	packet length
s_i	strategy of player $i \in N$
s_{-i}	strategy profile of the players other than player $i \in N$
s, s', s^*, s^Δ	strategy profile of all players
p_i	payment to player $i \in N$
u_i	utility of player $i \in N$

TABLE 1
Variables

For convenience, we use Table 1 to illustrate important variables used in our scheme.

4 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.* [40]. 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 select 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 be the most efficient routing decision. So it is important to find an incentive scheme that stimulates nodes' incentive to honestly participate in the routing despite multirate opportunistic transmissions.

Without losing generality, we assume

$$r^j < r^k, \forall j < k, 1 \leq j, k \leq |R|. \quad (9)$$

According to Wu *et al.*'s scheme, we have the transmission rate r_i and the expected number of transmissions $z_i^{r_i}$ at rate r_i for each node $i \in N$ as follows.

$$r_i = r^1, \quad (10)$$

$$z_i^{r_i} = \mathcal{F}(N, i, \{(j, k, \epsilon_{j,k}^{r_i}) | j, k \in N\}). \quad (11)$$

Their scheme requires each node i to send an auxiliary traffic of size $z_{i,j}$ to each of its neighbor j :

$$z_{i,j} = \frac{\alpha(1 - \epsilon_{i,j}^{r_i})^2}{2}. \quad (12)$$

Then, a payment p_i to the node i is determined as

$$p_i = \frac{\rho}{r_i} \left(z_i^{r_i} L + \sum_{(i,j) \in E} \alpha(1 - \epsilon_{i,j}^{r_i}) \right), \quad (13)$$

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

$$\begin{aligned} u_i(s_i^*, s_{-i}) &= p_i - c_i \\ &= \frac{\alpha\rho}{2r_i} \sum_{(i,j) \in E} (1 - \epsilon_{i,j}^{r_i}) \\ &= \frac{\alpha\rho}{2r^1} \sum_{(i,j) \in E} (1 - \epsilon_{i,j}^{r^1}). \end{aligned} \quad (14)$$

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

$$\exists i \in N, \exists r^b > r^1, \forall j \in N \setminus \{i\}, r^b(1 - \epsilon_{ij}^{r^b}) > r^1(1 - \epsilon_{ij}^{r^1}). \quad (15)$$

Thus the utility of node i becomes:

$$\begin{aligned}
 & u'_i(s', s_{-i}) \\
 = & p_i - c'_i \\
 = & p_i - \frac{\rho}{r^b} \left(z_i^{r^1} L + \sum_{j \in N \setminus \{i\}} \frac{\alpha(1 - \epsilon_{i,j}^{r^1})^2}{2(1 - \epsilon_{i,j}^{r^p})} \right) \\
 = & p_i - \frac{\rho z_i^{r^1} L}{r^b} - \frac{\alpha \rho}{2} \sum_{j \in N \setminus \{i\}} \frac{(1 - \epsilon_{i,j}^{r^1})^2}{r^p(1 - \epsilon_{i,j}^{r^b})} \\
 > & p_i - \frac{\rho z_i^{r^1} L}{r^1} - \frac{\alpha \rho}{2} \sum_{j \in N \setminus \{i\}} \frac{(1 - \epsilon_{i,j}^{r^1})^2}{r^1(1 - \epsilon_{i,j}^{r^1})} \\
 = & p_i - \frac{\rho}{r^1} \left(z_i^{r^1} L + \sum_{j \in N \setminus \{i\}} \frac{\alpha(1 - \epsilon_{i,j}^{r^1})^2}{2(1 - \epsilon_{i,j}^{r^1})} \right) \\
 = & p_i - c_i \\
 = & u_i(s_i^*, s_{-i}) \tag{16}
 \end{aligned}$$

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 rates. Consequently, it is important to find an incentive scheme that stimulates nodes' incentive to honestly participate in the routing despite multirate opportunistic transmissions.

5 INCENTIVE PROTOCOL

In this section, we present our practical incentive protocol COMO that achieves cooperation-optimality in multirate opportunistic routing, *i.e.*, it guarantees the faithfulness of each player, and thus achieve the social efficiency and strongly Pareto efficient Nash equilibrium with the faithfulness as a given property. 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 nodes cannot benefit by deviating from the protocol.

5.1 Protocol Details

The design of COMO is composed of three parts, including link loss probability measurement, payment cap computation, and payment determination.

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 results in inefficient routing decision.

We assume that there exists a key distribution scheme (*i.e.*, [13], [25]) in the wireless network, such that there is a secret key $key(S, i)$ established between the source node S and every intermediate forwarding node $i \in N \setminus \{S, D\}$ before or during the routing initialization phase.

When a session from source node S to destination node D initializes, each intermediate node $i \in N \setminus \{S, D\}$ 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 follows:

$$\langle PROBE, i, r, q, MAC_{key(S,i)}(PROBE, i, r, q) \rangle, \tag{17}$$

where q is a unique sequence number, and MAC is a keyed cryptographic Message Authentication Code function (*e.g.*, UMAC [35] and VMAC [36]). $MAC_{key(S,i)}()$ 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

$$\epsilon_{ij}^{rr} = 1 - \frac{m_{ij}^r}{m}. \tag{18}$$

Here, we use ϵ_{ij}^{rr} 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:

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

$$\begin{aligned}
 \hat{p}_i = & L\rho \sum_{j \in N \setminus \{i\}} \frac{\mathcal{F}\left(N \setminus \{i\}, j, \left(\epsilon_{jk}^{rr}\right)_{j,k \in N \setminus \{i\}, r \in R}\right)}{r_j} \\
 & - L\rho \sum_{j \in N \setminus \{i\}} \frac{\mathcal{F}\left(N, j, \left(\epsilon_{jk}^{rr}\right)_{j,k \in N, r \in R}\right)}{r_j}. \tag{19}
 \end{aligned}$$

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.

We note that the payment cap indicates the maximal amount of payment a node can gain through faithful participation. However, the final payment to the node also depends on the number of packets the node forwards.

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 packet it forwards. The format of cryptographic tag is similar to that of the probe message, except the transmission bit rate field r :

$$\langle DATA, i, q, MAC_{key(S,i)}(DATA, i, q) \rangle. \quad (20)$$

Then every intermediate node $i \in N \setminus \{S, D\}$ and the destination node D reports the received 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:

$$p_i = \eta_i^\Delta \eta_i^\nabla \hat{p}_i, \quad (21)$$

where

$$\eta_i^\Delta = \frac{\sum_{j>i} \min(f_{ji}, z_j (1 - \epsilon_{ji}^{r_j}))}{\sum_{j>i} z_j (1 - \epsilon_{ji}^{r_j})}, \quad (22)$$

$$\eta_i^\nabla = \left(\min \left(\min_{j<i} \left(\frac{f_{ij}}{z_i (1 - \epsilon_{ij}^{r_i})} \right), 1 \right) \right) ? 1 : 0. \quad (23)$$

Here, η_i^Δ calculates the sum of the normalized ratio of packets received by node i from its upstream nodes. If $\min \left(\min_{j<i} \left(\frac{f_{ij}}{z_i (1 - \epsilon_{ij}^{r_i})} \right), 1 \right) = 1$, $\eta_i^\nabla = 1$, else $\eta_i^\nabla = 0$. 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.

5.2 Analysis

In this section, we prove that COMO 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 requirement 1, the utility of a node i is

$$u_i^* = L\rho \sum_{j \in N \setminus \{i\}} \frac{\mathcal{F} \left(N \setminus \{i\}, j, \left(\epsilon_{jk}^r \right)_{j,k \in N \setminus \{i\}, r \in R} \right)}{r_j} - L\rho \sum_{j \in N} \frac{\mathcal{F} \left(N, j, \left(\epsilon_{jk}^r \right)_{j,k \in N, r \in R} \right)}{r_j}. \quad (24)$$

Lemma 1: When COMO 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

$$\epsilon_{ij}^{r_i} = 1 - h_i^r (1 - \epsilon_{ij}^r), \forall j \in N \setminus \{i\}. \quad (25)$$

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

$$\epsilon_{ji}^{r_j} = 1 - g_{ji}^r (1 - \epsilon_{ji}^r), \forall j \in N \setminus \{i\}. \quad (26)$$

Then node i 's payment cap is

$$\hat{p}'_i = L\rho \sum_{j \in N \setminus \{i\}} \frac{\mathcal{F} \left(N \setminus \{i\}, j, \left(\epsilon_{jk}^r \right)_{j,k \in N \setminus \{i\}, r \in R} \right)}{r_j} - L\rho \sum_{j \in N \setminus \{i\}} \frac{\mathcal{F} \left(N, j, \left(\epsilon_{jk}^r \right)_{j,k \in N, r \in R} \right)}{r_j}. \quad (27)$$

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 is

$$p'_i = \eta_i'^\Delta \eta_i'^\nabla \hat{p}'_i. \quad (28)$$

The node i 's utility is

$$u'_i = p'_i - c'_i = \eta_i'^\Delta \eta_i'^\nabla \hat{p}'_i - \frac{\bar{z}_i L\rho}{\bar{r}_i}. \quad (29)$$

Considering that

$$\begin{aligned}
 \eta_i^{\Delta} &= \frac{\sum_{j>i} \min \left(f'_{ji}, z'_j(1 - \epsilon_{ji}^{r'_j}) \right)}{\sum_{j>i} z'_j(1 - \epsilon_{ji}^{r'_j})} \\
 &= \frac{\sum_{j>i} \min \left(z'_j(1 - \epsilon_{ji})b_{ji}, z'_j(1 - \epsilon_{ji}^{r'_j}) \right)}{\sum_{j>i} z'_j(1 - \epsilon_{ji}^{r'_j})} \\
 &= \frac{\sum_{j>i} \min \left(z'_j(1 - \epsilon_{ji})b_{ji}, z'_j(1 - \epsilon_{ji})g_{ji} \right)}{\sum_{j>i} z'_j(1 - \epsilon_{ji})g_{ji}} \\
 &\leq \frac{\sum_{j>i} \min \left(z'_j(1 - \epsilon_{ji}), z'_j(1 - \epsilon_{ji})g_{ji} \right)}{\sum_{j>i} z'_j(1 - \epsilon_{ji})g_{ji}} \\
 &= 1
 \end{aligned} \tag{30}$$

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

$$u'_i \leq \eta_i^{\nabla} \hat{p}'_i - \frac{\bar{z}_i L \rho}{\bar{r}_i}. \tag{31}$$

Since only when

$$\bar{z}_i(1 - \epsilon_{ij}^{\bar{r}_i}) \geq z'_i(1 - \epsilon_{ij}^{r'_i})h_i^{r'_i}, \forall j < i, \tag{32}$$

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

$$\bar{z}_i = \max_{j < i} \left(\frac{z'_i(1 - \epsilon_{ij}^{r'_i})h_i^{r'_i}}{1 - \epsilon_{ij}^{\bar{r}_i}} \right). \tag{33}$$

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

$$\begin{aligned}
 u'_i &= L\rho \sum_{j \in N \setminus \{i\}} \frac{\mathcal{F} \left(N \setminus \{i\}, j, \left(\epsilon_{jk}^r \right)_{j,k \in N \setminus \{i\}, r \in R} \right)}{r_j} \\
 &\quad - L\rho \sum_{j \in N \setminus \{i\}} \frac{\mathcal{F} \left(N, j, \left(\epsilon_{jk}^r \right)_{j,k \in N, r \in R} \right)}{r_j} \\
 &\quad - \frac{\bar{z}_i L \rho}{\bar{r}_i}.
 \end{aligned} \tag{34}$$

Since the shortest multirate anypath algorithm computes the transmission bit rate that minimizes the overall distance to reach the destination [22], we have

$$\begin{aligned}
 &L\rho \sum_{j \in N} \frac{\mathcal{F} \left(N, j, \left(\epsilon_{jk}^r \right)_{j,k \in N, r \in R} \right)}{r_j} \\
 &\geq L\rho \sum_{j \in N \setminus \{i\}} \frac{\mathcal{F} \left(N, j, \left(\epsilon_{jk}^r \right)_{j,k \in N, r \in R} \right)}{r_j} + \frac{\bar{z}_i L \rho}{\bar{r}_i}.
 \end{aligned} \tag{35}$$

Finally, we have

$$\begin{aligned}
 u'_i &\leq L\rho \sum_{j \in N \setminus \{i\}} \frac{\mathcal{F} \left(N \setminus \{i\}, j, \left(\epsilon_{jk}^r \right)_{j,k \in N \setminus \{i\}, r \in R} \right)}{r_j} \\
 &\quad - L\rho \sum_{j \in N} \frac{\mathcal{F} \left(N, j, \left(\epsilon_{jk}^r \right)_{j,k \in N, r \in R} \right)}{r_j} \\
 &= u_i^*.
 \end{aligned} \tag{36}$$

This completes our proof. \square

Then, we prove that COMO satisfies the second requirement.

Lemma 2: When COMO 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 $s' \neq s^\Delta$, that can achieve a Pareto improvement over strategy profile s^Δ that every node truthfully measures the link loss probabilities and faithfully follows the computed routing decision made by the basic opportunistic routing protocol:

$$u_i(s') \geq u_i(s^\Delta) \geq 0, \forall i \in N \setminus \{S, D\}, \tag{37}$$

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

$$\begin{aligned}
 u'_i &= L\rho \sum_{j \in N \setminus \{i\}} \frac{\mathcal{F} \left(N \setminus \{i\}, j, \left(\epsilon_{jk}^r \right)_{j,k \in N \setminus \{i\}, r \in R} \right)}{r_j} \\
 &\quad - L\rho \sum_{j \in N \setminus \{i\}} \frac{\mathcal{F} \left(N, j, \left(\epsilon_{jk}^r \right)_{j,k \in N, r \in R} \right)}{r_j} \\
 &\quad - \frac{\hat{z}_i L \rho}{\bar{r}_i},
 \end{aligned} \tag{38}$$

where \hat{z}_i is the expected number of transmissions needed to make each node $j < i$ receive $z'_i(1 - \epsilon_{ij}^{r'_i})$ coded packets from i . Since the shortest multirate anypath algorithm computes the transmission bit rate that minimizes the overall distance to reach the destination [22], u'_i get maximized when the node i truthfully measures the link loss probabilities and faithfully follows the computed routing decision, *i.e.*, $s'_i = s_i^\Delta$. Similarly, we can get that given other nodes' strategy profile, every node i 's best strategy is s_i^Δ . Therefore, we have $s' = s^\Delta$. Here comes the contradiction. \square

Although the ‘‘secondary’’ shortest multirate anypath (*i.e.*, the path without node i 's participation) is considered as a reference to determine the payment cap of the node, the ‘‘primary’’ shortest multirate anypath (*i.e.*, the path considering all the nodes) is selected to forward packets. Furthermore, according to [22], the ‘‘primary’’ shortest multirate anypath is proven to be optimal in terms of end-to-end throughput. Therefore, COMO incentivize the nodes to faithfully participate, and thus also achieves optimal end-to-end throughput. Then, we have the following lemma.

Lemma 3: When COMO 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: COMO is a cooperation-optimal protocol. \square

6 EVALUATIONS

We implement COMO based on MORE and perform extensive experiments on the ORBIT wireless testbed [33]. Our experiments have two objectives. One is to verify that COMO can prevent nodes' selfish behavior. The other is to evaluate the impact of COMO on the performance of multirate opportunistic routing in a wireless mesh network with selfish nodes.

6.1 Methodology

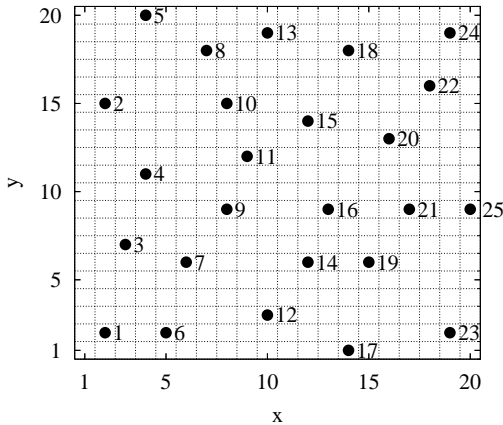


Fig. 2. Node topology.

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). Each node in the testbed runs Linux Debian with kernel v2.6.22, MadWifi v0.9.3.3 [26], Click v1.6.0 [34], and the MORE package [10]. 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.

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 multirate opportunistic routing in a wireless network with selfish nodes.

6.2 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 protocol and by deviating randomly, respectively. The experiment is repeated 100 times with randomly selected source-destination pairs.

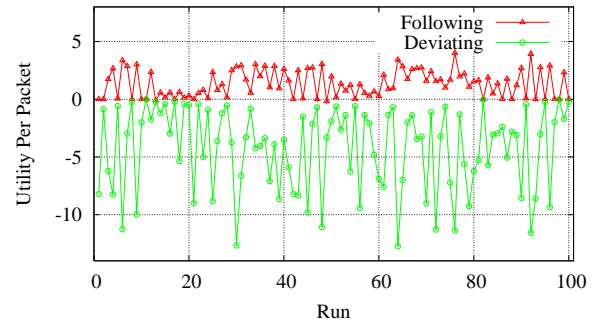


Fig. 3. Utilities obtained by an arbitrarily selected intermediate node when following and deviating. The figure demonstrates that the node can never benefit from cheating.

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.

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 of probe messages node i is expected to send, g_{ji} is the ratio of the number of probe messages node i receives and the number 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. This figure shows the utilities of node 11, 15, and 16, when they use 5 different strategies. We can observe that the highest utility is always achieved by the following strategy only.

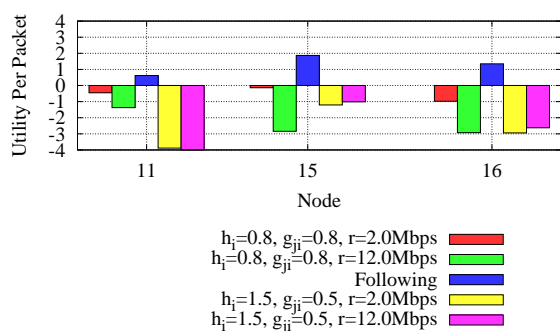


Fig. 4. Utilities of 3 nodes using 5 different strategies. The transmission is from node 3 to node 24. The strategy of following is always the best.

6.3 Impacts on End-to-End Throughput

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

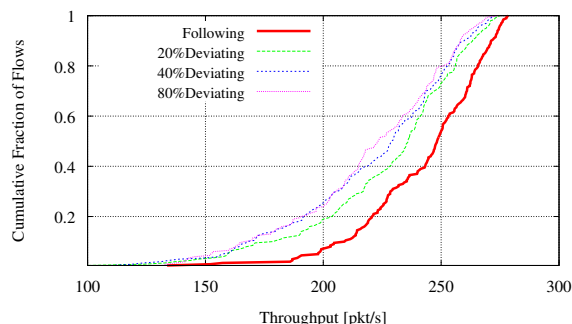


Fig. 5. CDF of the end-to-end throughput achieved with vs. without COMO on 200 source-destination pairs. When the basic opportunistic routing protocol is used, 20%, 40%, and 80% nodes cheat in the process of link loss probability measurement and deviate from the computed routing decision.

Figure 5 shows the cumulative distribution function (CDF) of the achieved throughput on 200 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 three scenarios, in which 20%, 40%, and 80% nodes deviate. We observe that the line representing “Following” is always the rightmost one. Therefore, the throughput achieved, when COMO is used, is significantly higher than those of the basic opportunistic routing protocol. Specifically, for the median case, our protocol achieves 5.39% (resp., 8.30%, 10.04%) higher throughput than the basic opportunistic routing protocol when 20% (resp., 40%, 80%) nodes deviate.

6.4 Communication Overhead

The incentive protocol COMO incorporates message authentication code tags in the probe messages and data packets. We

implement COMO with UMAC to generate 32 bits outputs. Consequently, the size of tags in probe messages and data packets is 8 bytes and 7 bytes, respectively. A probe message can be forwarded at most 3 times to reach the source node using the transmission rate of 1Mbps. Therefore, the communication overhead induced in the process of probing is up to 6.75Kbytes, while the communication overhead induced in the process of data packet forwarding is up to 1.4% of the total data traffic, in our experiments.

We note that the incentive protocol presented in this paper also inherit coding overhead, memory overhead, and packet header overhead from the underlying multirate opportunistic routing protocol. Since these overheads do not specifically belong to our incentive protocol, we do not measure them in our experiments.

7 CONCLUSION AND FUTURE WORK

In this paper, we have presented a practical incentive protocol, namely COMO, to solve the problem of selfish behavior in multirate opportunistic routing. COMO achieves cooperation-optimality in multirate opportunistic routing, *i.e.*, when everyone follows the routing and incentive protocol, the system performance is optimized and each node’s payoff is maximized. We have integrated our incentive protocol with MORE in a Linux implementation, and have demonstrated on the ORBIT wireless testbed that (a) cheating decreases a node’s utility under COMO; and (b) COMO can substantially improve overall network throughput when selfish nodes exist. As a future work, it would be interesting to study the problem of collusion among multiple nodes in multirate opportunistic routing.

ACKNOWLEDGEMENT

This work was supported in part by the State Key Development Program for Basic Research of China (973 project 2014CB340303 and 2012CB316201), in part by China NSF grant 61422208, 61472252, 61272443 and 61133006, in part by CCF-Intel Young Faculty Researcher Program and CCF-Tencent Open Fund, in part by the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry, and in part by Program for Changjiang Scholars and Innovative Research Team in University (IRT1158, PCSIRT) China. The opinions, findings, conclusions, and recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the funding agencies or the government.

REFERENCES

- [1] E. Adar and B. A. Huberman, “Free riding on gnutella,” *First Monday*, vol. 5, no. 10, Oct. 2000.
- [2] D. Aguayo, J. Bicket, S. Biswas, G. Judd, and R. Morris, “Link-level measurements from an 802.11b mesh network,” in *Proceedings of ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM)*, Portlan, Oregon, Aug. 2004.
- [3] I. F. Akyildiz and X. Wang, “A survey on wireless mesh networks,” *IEEE Communications Magazine*, vol. 43, no. 9, 2005.

- [4] L. Anderegg and S. Eidenbenz, "Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," in *Proceedings of the Ninth International Conference on Mobile Computing and Networking (MobiCom)*, San Diego, CA, Sep. 2003.
- [5] 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 *Proceedings of the Fourth ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Annapolis, MD, Jun. 2003.
- [6] S. Biswas and R. Morris, "Opportunistic routing in multi-hop wireless networks," in *Proceedings of ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM)*, Philadelphia, PA, Aug. 2005.
- [7] W. E. Bluhm, *Society of Actuaries 50th Anniversary Monograph*. Schaumburg, Ill., Society of Actuaries, etc., 1999, ch. V: Cumulative Anti-Selection Theory.
- [8] L. Buttyan and J. P. Hubaux, "Enforcing service availability in mobile ad-hoc WANS," in *Proceedings of the First ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Boston, Massachusetts, Aug. 2000.
- [9] 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*, vol. 22, no. 1, pp. 6–12, Jan.-Feb. 2008.
- [10] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading structure for randomness in wireless opportunistic routing," in *Proceedings of ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM)*, Kyoto, Japan, Aug. 2007.
- [11] T. Chen and S. Zhong, "INPAC: An enforceable incentive scheme for wireless networks using network coding," in *Proceedings of 29th Annual IEEE Conference on Computer Communications (INFOCOM)*, San Diego, CA, Apr. 2010.
- [12] D. S. J. D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *Proceedings of the Ninth International Conference on Mobile Computing and Networking (MobiCom)*, San Diego, CA, Sep. 2003.
- [13] W. Du, J. Deng, Y. S. Han, and P. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS)*, Washington D.C., USA, 2003.
- [14] 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 *Proceedings of the 19th International Parallel and Distributed Processing Symposium (IPDPS)*, Denver, CO, Apr. 2005.
- [15] M. K. Han, A. Bhartiya, L. Qiu, and E. Rozner, "O3: Optimized overlay-based opportunistic routing," in *Proceedings of The 12th ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Paris, France, May 2011.
- [16] J. W. Huang and V. Krishnamurthy, "Truth revealing opportunistic scheduling in cognitive radio systems," in *Proceedings of The 10th IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Perugia, Italy, Jun. 2009.
- [17] M. Jakobsson, J. P. Hubaux, and L. Buttyan, "A micro-payment scheme encouraging collaboration in multi-hop cellular networks," in *Proceedings of the Seventh International Financial Cryptography Conference (FC)*, Gosier, Guadeloupe, Jan. 2003.
- [18] S. Katti, D. Katabi, H. Balakrishnan, and M. Medard, "Symbol-level network coding for wireless mesh networks," in *Proceedings of ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM)*, Seattle, WA, Aug. 2008.
- [19] D. Koutsonikolas, C.-C. Wang, and Y. C. Hu, "CCACK: Efficient network coding based opportunistic routing through cumulative coded acknowledgments," in *Proceedings of 29th Annual IEEE Conference on Computer Communications (INFOCOM)*, San Diego, CA, Apr. 2010.
- [20] D. Laneman and G. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transaction on Information Theory*, vol. 50, no. 12, pp. 3062 – 3080, 2004.
- [21] P. Larsson, "Selection diversity forwarding in a multihop packet radio network with fading channel and capture," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 4, pp. 47–54, Oct. 2001.
- [22] R. Lauffer, H. Dubois-Ferri'ere, and L. Kleinrock, "Multirate anypath routing in wireless mesh networks," in *Proceedings of 28th Annual IEEE Conference on Computer Communications (INFOCOM)*, Rio de Janeiro, Brazil, Apr. 2009.
- [23] Y. Lin, B. Li, and B. Liang, "CodeOR: Opportunistic routing in wireless mesh networks with segmented network coding," in *Proceedings of the 16th International Conference on Network Protocols (ICNP)*, Orlando, FL, Oct. 2008.
- [24] Y. Lin, B. Liang, and B. Li, "SlideOR: oline opportunistic network coding in wireless mesh networks," in *Proceedings of 29th Annual IEEE Conference on Computer Communications (INFOCOM)*, San Diego, CA, Apr. 2010.
- [25] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS)*, Washington D.C., USA, 2003.
- [26] MadWifi Project Team, "<http://madwifi.org>."
- [27] A. K. Miu, H. Balakrishnan, and C. E. Koksal, "Improving loss resilience with multi-radio diversity in wireless networks," in *Proceedings of The Eleventh International Conference on Mobile Computing and Networking (MobiCom)*, Cologne, Germany, Sep. 2005.
- [28] M. J. Osborne and A. Rubenstein, *A Course in Game Theory*. MIT Press, 1994.
- [29] B. Radunovic, C. Gkantsidis, P. Key, and P. Rodriguez, "An optimization framework for opportunistic multipath routing in wireless mesh networks," in *Proceedings of 27th Annual IEEE Conference on Computer Communications (INFOCOM)*, Phoenix, AZ, Apr. 2008.
- [30] H. Rahul, H. Hassanieh, and D. Katabi, "Sourcesync: A distributed wireless architecture for exploiting sender diversity," in *Proceedings of ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM)*, New Delhi, India, Aug.-Sept. 2010.
- [31] E. Rozner, M. K. Han, L. Qiu, and Y. Zhang, "Model-driven optimization of opportunistic routing," *IEEE/ACM Transactions on Networking*, vol. 21, no. 2, pp. 594–609, April 2013.
- [32] 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.
- [33] Rutgers ORBIT project team, "<http://www.orbit-lab.org>."
- [34] The Click Modular Router Project Team, "<http://www.read.cs.ucla.edu/click/>."
- [35] UMAC, "UMAC: Message authentication code using universal hashing," <http://tools.ietf.org/html/rfc4418>, Mar. 2006.
- [36] VMAC, "VMAC: Message authentication code using universal hashing," <http://www.fastcrypto.org/vmac/draft-krovetz-vmac-01.txt>, Mar. 2010.
- [37] W. Wang, S. Eidenbenz, Y. Wang, and X.-Y. Li, "Ours—optimal unicast routing systems in non-cooperative wireless networks," in *Proceedings of The Twelfth International Conference on Mobile Computing and Networking (MobiCom)*, Los Angeles, Sep. 2006.
- [38] W. Wang, X.-Y. Li, and Y. Wang, "Truthful multicast in selfish wireless networks," in *Proceedings of the Tenth International Conference on Mobile Computing and Networking (MobiCom)*, Philadelphia, PA, Sep. 2004.
- [39] Z. Wang, Y. Chen, and C. Li, "CORMAN: A novel cooperative opportunistic routing scheme in mobile ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 289–296, 2012.
- [40] F. Wu, T. Chen, S. Zhong, L. E. Li, and Y. R. Yang, "Incentive-compatible opportunistic routing for wireless networks," in *Proceedings of The Fourteenth International Conference on Mobile Computing and Networking (MobiCom)*, San Francisco, CA, Sep. 2008.
- [41] F. Wu and N. Vaidya, "Workload-aware opportunistic routing in multi-channel, multi-radio wireless mesh networks," in *Proceedings of the 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Seoul, Korea, Jun. 2012.
- [42] H. Yao and S. Zhong, "Towards cheat-proof cooperative relay for cognitive radio networks," in *Proceedings of The 12th ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Paris, France, May 2011.
- [43] K. Zeng, Z. Yang, and W. Lou, "Opportunistic routing in multi-radio multi-channel multi-hop wireless networks," in *Proceedings of 29th Annual IEEE Conference on Computer Communications (INFOCOM)*, San Diego, CA, Apr. 2010.
- [44] X. Zhang and B. Li, "Dice: a game theoretic framework for wireless multipath network coding," in *Proceedings of The Ninth ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Hong Kong, China, Sep. 2008.
- [45] 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 *Proceedings of The Eleventh International*

Conference on Mobile Computing and Networking (MobiCom), Cologne, Germany, Sep. 2005.

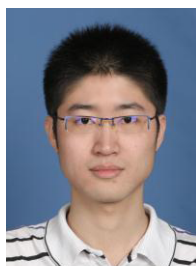
- [46] S. Zhong, J. Chen, and Y. R. Yang, "Sprite, a simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Proceedings of 22nd Annual IEEE Conference on Computer Communications (INFOCOM)*, San Francisco, CA, Apr. 2003.
- [47] S. Zhong and F. Wu, "On designing collusion-resistant routing schemes for non-cooperative wireless ad hoc networks," in *Proceedings of The Thirteenth International Conference on Mobile Computing and Networking (MobiCom)*, Montreal, Canada, Sep. 2007.
- [48] Z. Zhong, J. Wang, S. Nelakuditi, and G.-H. Lu, "On selection of candidates for opportunistic anypath forwarding," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 10, no. 4, pp. 1–2, Oct. 2006.



Fan Wu is an associate professor in the Department of Computer Science and Engineering at Shanghai Jiao Tong University, P. R. China. He received his B.S. in Computer Science from Nanjing University in 2004, and Ph.D. in Computer Science and Engineering from the State University of New York at Buffalo in 2009. He has visited the University of Illinois at Urbana-Champaign (UIUC) as a Post Doc Research Associate. His current research interests include wireless networking and mobile computing, algorithmic network economics, and privacy preservation. He is a recipient of China National Natural Science Fund for Outstanding Young Scientists in 2014 and Pujiang Scholar award in 2012. He is a member of ACM, CCF, and IEEE. For more information, please visit <http://www.cs.sjtu.edu.cn/~fwu/>.



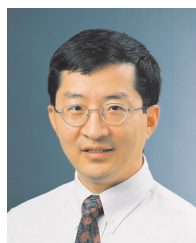
Kai Gong is currently working in SAIC Motor Corporation Limited. He received his B.S. in Computer Science and Engineering from Shanghai Jiao Tong University in 2012.



Tianrong Zhang is currently pursuing his Ph.D. degree in the Department of Computer Science at the University of North Carolina at Chapel Hill, USA. He received his B.S. in Computer Science and Engineering from Shanghai Jiao Tong University in 2012. His research interests include computer networks, networked systems, and distributed systems.



Guihai Chen earned his B.S. degree from Nanjing University in 1984, M.E. degree from Southeast University in 1987, and Ph.D. degree from the University of Hong Kong in 1997. He is a distinguished professor of Shanghai Jiaotong University, China. He had been invited as a visiting professor by many universities including Kyushu Institute of Technology, Japan in 1998, University of Queensland, Australia in 2000, and Wayne State University, USA during September 2001 to August 2003. He has a wide range of research interests with focus on sensor networks, peer-to-peer computing, high-performance computer architecture and combinatorics. He has published more than 200 peer-reviewed papers, and more than 120 of them are in well-archived international journals such as IEEE Transactions on Parallel and Distributed Systems, Journal of Parallel and Distributed Computing, Wireless Networks, The Computer Journal, International Journal of Foundations of Computer Science, and Performance Evaluation, and also in well-known conference proceedings such as HPCA, MOBIHOC, INFOCOM, ICNP, ICPP, IPDPS and ICDCS.



Chunming Qiao is a professor at the University at Buffalo, the State University of New York (SUNY), where he directs the Lab for Advanced Network Design, Evaluation and Research (LANDER). His pioneering work on integrating cellular and ad hoc relaying using, for example, 802.11 in 1999 has been featured in the BusinessWeek, Wireless Europe, as well as NewScientists and CBC. He is also recognized for his research on Optical Internet, and in particular, the optical burst switching (OBS) paradigm.

He has given several keynote speeches, invited talks and tutorials, and is an editor of several journals and magazines including the IEEE/ACM Transactions on Networking (ToN), the IEEE Transactions on Parallel and Distributed Systems (TPDS), and a guest editor for several issues of the IEEE JSAC and ACM MONET. He has chaired and cochaired more than a dozen of international conferences and workshops, and is currently the chair of the IEEE Technical Committee on High-Speed Networks, and the founding chair of the new IEEE TC on integrated optical and wireless networks. He has published 80 papers in leading technical journals and more than 120 papers in conference proceedings, and his research has been sponsored by several US National Science Foundation (NSF) grants including two prestigious ITR awards, and six major telecommunications and networking research labs. He is a fellow of the IEEE.