This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2014.2320255, IEEE Transactions on Mobile Computing

A P2P-based Market-guided Distributed Routing Mechanism for High-Throughput Hybrid Wireless Networks

Haiying Shen*, *Senior Member, IEEE*, Ze Li, *Student Member, IEEE*, Lei Yu

Abstract—In a hybrid wireless network that combines a mobile ad-hoc network and an infrastructure network, efficient and reliable data routing is important for high throughput. Existing routing schemes that simply combine ad-hoc and infrastructure routings inherit the drawbacks of ad-hoc routing including congestion and high overhead for route discovery and maintenance. Although current reputation systems help increase routing reliability, they rely on local information exchanges between nodes to evaluate node reputations, so they are not sufficiently effective and efficient. A challenge here is if we can coordinately develop an efficient routing algorithm and effective cooperation incentives for reliable routing. To handle this challenge, this paper presents a peer-to-peer (P2P)-based Market-guided Distributed Routing mechanism (MDR). MDR takes advantage of widespread base stations to coordinately realize highly efficient data routing, and effective reputation management and trading market management for reliable data routing. The packets from a source node are distributively transmitted to base stations directly or indirectly, and then they are transmitted to the destination. The base stations form a P2P structure for reputation collection and querying to avoid local information exchanges, and for managing the service transactions between nodes in the trading market. By leveraging the single-relay transmission feature, base stations can monitor the actual transmitted packets of relay nodes to more accurately and efficiently evaluate their reputations and execute trading market management, as well as detect falsely reported reputation information. We further propose market-based policies to strengthen cooperation incentives. Simulation results show that MDR outperforms the traditional hybrid routing schemes and reputation systems in achieving high throughput.

Index Terms—Hybrid wireless networks, Routing, Reputation systems, Trading market model

1 Introduction

A hybrid wireless network is a combination of a mobile ad-hoc network (MANET) and an infrastructure network. In such a network, base stations (BSes) in the infrastructure act as relays for mobile nodes (MNs) in the MANET for long distance communications and Internet access, while MANET extends the coverage of the infrastructure network [1]. Examples of promising applications for hybrid networks include mobile file/video sharing networks and vehicular networks [2].

Equipped with both a high-power 3G interface and a low-power WiFi interface, current smartphones (e.g., iPhone and Android phones) are capable of seamlessly switching between MANET and 3G cellular network. Mobile devices are quickly growing in their capabilities, and their growth rate seems to be outpaced by the needs of sophisticated (e.g., multimedia) applications with requirements of a high throughput capacity. It was reported recently that the mobile data traffic grows at an annual rate of 40% between 2009 and 2014 and is expected to reach 40 billion gigabytes by 2014. To achieve high data throughput and support bandwidth-intensive applications, an efficient and reliable routing scheme is increasingly needed.

Most of the routing schemes used in hybrid networks [3]–[13] simply combine existing routing schemes in MANETs and infrastructure networks. A message is forwarded in MANET through WiFi links to a node closer to a BS, and then it is forwarded to the BS, and then to the BS where the destination MN resides based on routing algorithm in cellular networks. Finally, it is forwarded to the destination node. Such routing inherits the problems in ad-hoc routing, such as congestion and high overhead for route discovery and maintenance [1], which prevents hybrid networks from achieving a high throughput. Although BSes are widely spread over a hybrid network, most previously proposed high-throughput routing algorithms are mainly focused on the routing in one single BS and fail to take advantage of the dispersed BSes for higher efficiency.

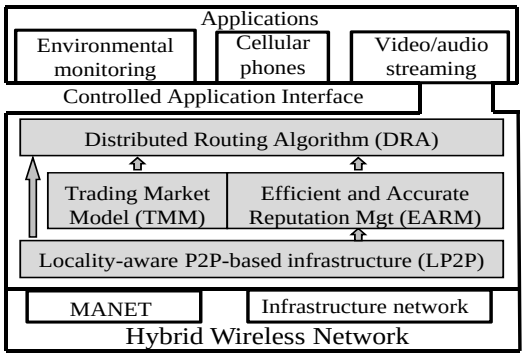


Fig. 1: A high-level view of the MDR mechanism.

Reliable routing is faced with a severe challenge posed by selfish nodes that tend not to forward data in order to save resources of their own. To avoid selfish nodes, a routing algorithm can choose high-reputed nodes as relay nodes by using reputation systems [14]–[24]. In most current reputation systems, each node locally evaluates other nodes' reputation values based on reputation information exchanged between neighbors. This frequent information exchange generates high overhead and reputation evaluation based on local partial information (i.e., partial forwarding activities of a node) may result in an insufficiently accurate reputation value. Calculating a node's reputation based on all reputation information on this node (i.e., all forwarding activities of this node) can more accurately reflect the node's cooperative behavior. Furthermore, the reputation systems cannot avoid falsely reported reputation information and cannot effectively provide incentives for cooperation.

To increase the throughput of hybrid networks through highly efficient and reliable routing, a challenge here is if we can take advantage of the widespread BSes to coordinately develop an efficient routing algorithm

* *Corresponding Author. Email: shenh@clemson.edu; Phone: (864) 656 5931; Fax: (864) 656 5910.*

The authors are with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, 29634. E-mail: {shenh, zel, leiy}@clemson.edu

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2014.2320255, IEEE Transactions on Mobile Computing

and effective cooperation incentives for reliable routing; the routing algorithm facilitates the implementation of the cooperation incentives to overcome aforementioned drawbacks. To handle this challenge, we propose a peer-to-peer (P2P)-based Market-guided Distributed Routing mechanism (MDR). MDR takes advantage of widely-scattered BSes to facilitate highly efficient single-relay distributed data routing, in which the segments of a message are transmitted directly or indirectly to BSes in a distributed manner through multiple relay nodes. The BSes form a P2P structure for reputation collection and querying to avoid local information exchanges, and for managing the service transactions between nodes in the trading market. By leveraging the single-relay transmission feature, BSes can monitor the actual transmitted packets of relay nodes to evaluate their reputation and execute trading market management, as well as detect falsely reported reputation information. Thus, a node's reputation is based on i) its actual relaying behavior, and ii) all rather than partial reputation information, which can calculate more accurate reputation. Specifically, MDR consists of four components: a locality-aware P2P-based infrastructure (LP2P), a distributed routing algorithm (DRA), an efficient and accurate reputation management system (EARM), and a trading market model (TMM). Figure 1 shows a high-level architecture of MDR. LP2P supports the efficient operations of EARM, TMM and DRA. EARM and TMM provide cooperation incentives and hence enhance routing reliability in DRA.

(1) LP2P. LP2P is an auxiliary component for other components. By leveraging the widely-scattered BSes, we construct a locality-aware structured P2P on the infrastructure component of a hybrid network to support efficient operations for other components.
(2) DRA. DRA divides a source stream into segments using erasure coding [25] and distributively transmits them to selected reliable neighbors through two hops to BSes. The single-relay transmission feature enables BSes to easily monitor the routing behaviors of nodes for the EARM and TMM management, which in turn provide cooperation incentives for reliable routing. LP2P helps to efficiently marshal segments to the mobile destination.
(3) EARM. Instead of using local information exchange, EARM relies on LP2P to collect all rather than partial reputation reports on a node for more accurate reputation evaluation and efficient reputation querying. Moreover, rather than relying on the reports from other nodes, EARM calculates reputation of a node based on the number of its actual relayed messages which avoids falsely reported information by taking advantage of the single-relay feature of DRA.
(4) TMM. In TMM, a node pays credits to a relay node for forwarding service and earns credits by forwarding others' messages. Also, nodes adjust their routing service price to adaptively control their loads. Two market-based policies are further proposed to strengthen cooperation incentives. TMM fosters the effectiveness in deterring selfish behaviors and providing cooperation incentives.

As far as we know, MDR is the first work that takes advantage of widespread BSes to coordinately realize efficient distributed routing, reputation management and trading market management to enhance routing efficiency and reliability. The rest of this paper is organized as follows. Section 2 details the MDR mechanism with descriptions of the different MDR components. Section 3 briefly discusses our strategies to handle node misbehaviors that exploit the vulnerabilities of MDR to gain unfair benefits. Section 5 shows the performance of MDR in experiments. Section 6 presents a review of related work. Finally, Section 7 concludes the paper with remarks on our plans for future work.

2 MDR: P2P-based Market-guided Distributed Routing Mechanism

In this section, we introduce the four components of MDR, respectively.

2.1 Locality-aware P2P-based Infrastructure (LP2P)

As shown in Figure 2, MDR builds LP2P for the substrate of the infrastructure component of a hybrid network. The overlay network provides two main functions `Insert(ID,object)` and `Lookup(ID)` to store an object to a node responsible for the ID of the object, and to retrieve the object based on its ID, respectively. In LP2P, the logical proximity abstraction derived from the overlay network matches the physical proximity information in reality, which enables BSes to communicate with their physically closest nodes for high efficiency.

Specifically, we use the landmark method described in [26] to build LP2P. The landmark clustering technique is based on the intuition that nodes located close to each other are likely to have similar distances to a few selected landmark nodes. Given $\tilde{m}$ landmark BSes that are randomly scattered in the network, each BS measures its physical distances to landmarks and uses the vector of distances $< d_1, d_2, \ldots, d_{\tilde{m}} >$ as its coordinate. Two physically close BSes have similar landmark vectors. A Hilbert space-filling curve [27] is a technique for dimension reduction of vectors while still preserving the relative distances among points in a multi-dimensional space. We then use the technique to map landmark vectors to real numbers, called Hilbert numbers. The closeness of the BSes' Hilbert numbers represents the physical closeness of the BSes on the network. Then, we directly use a BS's Hilbert number as its ID for constructing structure P2P infrastructure and P2P routing. Based on the `Insert(ID,object)` and `Lookup(ID)` functions provided by the structured P2P, we can efficiently operate the information stored in the distributed BSes.

2.2 Distributed Single-Relay Routing Algorithm (DRA)

As shown in Figure 2, to send a message D from the source node to the destination, DRA is comprised of five steps as follows:
(1) The source node first uses the erasure coding technique to encode the message D into D_1 to D_{n_r} coded segment.
(2) The source node sends these segments to different capable neighbors selected in a distributed manner. To do that, the source node first broadcasts a request with the segment length. Its neighbors with sufficient capacity for the forwarding reply to the source node. The source node relies on EARM and TMM for reliable and cooperative relay node selections (details will be presented in Sections 2.3 and 2.4). It then sends its segments to the selected relay nodes.
(3) The relay nodes carry the segments and send the segments to BSes when they enter their coverage areas.
(4) The BSes then forward the segments to the BS where the destination resides [28]. To locate the destination BS, DTR takes advantage of LP2P for destination tracking. Each MN has a P2P ID which is the consistent hash value

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2014.2320255, IEEE Transactions on Mobile Computing

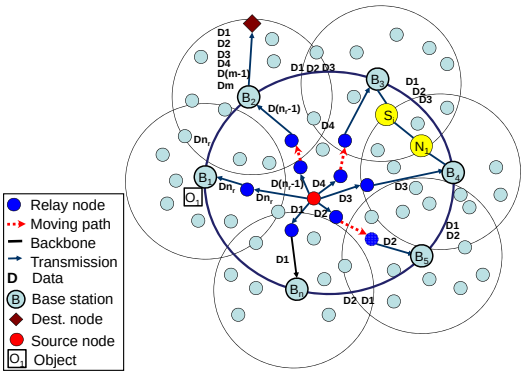


Fig. 2: MDR in a hybrid wireless network.

of its IP address. It has an owner BS which is the owner of its ID in the P2P. Each MN's location is maintained in its owner BS. Basically, every time a MN n_i moves to another cell, the BS in the cell, denoted by B_i, reports to n_i's owner BS by the P2P function `Insert`(ID_{n_i}, B_i). The destination BS B_i can be obtained by asking n_i's owner BS with `Lookup`(ID_{n_i}).

(5) The BS where the destination resides forwards the segments of a message to the destination node, and the destination reassembles the message.

In DRA, only one single relay is used to forward a segment between the source node and BS. Such routing helps to generate a higher throughput with two-hop short path length and adaptive selection of relay nodes based on EARM and TMM. It also avoids dynamically maintaining the paths among mobile nodes. On the other hand, due to the single relay routing, the transmission behavior of relay nodes can be easily monitored by the BSes, which ensures efficient and accurate reputation evaluation.

Erasure coding based segmentation strengthens DRA's tolerance ability to forwarding failure and delay in the distributed packet trading process. The erasure coding technique breaks a message D of length $|D|$ into m segments and recodes them into n_r coded segments. The length of each segment is $\frac{|D|}{m}$ and m coded segments are sufficient for reconstructing the original message. Thus, only $\frac{1}{r}$ of the n_r coded segments are required to reconstruct the message, where $r = \frac{n_r}{m}$ is a replication factor. DRA can tolerate $(1-\frac{1}{r})$ forwarding failures based on the feature of erasure coding. That is, even if $n_r - m$ segments cannot be forwarded to their destination in time, DRA is still able to reconstruct the original data.

2.3 Efficient and Accurate Reputation Management (EARM)

A challenge in reliable data routing is how to avoid selfish nodes. EARM helps achieve this objective while offering incentives for node cooperation in routing. Compared to traditional reputation systems, EARM has the following advantages: (1) Rather than depending on frequent local information exchange among neighbors, which does not guarantee the accuracy of reputation values due to partial reputation information for reputation calculation and incurs a high overhead, EARM relies on LP2P to efficiently collect all reputation information on each node that helps calculate more accurate reputation values; (2) Taking advantage of the single-relay feature of DRA, EARM calculates a node's reputation value based on its actual number of forwarded bytes rather than other nodes' feedback, which may be falsely reported by misbehaving nodes; and (3) Relying on LP2P, EARM offers efficient global reputation querying.

Reputation value calculation. As the BSes are maintained by authorized telecommunication companies or government which are generally trustworthy, we use BSes to serve as authorities to supervise the transactions between source nodes and relay nodes in order to improve the throughput of hybrid wireless networks. In EARM, the reputation is measured by a value between 0 and 1. Every node is initially considered to be untrustworthy with zero initial reputation value. A BS increases the reputation value of a relay node when receiving a forwarding segment from the node. That is, $R \leftarrow \min\{R + \beta \cdot l, 1\}$, where R is a node's reputation value ($0 \leq R \leq 1$), β denotes a constant and l denotes the length of the received segment. In order to reflect the recent behaviors of nodes, like current reputation systems, BSes periodically decrease the reputation values of their nodes by $R = \gamma R$, where γ ($\gamma < 1$) is a discount factor for a node's past behaviors.

In order to wisely use channel resources to enhance a system's throughput while rewarding relay nodes, we further propose reputation-based bandwidth allocation. Specifically, a BS assigns more bandwidth to higher-reputed MNs by $BW = BW_{min} + \eta R$, where BW denotes the assigned bandwidth, BW_{min} is the minimum bandwidth which every node can get in the system, and $\eta = BW_{max} - BW_{min}$ such that the nodes with the highest reputation $R = 1$ can get maximum bandwidth BW_{max} allowed by the system . This algorithm provides incentives for node cooperation in data forwarding while improves system throughput.

Reputation value collection and querying. A BS calculates the local reputation value of node n_i in its own range based on the number of bytes n_i forwards to it, and periodically reports the value to LP2P by using `Insert`(ID_i, R_i). Based on the P2P object assignment policy, n_i's local reputation values are then collected in its owner BS. The owner BS calculates the average of the local reputation values of n_i as n_i's global reputation value, and stores it locally.

When node n_j queries for node n_i's reputation value, it asks its closest BS. If the BS is not the owner of n_i, it executes `Lookup`(ID_i). Using the P2P routing algorithm, the request will be forwarded to node n_i's owner BS that has node n_i's global reputation value. Since the queries for reputation are always for the MNs in a BS's coverage area, the BS can cache queried node reputation values for subsequent querying from its MNs in order to reduce the query delay. The P2P-based reputation system offers efficient global reputation information collection and querying. Also, calculating a node's global reputation based on all of its actual forwarding activities enhances reputation evaluation accuracy.

2.4 Trading Market Model (TMM)

2.4.1 Basic Trading Market Model

TMM manages data transmission operations between source nodes and relay nodes for reliable and efficient data transmission. Each node is assigned a certain amount of credits initially when it joins the system. Source nodes pay credits to relay nodes and relay nodes charge source nodes for data forwarding services. Since the data forwarding cost is directly related to the data length, TMM uses the product of the data length and unit service price per byte to determine the forwarding service price. Each node determines its service price

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2014.2320255, IEEE Transactions on Mobile Computing

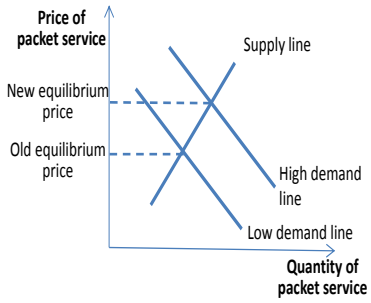


Fig. 3: Equilibrium price in the market.

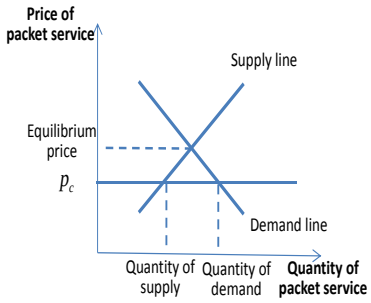


Fig. 4: Pricing ceiling in the market.

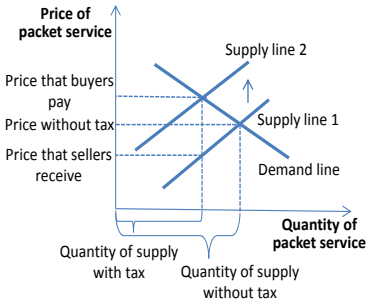


Fig. 5: Equilibrium price with taxing.

based on the supply and demand equilibrium. Specifically, a node considers two factors: its QoS and the business competition between nodes. For the former, higher-QoS nodes tend to claim higher prices and vice versa. For the latter, in order to attract more business to earn more credits and higher reputations, nodes should offer lower price and vice versa.

These two factors can be reflected by the queuing length in a node's queue. Long queuing length of a benign node means it may not have additional capacity for offering high QoS to more requests and has already received many requests for accumulating its reputation. In this case, the node can increase its service price to avoid being overloaded and offering low QoS. In contrast, short queuing length of a benign node means it has sufficient capacity to offer a high QoS and receive more requests to increase its reputation. In this case, the node can decrease its price to attract more requests. Accordingly, we propose a price determination function by leveraging the polynomial price function in the economics area [29] that keeps the supply and demand equilibrium. We use P to denote a node's forwarding service price per byte. Then,

$$P = \bar{p} + \sum_{i=1}^{\delta} \alpha \cdot \left(\frac{l_q}{L_q}\right)^i, \quad (1)$$

where l_q and L_q are the lengths of the occupied part and entire part of its queue respectively, $\bar{p}$ is the base price, and α and δ are the scaling parameters for the price. This price determination function enables nodes to adjust their routing service price to adaptively control their loads. Formula (1) indicates that if a node receives few requests (i.e., has a short queuing length), it decreases its price to attract more requests. On the other hand, if a node receives a large amount of forwarding requests (i.e., has a long queuing length), it raises its price to avoid being overloaded.

As described in Section 2.2, the source needs to select a relay node for each segment. With neighbors' reputations returned by EAR, the source node considers the higher-reputed nodes with higher priority because such nodes help to achieve higher routing reliability. The source node then chooses the neighbors whose service charges are affordable. For two neighbors with the same reputation, the source selects the one with the lower price. Therefore, the amount of credits owned by the source C_a should satisfy $C_a \geq \sum_{i=1}^{n_r} P_i \cdot l_i$, where P_i and l_i are the service price of selected neighbors and data length for the i^{th} segment, respectively. Each node n_i's owner BS manages n_i's credit account and conducts credit transfer for n_i's forwarding transactions. A source node n_i pays its relay n_j by notifying n_i's owner BS along with the transmitted packet size and price. n_i's owner BS transfers credits to n_j's owner BS after they confirm the correctness of the information from the source node. We will introduce the information correctness validation in Section 3.

If the source node cannot afford the service charge of any relay node, it needs to earn more credits by forwarding data for others. Thus, TMM not only serves as an effective means to provide cooperation incentives, but also deters the behaviors of uncooperative nodes by starving their credits. Our previous game theoretical analysis work [30] confirms the effectiveness of the node cooperation incentives in price-based systems. TMM also balances node load by enabling nodes to automatically adjust their service price based on the supply and demand equilibrium.

2.4.2 Market-based Policies

In the economic market, the supply and demand determine the price for the packet forwarding service (service in short). Figure 3 shows the relationship between the market equilibrium price and the demand/supply in the market according to the economic theory [31]. The *supply* line illustrates the relationship between the service price and the quantity of the service supplied in the market. The quantity of the service in supply increases as the service price increases. That is, if the service price is high, more nodes are encouraged to provide services, which leads to service quantity increase in the market. The *demand* line illustrates the relationship between the service price and the quantity of services in demand. We see that the quantity of service in demand increases as the price decreases in the market. The supply line shifts up when the quantity of the service the producer can provide at every price decreases. The demand line shifts up when the consumer increases the quantity demanded at every price, referred to as *an increase in demand*. The crossing point of the supply line and the demand line is the equilibrium price that balances the demand and supply in the market. The figure indicates that an increase in demand leads to a higher market equilibrium price.

Based on the previous basic trading market model, if we completely let the nodes autonomously determine the price in the market, a low-traffic region generates low equilibrium price and a high-traffic region generates high equilibrium price. This is because the quantity of packet service in demand in low-traffic region is lower than that in the high-traffic region. Given a supply line, a lower demand incurs a lower market equilibrium price, as shown in Figure 3. As a result, cooperative nodes in a low-traffic region cannot earn many credits since they cannot sell their services at a specified high price, and thus cannot buy services. In contrast, uncooperative nodes in a high-traffic region can still sell service at a high price because the service demand in this region is high. Such a result may discourage cooperative nodes

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2014.2320255, IEEE Transactions on Mobile Computing

to continuously be cooperative in low-traffic regions and fail to punish wealthy and uncooperative nodes in high-traffic regions. To deal with this problem, we propose two policies to control the price to provide more effective cooperation incentives.

Policy 1: Set a price ceiling in the market and give higher-reputed nodes higher priority to buy services. The price ceiling is an offered price threshold that every node cannot exceed, and it should be lower than the market equilibrium price. We first analyze the effect of price ceiling on the market equilibrium price. Figure 4 shows how a price ceiling affects the demand and supply in the market. We see that the quantity of supply is less than the quantity of demand after setting a price ceiling. This leads to a shortage of the supplies, especially the high-QoS supplies. With Policy 1, suppliers offer their limited services to the nodes with higher reputation. Uncooperative nodes in high-traffic regions, even those with many credits, would have few chances to receive services, thus getting punished. Also, as the price of high-QoS service is bounded by the ceiling price that is lower than the equilibrium price, cooperative nodes in a low-traffic region can have more chances to sell their services and also purchase high-QoS services. Policy 1 thus provides high incentives for uncooperative nodes to be cooperative and creates more chances for high-reputed nodes to purchase high-QoS services in both low-traffic and high-traffic regions. We cannot set the ceiling price too low as the supply shortage would crash the market and lead to a low system throughput. Thus, we propose Policy 2 below to further ensure that the cooperative nodes in low-traffic regions can always buy high-QoS services.

Policy 2: Levy tax on nodes based on their revenues and subsidize cooperative nodes. Since the transactions of nodes are monitored by their owner BSes, the owner BSes can tax sellers on their transactions by directly reducing credits from their accounts. Figure 5 illustrates how taxing affects the equilibrium price in the market. We see that when tax is levied on sellers, there is a shift from supply line 1 to supply line 2 because the sellers must increase their service price in order to offset the tax on the goods. This supply line shift leads to an increase of the equilibrium price. Thus, uncooperative nodes' chances to sell their services are reduced and the quality and quantity of services they are able to buy are reduced. These levied tax credits can be subsidized to the cooperative nodes with low revenues in the low-traffic regions. The subsidy can help these cooperative nodes buy more high-QoS services.

3 Misbehavior Prevention

In this section, we briefly discuss our strategies to handle node misbehaviors that exploit the vulnerabilities of MDR to gain unfair benefits.

Misbehavior 1: Packet forging and modification. Since a node's reputation R is determined by the size and the number of its forwarded packets, a selfish relay node may send bogus packets or insert junk data into the packet to earn higher R. To prevent these attacks, we use symmetric key to ensure the authenticity and integrity of the packets, considering that the public key authentication [32] consumes immense energy of the nodes and leads to long transmission delay [33]. Basically, every node shares a symmetric key with all the BSes and sends messages with Message Authentication Code (MAC) computed by this key. Then, once receiving a packet from a relay node, the BS verifies the authenticity and integrity of the packet by recomputing MAC with the key of the source node.

An important issue for the symmetric key approach is the management of the symmetric keys shared between nodes and the BSes. To ease the key management and update, we use one-way-hash chain [34] to generate the symmetric keys. When a node n joins in the network, it generates a one-way-hash chain via a globally known cryptographically secure hash function $h(*)$ as follows:

$$H_L \overset{h}{\leftarrow} H_{L-1} \overset{h}{\leftarrow} \ldots \overset{h}{\leftarrow} H_i \overset{h}{\leftarrow} H_{i-1} \overset{h}{\leftarrow} \ldots \overset{h}{\leftarrow} H_0 = h(r_n) \quad (2)$$

where $H_i = h(H_{i-1})$, r_n is a random generated key by node n and L is the length of the hash chain. Then, the node signs r_n by its private key and encrypts r_n with the public key of the BS which r_n is sent to. This BS then sends r_n to all other BSes. Here we assume all BSes are secure since BSes are usually maintained by authorities and it has a high capacity (e.g., computing and networking capacities) to ensure security [35]. Node n uses each hash value in the order from H_L to H_0 along the chain as the key for a period. When the period expires, n chooses the next hash value as the key. If the hash values in the hash chain are used up, a node re-generates a new hash chain with a new random generated key r_n and securely sends it to the BS. When node n needs to send message P, it uses current key H_i to compute MAC for P along with a nonce value $Nonce$ as $MAC(H_i, P|Nonce)$, and then sends packet $\{P, Nonce, i, MAC(H_i, P|Nonce)\}$ to the relay node. When receiving a packet, the BS drops the packet if the nonce in it is repeated with old packets; if not, it then computes $H_i = h^{i+1}(r_n)$ and re-computes the MAC of P_j to check whether it is consistent with the MAC in the packet. The packet is considered to be forged if MACs are not consistent.

With one-way-hash chain, each BS only needs to maintain a single initial random key r_n for each node n since the used key can be computed on-the-fly with key index. The cost for the key updating is small, since the next key index is used as key updating and only when the chain is used up, public-key based encryption and signature are conducted for securely transmitting initial random key. For the security, even if the previous hash values used for authentication (i.e., H_j $(j > i)$) are exposed, they still cannot derive H_i due to the one-way property of cryptographically secure hash functions. The security property of one-way-hash chain has been exploited in previous works [36], [37] to provide authentication of routing requests or transaction requests for credit-based cooperation in MANET. The hash values are disclosed in order such that the hash value H_{i-1} can be verified by checking $H_i = h(H_{i-1})$ where H_i has been disclosed before. In contrast, we use one-way-hash chain to reduce the overhead of key management.

Nonce value helps to prevent the relay nodes from sending a message multiple times to the same BS, but it cannot detect old messages if a relay node can move to the cell of another BS to replay messages. Thus, we propose a log comparing strategy that compares the packet transmission activities observed by BSes and reported by the sources. A BS maintains a log recording the forwarding activities (packet size, nonce, time and source) of relay nodes. After each authentication on a packet forwarded by a relay node, the BS updates its log. Each BS reports the log of each relay node n_i to n_i's owner BS periodically by executing `Insert(`ID_i`,` A_{ID_i}`)`, where ID_i is the ID of n_i and A_{ID_i} denotes the log information of n_i. A source node also keeps a log of its own packets that have been sent out by each relay node. Once it is in the range of a BS, it

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2014.2320255, IEEE Transactions on Mobile Computing

sends its log to the BS. The BS executes `Insert(`ID_i`,` A_{ID_i}`)`. Consequently, the logs of source nodes and of BSes about a specific relay's activities will be gathered and compared in the relay node's owner BS. If the owner BS observes that there is an inconsistency between the two logs, it is likely that n_i replayed the packet. Then, n_i's reputation is decreased.

Misbehavior 2: False transaction reporting. Since a source node needs to pay for the packet forwarding service, it may report a smaller number of packets to its owner BS than the actual number in order to pay less. The source's owner BS and relay's owner BS serve as the proxies for the relay service payment. The relay's owner BS checks the correctness of the source's reported packet size before payment. Recall that the relay's owner BS receives logs from other BSes that receive the packets from the relay. In the relayed packets, MACs can serve as a signature of the source node, which prevents the source node from falsely reporting the number of packets it has sent. If the relay's owner BS detects that the number of packets reported by source node n is less than the actual number of packets sent by n reported by other BSes, it notifies the source's owner BS, which will reduce the reputation of n.

Misbehavior 3: Colluding. In a collusion, colluders report high reputation values for each other in order to boost their reputations. In TMM, since R is calculated based on actual forwarding activities recorded by BSes rather than reported reputation by nodes, such collusion misbehavior can essentially be avoided. Two nodes can boost their reputations by repeatedly forwarding packets for each other and paying credits back and forth. In this case, these nodes truly consume resources to relay packets though the packets may not be useful. Here, the colluders consume the same amount of resources to gain the same reputation and credits as other cooperative nodes. Since there is no extra benefit from this collusion, the colluders do not have incentives for such behaviors and still follow the MDR policy. In a Sybil attack, an attacker creates a large number of pseudonymous identities to boost its own reputation. Similarly, in order to earn reputation and credits, a node must truly relay packets without extra benefits, which provides no incentives to launch Sybil attacks.

Misbehavior 4: Packet dropping. Since the reputation is calculated based on the number of segments received, for the nodes that do not want a high reputation, they can drop the packets on purpose to maintain their reputation value to a certain degree. Previous price systems cannot monitor the packet dropping behavior. In MDR, as explained previously, based on the sequence of the hash value in hash chain, BSes can censor the dropping behaviors of the mobile nodes by counting the number of used hash values in the hash chain. The log comparing strategy can also detect the packet dropping behaviors by comparing the logs reported by source nodes (that send packets to a relay node) and by BSes (that actually receive packets from the relay node).

4 Performance Analysis

In this section, we analyze the performance of MDR. We study the effect of DRA and TMM on the improvement of system throughput, respectively. We assume that the nodes are independent and identically distributed (i.i.d.) in the system.

4.1 Cost Analysis

Communication Cost. In MDR, BSes communicate with each other through wired WLAN, so the transmission cost among BSes is negligible. We consider the communication cost of mobile nodes. Considering that the communication cost via WiFi interface is lower than that via 3G interface, we weight the message complexity through WiFi and 3G with c_1 and c_2, respectively. Suppose the maximum number of nodes in a node's neighborhood is Δ. To send a message, the source first sends a forwarding request to its neighbors and receives replies, which incurs $O(c_1\Delta)$ message complexity. The source then queries the reputations of its neighbors through 3G to the closest BS, which incurs $O(c_2\Delta)$ message complexity. Thus, the cost of control messages for a message transmission is $O((c_1+c_2)\Delta)$. This control overhead is amortized over all messages of data stream sent from the source node to the destination. Each message D is encoded into n_r segments and sent to different relay nodes, resulting in $O(c_1 n_r)$ messages. Through single-relay transmission, these segments are sent to the BSes and then forwarded by BS to the destination via 3G, with $O(c_2 n_r)$ messages. Thus, the transmission cost for a message is $O((c_1+c_2)n_r)$.

Suppose there are N_s sources in the network, each having M_i $(i = 1, 2, ..., N_s)$ messages to send to a destination. The control overhead is $O((c_1+c_2)\Delta N_s)$. The total cost including the control coverhead is $O((c_1+c_2)(\Delta N_s + n_r \sum_{i=1} N_s M_i))$. Then, the percentage of control overhead is $\frac{\Delta}{\Delta + n_r M}$, where M is the average number of messages from every source. Thus, we can see that the control overhead in MDR becomes very low when M is large enough, which is also verified in the simulation evaluation shown in Figure 6(d).

Computation Cost. The cost of the cryptographic operations at mobile nodes is small. The one-way hash function SHA-1 computation cost of one-way-hash chain is amortized over the whole duration of one-way-hash chain usage. The only expensive computation cost is the public key based signature and encryption for the initial random key in the hash chain, which, however, occurs only when the current hash chain is used up. Suppose that the length of symmetric keys is 160 bits and SHA-1's energy cost is 5.9 $\mu J/bytes$ [38]. We use SHA-1 as one-way hash function. Then, generating the hash chain of length 50 needs 5.9 mJ. An RSA public-key based operation needs about 300 mJ [38]. Then, it takes about 300 mJ to start to use another hash chain of length 50, and the cost of public-key based operations is high. However, considering that the hash chain is sufficiently long and each hash value is used as a key for a time period, the cost of public-key operation amortized to every symmetric key can be very small, which is about 300/50=6 mJ in our example.

4.2 Routing Performance Analysis

The benefit of using a single relay node on the routing path from a source to a BS enables efficient and more accurate reputation management and also avoids dynamically maintaining the paths among mobile nodes. One side-effect is that the throughput highly depends on the delay for the relay node to meet any BS. DRA reduces this delay by using the erasure coding technique, in which a message is coded into multiple segments in transmission to increase the probability of segments being delivered quickly, and reduce the delay and improve the throughput.

Proposition 4.1: The expected transmission delay of a message in the erasure coding-based DRA is

$$E(T_r) = \bar{t} \cdot \sum_{i=1}^{m} \frac{1}{n_r - i + 1}, \tag{3}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2014.2320255, IEEE Transactions on Mobile Computing

where T_r is the transmission delay of a message from the source to the destination in DRA and $\bar{t}$ is the expected transmission delay of a single segment.

Proof Suppose that the arrival of segments follows the Poisson process, i.e., the arrival interval of each segment is independent and exponentially distributed in DRA. Therefore, among m' segments, the probability that the i^{th} segment's transmission delay (T_i) is longer than t is

$$Pr(T_i > t) = e^{-t/\bar{t}} \ (1 \leq i \leq m').$$

We use T_i to denote the delay of the i^{th} arriving segment. We use $T_{min} = min(T_1, T_2, ...T_{m'})$ to denote the transmission delay of the shortest-delay segment. Thus, the cumulative distribution function for T_{min} with delay less than t is

$$\begin{aligned} &Pr(T_{min} \leq t) \\ &= 1 - Pr(min(T_1, T_2, ..., T_{m'}) > t) \\ &= 1 - \Pi_{i=1}^{m'} Pr(T_i > t) = 1 - e^{-m' \cdot t/\bar{t}}. \end{aligned}$$

Then, the expected delay for the shortest-delay segment is

$$E(T_{min}) = \frac{\bar{t}}{m'}.$$

The delay of the i^{th} arriving segment in n_r segments equals the minimum delay of the segment in the remaining $(n_r - i + 1)$ segments. Then

$$E(T_i) = \frac{\bar{t}}{n_r - i + 1}. \quad (4)$$

The expected transmission delay of the first m arriving segments using erasure coding is

$$E(T_r) = E(T_1 + T_2 + ... + T_m) = \bar{t} \sum_{i=0}^{m} \frac{1}{n_r - i + 1}.$$

From Proposition 4.1, we can see that a larger number of coded segments for a message transmission lead to a decreased expected transmission delay, as long as the network is not overloaded by the increased traffic. The reduced transmission delay may not lead to higher network throughput, because it is at cost of increased traffic. Thus, we further consider the relationship between the network throughput and the traffic intensity.

Proposition 4.2: The throughput of a hybrid network equals to $min(T_a, T_a(1 - \frac{A^N/N!}{\sum_{i=0}^{N}(A^i/i!)}))(i \in \{0, 2, ..., N\})$, where A is the traffic intensity, N is the number of channels in the infrastructure network, T_a is the throughput of the MANET component.

Proof For a pair of S-D nodes, the traffic from a source node in the MANET goes through infrastructure network to the destination nodes. Blocking rate in the infrastructure network refers to the failure probability of a random channel access. It is approximately $\frac{A^N/N!}{\sum_{i=0}^{N}(A^i/i!)}$ [39]. Then, the throughput of the infrastructure network is $T_a(1 - \frac{A^N/N!}{\sum_{i=0}^{N}(A^i/i!)})$. Therefore, the throughput of the whole network is $min(T_a, T_a \cdot (1 - \frac{A^N/N!}{\sum_{i=0}^{N}(A^i/i!)}))$.

Proposition 4.3: DRA using the erasure coding technique produces higher reliability and efficiency than DRA without using the technique.

Proof Since the MNs in the system are i.i.d., the probability that the transmission time τ of each segment is less than a certain time t conforms to the exponential distribution [40]. That is, $F(t) = P(\tau < t) = 1 - e^{-t/\bar{t}}$, where $\bar{t}$ is the average transmission time. n_r denotes the number of coded segments in the erasure coding data segmentation, and m coded segments are sufficient for original data reconstruction. Thus, the probability that m segments among the n_r segment can be forwarded to the destination within time t is

$$P(x \geq m) = \sum_{x=m}^{n_r} C_{n_r}^{x} F(t)^x (1 - F(t))^{n_r - x}.$$

In the case that a message is divided into n_r segments without erasure coding, the probability that n_r non-coded segments are transmitted to a BS within time t is $F(t)^{n_r}$. Because $\sum_{x=m}^{n_r} C_{n_r}^{x} F(t)^x (1 - F(t))^{n_r - x} > F(t)^{n_r}$, segmentation using erasure coding technique leads to higher transmission reliability and efficiency than segmentation without using the technique.

5 Performance Evaluation

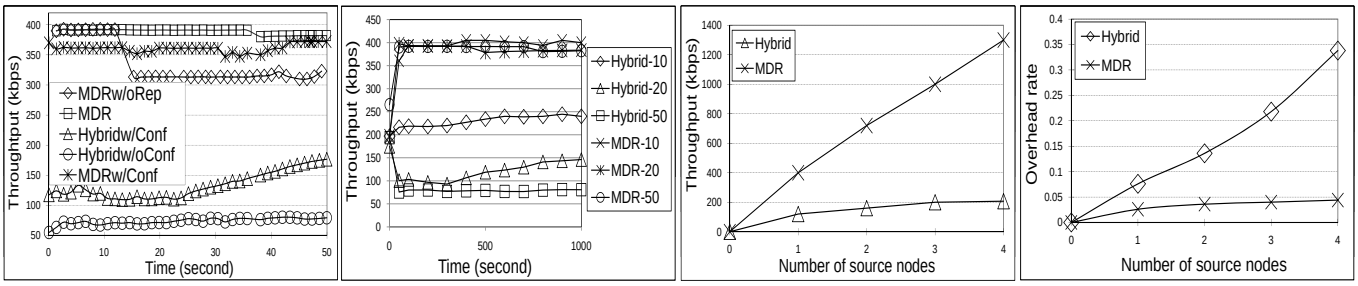
This section demonstrates the distinguishing properties of MDR through simulations on NS-2 [41]. We used the Distributed Coordination Function (DCF) of IEEE 802.11 as the MAC layer protocol, two-way propagation model in the physical layer, and the constant bit rate traffic model for all connections. The default settings are presented below unless otherwise indicated. We set the total number of MNs and BSes to 50 and 5, respectively, and set their transmission range to 250m and 500m, respectively. The BSes were uniformly distributed in an 1000×1000 square area. To simulate the node mobility, we used the Random Way Point model [42], in which each MN randomly selects and moves toward a destination point with a speed randomly selected from [1-20]m/s. The bandwidth of each node was set to 54Mbit/s. We randomly chose one source-destination pair every 10 seconds to transmit data for 50 seconds. The data generating and forwarding rate was set to 1Mbit/s. We randomly assigned a reputation value $R \in [0, 1]$ to each node. We set the percent of the selfish node to 20% that always drop their received messages. The warm up time was set to 100s. For each experiment, we ran ten tests and report the average results.

We compared MDR with a routing scheme proposed in [3], denoted by *Hybrid*, which directly combines the ad-hoc routing with infrastructure routing. We also compared MDR with the *Confidant* [16] reputation system in MANETs, in which each node evaluates the reputation of its neighbors based on their packet forwarding and receiving rates and exchanges reputation information with its neighbors. Unless otherwise specified, MDR does not include the market-based policies. In the experiments, the metric *throughput* (kbps) is used to evaluate the throughput capacity of a routing scheme. *Overhead rate* is defined as the percent of the control messages among the successfully forwarded messages. *Message delivery delay* is the average delay of all segments of a message arriving at the destination.

5.1 Comparison of Throughput

In the experiment, we measured the throughput of MDR, MDR with neither EARM nor TMM (*MDRw/oRep*), MDR with *Confidant* (*MDRw/Conf*), *Hybrid* with *Confidant* (*Hybridw/Conf*) and *Hybrid* without *Confidant* (*Hybridw/oConf*). Figure 6(a) demonstrates the throughput of different methods over a time period. We see that the throughput of MDR remains almost constant over time and it is also much higher than *Hybrid*. This result confirms that MDR is superior to *Hybrid* due to its DRA, EARM and TMM by relying on LP2P. We also find that the throughput of *Hybridw/Conf* increases slightly after 30 seconds. This is because as time elapses,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2014.2320255, IEEE Transactions on Mobile Computing



(a) Throughput (b) Scalability (c) Congestion avoidance (d) Overhead rate

Fig. 6: Performance of MDR, *Hybrid* and *Confidant* in a hybrid network.

some message holders are closer to the destinations and the interference on transmissions lessens.

We also observe that MDR generates a higher throughput than *MDRw/oRep*. This is because in *MDRw/oRep*, source nodes cannot avoid selfish nodes while MDR enables source nodes to choose highly-reputed nodes to forward segments. This figure also shows that MDR leads to a higher throughput than *MDRw/Conf*. This implies that EARM and TMM have a greater effectiveness than *Confidant* in guiding reliable relay selections and encouraging node cooperation. Unlike *Confidant*, which uses local feedback exchange for reputation calculation, EARM collects all feedback information of a MN for a global reputation calculation. Thus, it produces a more accurate reputation to reflect a node's behavior. Although *Hybridw/Conf* can improve the system throughput of *Hybridw/oConf* due to the aid of *Confidant*, its throughput is still lower than that of *MDRw/oRep* because some messages were not successfully forwarded due to broken links in multi-hop transmission. This result shows the higher performance of DRA over multi-hop routing caused by its fewer routing hops and shorter path lengths in transmission. In summary, the results indicate that MDR leads to a higher throughput than previous routing algorithms in hybrid networks and that EARM and TMM are effective in enhancing the reliability of data routing with previous reputation systems.

5.2 Comparison of Scalability

To evaluate the scalability of MDR compared with *Hybrid*, we measured their throughput in networks with no selfish nodes. The number of nodes in the networks was set to 10, 30 and 50. Figure 6(b) shows that as the number of nodes increases, the throughput of *Hybrid* decreases while the throughput of MDR remains stable. The results show that MDR has a higher scalability than *Hybrid*. This is due to MDR's distinguishing features including distributed routing, relay node selection based on EARM and TMM, short transmission distance and path length by relying on LP2P. These features contribute to reliable and efficient data routing. In *Hybrid*, messages are routed in a multi-hop manner and are easily congested at gateway nodes due to the single routing path, which leads to many transmission failures.

Figure 6(c) demonstrates the throughput of MDR and *Hybrid* versus the number of source nodes when the number of MNs in the network is 100. We can observe that the throughput of MDR increases dramatically, but that of *Hybrid* only increases marginally with the growth in the number of source nodes. More source nodes generate more traffic. The gateway in *Hybrid* could easily become a bottleneck due to the single routing path, leading to high packet dropping rate. MDR outperforms *Hybrid* since it distributes loads among several nodes by sending segments to different gateway nodes in the hybrid network. In addition, the results demonstrate that MDR produces an increase in throughput almost linearly with the number of source nodes, indicating that the system's throughput in MDR is comparatively stable. The considerably higher throughput of MDR compared to *Hybrid* in high traffic illustrates the effect of the distributed routing in MDR.

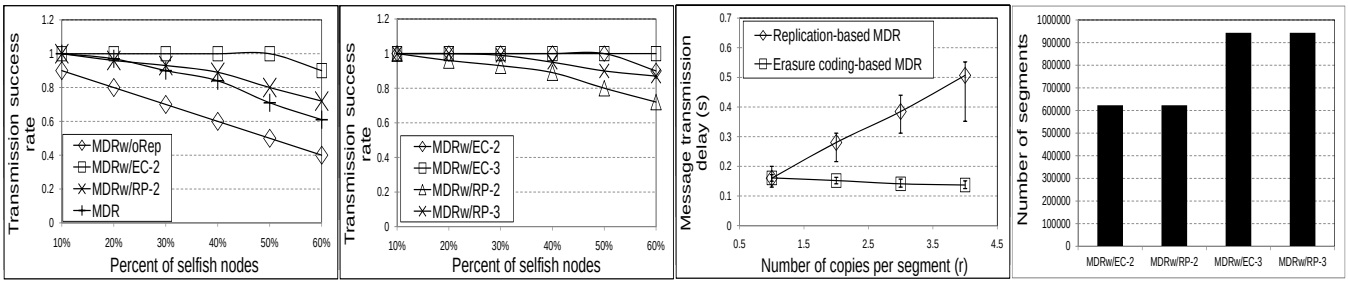
Figure 6(d) shows that the overhead rate of *Hybrid* is much higher than that of MDR. In addition, the overhead rate of MDR remains nearly the same whereas that of *Hybrid* increases sharply as the number of source nodes grows. Recall that MDR does not need to maintain and discover routes for transmissions. Its number of control messages remains the same and its overhead rate is very low regardless of the transmission load. In contrast, *Hybrid* is under the heavy burden of discovering and maintaining routes, which generates many control messages. These results confirm that MDR produces much less overhead than *Hybrid*.

5.3 Evaluation of the Erasure Coding-based DRA

In this experiment, we compare the effectiveness of erasure coding with replication in their ability to enhance routing reliability. With replication [43], multiple replicas of a segment are transmitted to increase the reliability. Erasure coding-based DRA needs to transmit n_r coded segments for a message D consisting of m segments. To achieve the same transmission overhead as erasure coding-based DRA (i.e., total n_r segments for a message transmission), replication-based DRA replicates every segment of the m segments for $\frac{n_r-m}{m}$ times, and these replicas are distributively transmitted to the destination. Because the whole message is divided to m segments, it needs to transmit m different segments to the destination for a successful message transmission. Specifically, We divide each message into $m = 10$ segments in *MDR* and *MDRw/oRep*. We use *MDRw/EC-2* and *MDRw/RP-2* to denote MDR using erasure coding and replication techniques with replication factor r=2, respectively. That is, *MDRw/RP-2* creates a replica for each segment in m segments.

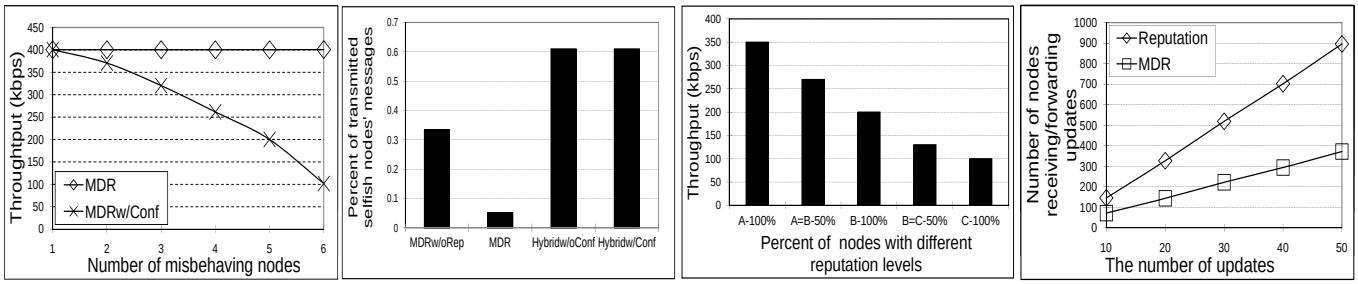
We define the *success rate* as the percent of the received non-duplicated segments used for message recovery among all original segments. Figure 7(a) compares the success rate of different methods versus the percent of selfish nodes in the system. The figure shows that the success rate follows *MDRw/EC-2*>*MDRw/RP-2*>*MDR*>*MDRw/oRep*. For *MDRw/EC-2*, since any m received segments can recover the original message, its success rate is the highest and it can tolerate up to 50% selfish nodes in the system. For *MDRw/RP-2*, only m different segments can recover the original message. Therefore, its success rate is much lower than *MDRw/EC-2*, especially when selfish nodes constitute a large portion of the network. Using the replication technique,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2014.2320255, IEEE Transactions on Mobile Computing



(a) Success rate (b) Effect of the number of copies (c) Delay (d) Number of segments

Fig. 7: Effectiveness of the erasure coding-based DRA in MDR.



(a) Throughput (b) Economic trading (c) Reputation versus throughput (d) Overhead

Fig. 8: Effectiveness and efficiency of the EARM reputation management system.

MDRw/RP-2 produces a higher success rate than *MDR*. *MDR* increases the success rate of *MDRw/oRep* by forwarding the segments to high-reputed nodes. We can see that the success rates of all methods drop as the number of selfish nodes increases since more selfish nodes lead to more dropped messages. Since *MDRw/oRep* does not have any mechanism to avoid transmitting segments to selfish nodes, its success rate decreases dramatically.

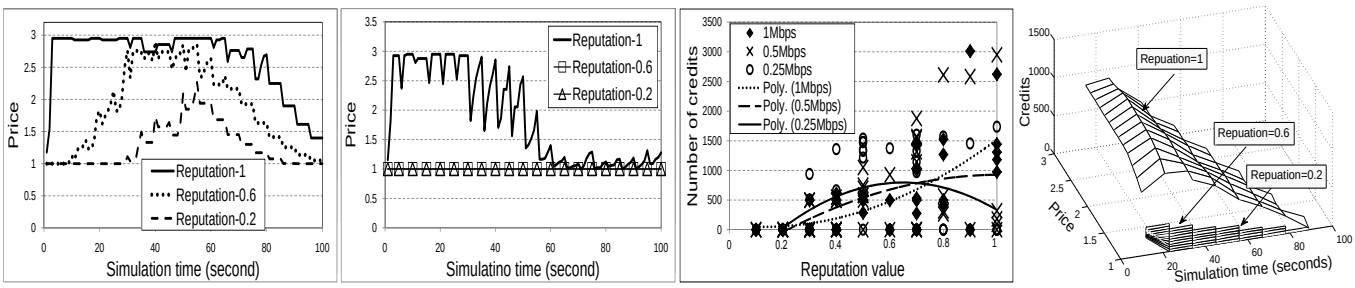
To evaluate the effect of the number of segment copies on the effectiveness of erasure coding and replication, we varied the value of the replication factor r and tested the success rate accordingly. Figure 7(b) shows that *MDRw/EC-2* and *MDRw/EC-3* exhibit approximately the same performance except for when the percentage of selfish nodes in the network reaches 60%. This means when the selfish nodes occupy no more than half of the total nodes, $r = 2$ is sufficient to ensure successful transmission. Also, higher r with more segment copies helps enhance routing reliability. The figure also shows that *MDRw/RP* leads to lower success rate than *MDRw/EC*, and *MDRw/RP-3* generates higher success rate than *MDRw/RP-2*. This is because to successfully transmit a message, *MDRw/RP* requires the arrival of different m segments while *MDRw/EC* only requires the arrival of any m segments. This is also the reason that more replicas in replication help achieve a higher success rate.

Figure 7(c) plots the average, maximum and minimum delay of *MDRw/EC* and *MDRw/RP* versus the number of copies per segment (i.e., r) when the percentage of selfish nodes in a system is 40%. The figure shows that as r increases, the delay of *MDRw/EC* decreases whereas the delay of *MDRw/RP* increases. Also, *MDRw/EC* exhibits a smaller variance than *MDRw/RP*. More segments being transmitted in the system lead to a higher queuing delay of the messages in the nodes. Since *MDRw/RP* requires the destination to receive m different segments of a message before recovering it, the total transmission delay is increased. *MDRw/EC* can recover the original message using the first m arriving segments, so more copies help reduce the delay. This is also the reason why *MDRw/EC* has a smaller variance in delay than *MDRw/RP*. Figure 7(d) further shows the total number of segments in *MDRw/EC-2*, *MDRw/EC-3*, *MDRw/RP-2* and *MDRw/RP-3*. We see that *MDRw/EC-3* and *MDRw/RP-3* generate much more traffic than *MDRw/EC-2* and *MDRw/RP-2*. From the previous results, we know that in *MDRw/EC*, when the percent of selfish nodes is small, r does not need to be set to a large value which otherwise produces more segments and hence more forwarding overhead. In *MDRw/RP*, larger r leads to higher transmission success rate, but at the cost of more forwarding overhead.

5.4 Evaluation of the EARM Reputation System

To test the performance of EARM in preventing false reputation reports compared to *Confidant*, we measured the throughput of MDR and *MDRw/Conf* with the presence of false reputation reporting nodes. In this experiment, we randomly chose a number of nodes to act as misbehaving nodes that always report a high reputation values for their low-reputed neighbors in an attempt to increase their reputation values in reputation exchange in *MDRw/Conf*. Figure 8(a) shows the throughput of MDR and *MDRw/Conf* with a different number of misbehaving nodes. We can see that the throughput of MDR is significantly higher than *MDRw/Conf*. *Confidant* is unable to identify false information by relying on neighbor information exchanges for reputation evaluation. Thus, a node's reputation value may not be accurate enough to reflect its behavior and the selfish nodes may be considered as reputed nodes for data forwarding. As a result, *MDRw/Conf* leads to lower throughput. EARM calculates a node's reputation value based on global information of its actual forwarded data length with the aid of LP2P. Thus, EARM provides more accurate reputation evaluation for nodes. Even if relay nodes send bogus packets or insert junk data into the packets to earn higher reputation or drop packets, the hash chain mechanism can detect such misbehavior. Further, MDR also compares the source nodes' reported relay activities with the BSes' reported relay activities to avoid such misbehavior. In this way, MDR also can detect

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2014.2320255, IEEE Transactions on Mobile Computing



(a) Price (forwarding rate=0.25Mbps) (b) Price (forwarding rate=1Mbps) (c) Credits vs. reputation (d) Credits vs. price vs. reputation

Fig. 9: Effectiveness of the TMM trading market model.

false information from source nodes that report fewer forwarded packets in order to pay less.

In this experiment, one selfish source node continuously sent out messages and two other high-reputed source nodes periodically sent out messages. The selfish node initially only had 100 credits and the high-reputed nodes had sufficient credits to support their data transmission. Figure 8(b) shows the percent of successfully transmitted messages of selfish nodes among all successfully transmitted messages. We can observe that MDR leads to a lower percent rate than *MDRw/oRep*. *Hybridw/oRep* and *Hybridw/Conf* produce the highest percent rates. Since every node needs to pay credits for message forwarding in MDR, when the selfish node's credits are used up, it is unable to transmit its messages. In other methods, the selfish node's messages constitute a large percent of all the transmitted messages. The reason *Hybrid* generates a higher percent rate than *MDRw/oRep* is because the selfish node's large amount of messages are likely to congest node channels, leading to message drops. MDR's distributed routing avoids generating congestions.

The next experiment investigates how a node's reputation level impacts the throughput in MDR. We assigned three reputation levels, A, B and C, to a certain percentage of nodes in the system. Nodes with A, B and C levels have probabilities randomly chosen in $[1, 0.9], [0.9, 0.8]$ and $[0.8, 0.7]$ to forward a received segment, respectively. We use "A-100%" to represent the scenario that 100% nodes have reputation level A and the same is applied to other notations. Figure 8(c) illustrates the throughput of various scenarios. We can see that more high-reputed nodes lead to higher throughput. Recall that high-reputed nodes can receive more bandwidth from BSes and low-reputed nodes tend to drop transmission data. Therefore, more high-reputed nodes in the system help increase the throughput. These results imply that the throughput of a system can be enhanced by choosing relay nodes with high reputation levels. The results also confirm the effectiveness of assigning different bandwidth to nodes based on their reputations in MDR.

In *Confidant*, neighbors exchange reputation information. After node n_i locally updates the reputation of its neighbor n_j, node n_i sends the update to its neighbors, which update node n_j's reputation and notify their neighbors. This process is repeated. In EARM, BSes that have received messages from node n_j send its updated local reputation to node n_j's owner BS using `Insert(`ID_i`,`R_i`)`, which calculates node n_j's global reputation. In order to evaluate the overhead of both methods, we varied the number of updates of each node during the simulation time from 10 to 50 with an increment step of 10 and recorded the total number of nodes that have received or forwarded all the updates. We set the number of hops for update forwarding in *Confidant* to 3. Figure 8(d) shows that the total number of nodes receiving/forwarding the updates increases as the number of initiated updates grows. Also, the experimental result in *Confidant* is much higher than MDR. In MDR, when a BS wants to update the reputation of another node, it only needs to send one message which is forwarded for $\log N_b$ hops on average, where N_b is the number of BSes. Reputation exchange in *Confidant* generates many messages. The result implies that by taking advantage of the BSes in a hybrid network, EARM leads to a much lower overhead than *Confidant* in reputation information collection and update.

5.5 Evaluation of the Basic TMM Trading Market Model

In Formula (1) for the price determination, we set $\delta = 4$, $\alpha = 0.5$ and $\bar{p} = 1$. We randomly selected these parameter values within reasonable value ranges. We assigned each node 500 credits initially and chose 7 source nodes every second for message transmission. We set the transmission rate of nodes to 0.2Mbps. Figure 9(a) shows the price of three nodes randomly selected from node groups with R=1, 0.6, and 0.2, respectively. We can see that for the node with $R = 1$, its price is quickly raised to 3. This is because the node's high reputation attracts many service requests when its price is affordable. According to Formula (1), a longer queuing length leads to a higher price. Then, its price fluctuates around 3, which is the supply and demand equilibrium point. When the node receives more service requests, it increases its price to reduce the number of requests and when it receives fewer service requests, it decreases its price to attract more service requests. After that, the price gradually drops. This is because more and more nodes cannot afford the high-reputed node's service as they are consuming their credits. Short queuing length leads to low price, which helps attract more requests. When some nodes cannot afford a high price, they will select lower-reputed nodes that offer lower prices. Therefore, the price of the node with $R = 0.6$ increases later on. The node's supply and demand equilibrium price point is 2.7. For the same reason, the price of the node with $R = 0.2$ subsequently increases. As the figure shows, the node gradually reduces its price to attract more requests when it has not received requests for 60 seconds.

Figure 9(b) shows the change of the service price of the selected three nodes when the forwarding rate is 1Mbps. We observe that the prices of the nodes with $R = 0.6$ and $R = 0.2$ stay at the base price of 1, while the price of the node with $R = 1$ is greater than 1 before 60 seconds. Compared to Figure 9(a), a higher forwarding rate in Figure 9(b) implies shorter service latency for each segment. Then, the queues of high-reputed forwarding nodes are less likely to be congested, leading to a lower

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2014.2320255, IEEE Transactions on Mobile Computing

price. Comparatively, a reasonable price and a high QoS of the high-reputed node attract most service requests, while the lower-reputed nodes hardly receive service requests and thus keep the base price. The figure also shows that the price of the high-reputed node fluctuates between 2-3 due to the adaptive price adjustment.

Figure 9(c) plots the credits of each node when the simulation ran 100 seconds versus the node's reputation with the forwarding rate was set to 1Mbps, 0.5Mbps and 0.25Mbps, respectively. "*Poly. (1Mbps)*" denotes the linear regression curve for the experimental results with forwarding rate 1Mbps based on the Polynomial distribution model [40]. The same applies to the other denotations. The figure shows that the number of credits of a node increases as the node reputation increases when the forwarding rate is 1Mbps and 0.5Mbps. A higher-reputed node receives more requests, which leads to higher price and more earned credits. The figure also shows that higher forwarding rate leads to a higher credit increasing rate. A higher forwarding rate for a node leads to a shorter queuing length and lower prices, which attracts many requests. It is intriguing to see that when the forwarding rate decreases to 0.25, the nodes with median reputation values have more credits. This is because when the packet forwarding rate is small, the queue of a forwarding node is very likely to become congested. Then, a high-reputed node increases its price to reduce the number of requests it receives. Subsequently, many nodes resort to median-reputed nodes with lower price.

Figure 9(d) shows the change of price and credits versus the simulation time when the forwarding rate is 1Mbps. The figure shows that there is a positive correlation between price and credits in the nodes with reputation equals to 1 due to the same reasons explained in Figure 9(a). The figure also shows that although the low-reputed nodes gain a small amount of credits, their price is kept at the base price 1. Because the prices of the high-reputed nodes are low, low-reputed nodes receive few requests and they keep the lowest price in order to attract more requests.

5.6 Evaluation of the Market-based Policies

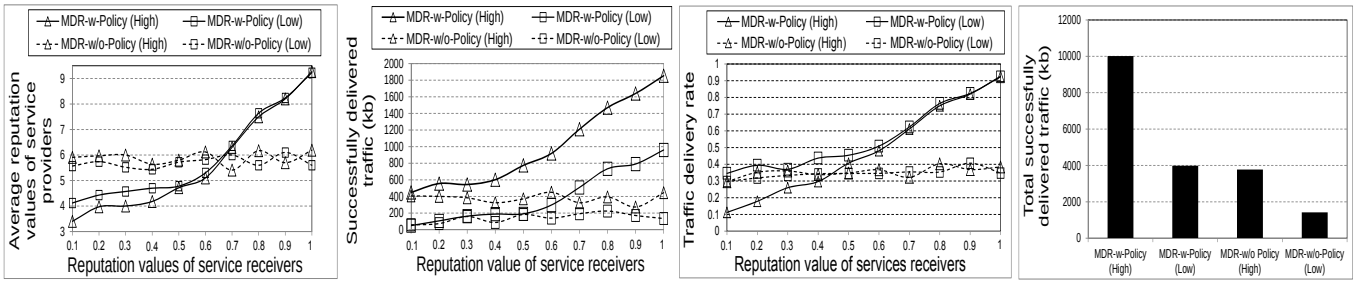
In this section, we evaluate the effectiveness of the two market-based policies on enforcing the effectiveness and fairness of cooperation incentives. We randomly assigned the nodes in the system with a reputation value within [0.1-1]. A node with reputation R has probability of R to forward a packet to a BS. The entire simulation area was divided into two regions, a low-traffic region and a high-traffic region. We randomly assigned 30% of the nodes to the low-traffic region and 70% of the nodes to the high-traffic region. Initially, we set the queue length of each node to 50 messages and assigned 100 credits to each node. Each node determines its service price based on Formula (1) with $\alpha = 0.8$ and $\delta = 6$. The price ceiling was set to 1.5 and the tax rate for all nodes was set to 5%. We randomly selected these parameter values within reasonable ranges. Each node whose reputation value is larger than 0.6 is subsidized with 50 credits in every 10 seconds. The total simulation time was 60 seconds. In each second, every node sent out 5 packets to a neighboring node. A node chose its neighbor with the highest reputation value within its transmission range to send packets. When node n_j receives several requests from other nodes, it accepts the requests in the order from requesters with higher reputations to lower reputations until its queue is full. Node n_j then sends its service price to its selected requesters. If a requester can afford the price, it sends its packet to node n_j; otherwise, it informs node n_j. Node n_j then selects other requesters until its queue is full, and sends "reject" messages to other requesters. The requesters whose packets fail to send out due to full queues or unaffordable prices will try to send out these packets in the next second. We use MDR-w-Policy (High) and MDR-w-Policy (Low) to denote the MDR protocol with the proposed two market-based policies in the high-traffic region and low-traffic region, respectively. We also use MDR-w/o-Policy (High) and MDR-w/o-Policy (Low) to denote the MDR protocol without the two market-based policies in the high-traffic region and low-traffic region, respectively.

For all pairs of service receiver-provider, we grouped the service providers for the service receivers with the same reputation value, and then calculated the average reputation of each group of providers. Figure 10(a) plots the average reputation value of each service provider group versus the reputation value of the group's corresponding service receivers. We see that in MDR-w/o-Policy (High) and MDR-w/o-Policy (Low), the average reputation values of the service providers maintain around 6. In contrast, in MDR-w-Policy (High) and MDR-w-Policy (Low), higher-reputed nodes receive services from higher-reputed service providers and vice versa. That is, the two market policies can enable more cooperative nodes to receive higher-QoS services even in the low-traffic region, while constraining more uncooperative nodes to lower-QoS services.

In MDR-w/o-Policy, as no service priority is given to cooperative nodes, wealthy uncooperative nodes can also buy services from high-reputed nodes. Also, as there is no tax, some uncooperative nodes have more opportunities to earn many credits to buy high-QoS services. In addition, as no subsidy is given to cooperative nodes in the low-traffic region, poor cooperative nodes can only buy services from low-reputed nodes due to high service price of high-reputed nodes. Therefore, the reputation value of the service requesters does not affect their received QoS. In MDR-w-Policy, the price ceiling policy (in Policy 1) bounds the service price, so that poor cooperative nodes can afford the service from high-reputed nodes. As explained in Section 2.4.2, the price ceiling policy will lead to a shortage of the services provided by high-reputed nodes, and with the service priority policy (in Policy 1) that high-reputed nodes have higher priority to buy services, the higher-reputed nodes in MDR-w-Policy can purchase more services from higher-reputed nodes compared to MDR-w/o-Policy. We can also see from the figure that in MDR-w/o-Policy, the average reputation values of the service providers in the low-traffic region is slightly lower than those in the high-traffic region. This is because the nodes in the low-traffic region do not have enough credits to purchase high-QoS services. In MDR-w-Policy, the average reputation values of the service providers in the low-traffic region is higher than those in the high-traffic region for low-reputed service requesters. As the high reputed nodes in the low-traffic region are not likely to be congested since the traffic is low, more low-reputed nodes can purchase services from high-reputed nodes.

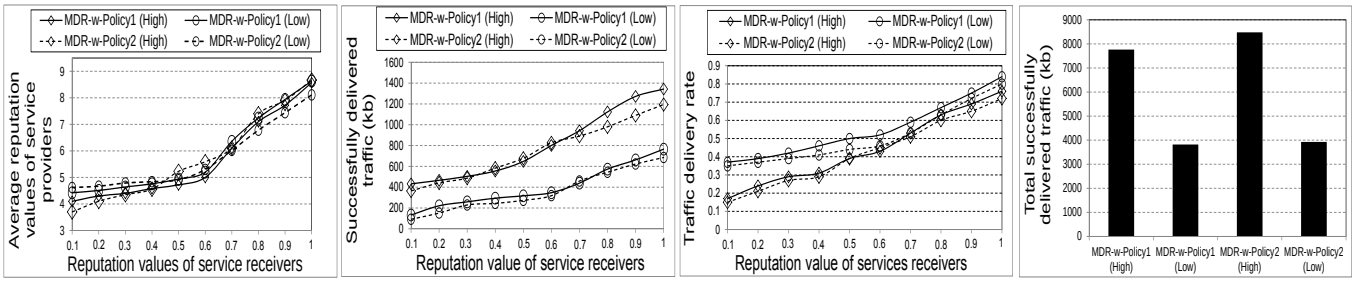
We grouped service receivers based on their reputation values, and calculated the sum of successfully delivered traffic of the nodes in each group. Figure 10(b) shows the total successfully delivered traffic of each group of service receivers versus each group's reputation value. We can observe similar experimental results from the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2014.2320255, IEEE Transactions on Mobile Computing



(a) Reputation of service providers (b) Total traffic of service receivers (c) Traffic delivery rate of service receivers (d) Total delivered traffic

Fig. 10: Effectiveness of the market-based policies.



(a) Reputation of service providers (b) Total traffic of service receivers (c) Traffic delivery rate of service receivers (d) Total delivered traffic

Fig. 11: Effectiveness of the individual market-based policies.

figure as those in Figure 10(a). That is, the total successfully delivered traffic in both MDR-w/o-Policy (High) and MDR-w/o-Policy (Low) maintains nearly constant, while in MDR-w-Policy (High) and MDR-w-Policy (Low), higher-reputed nodes have higher total successfully delivered traffic while lower-reputed nodes have lower total successfully delivered traffic. The reasons are the same as those in Figure 10(a). Also, MDR-w-Policy (High) generates more total successfully delivered traffic than MDR-w-Policy (Low) due to the heavier traffic in the high-traffic region. The experimental results in Figure 10(a) and Figure 10(b) imply that the two market policies enable high-reputed nodes to receive higher-QoS and vice versa no matter in the low-traffic region or in the high-traffic region. Without the two policies, the QoS received by both high-reputed and low-reputed nodes is similar and every node has the same chance to buy service from high-reputed nodes.

Figure 10(c) shows the traffic delivery rate of each of the groups of service receivers versus the group's reputation value. We can see that as the reputation value of the service receivers increases, the traffic delivery rate increases in both MDR-w-Policy (High) and MDR-w-Policy (Low), but the traffic delivery rates of MDR-w/o-Policy (High) and MDR-w/o-Policy (Low) maintain nearly constant. The reason is the same as Figure 10(a). The figure also shows that the low-reputed nodes in MDR-w-Policy (High) have lower traffic delivery rate than in MDR-w-Policy (Low). Since in the high-traffic region, the low-reputed nodes have low priority in service competition and they cannot receive subsidy, they have to buy service from low-reputed nodes which have low packet forwarding probability. In the low-traffic region, nodes do not receive many requests, thus the low-reputed nodes are able to purchase service from high-reputed nodes, which leads to a higher traffic delivery rate for low-reputed nodes. These experimental results further confirm the effectiveness of the two market-based policies in strengthening cooperation incentives.

Figure 10(d) shows the total amount of successfully delivered traffic in MDR-w-Policy and MDR-w/o-Policy. We see that the experimental results in the figure are consistent with those in Figure 10(b). That is, MDR-w-Policy generates more successfully delivered traffic than MDR-w/o-Policy and the high-traffic area generates more successfully delivered traffic than the low-traffic area. The latter result is caused by the reason that more traffic is initiated in the high-traffic area than in the low-traffic area. In MDR-w-Policy, because of the two market-based policies, reputed-nodes are able to buy high-QoS service with high probability of successful forwarding, generating much successfully delivered traffic. In contrast, in MDR-w/o-Policy, both high-reputed nodes and low-reputed nodes are not able to buy high-QoS services due to lack of credits. In the low-traffic area, nodes have few chances to earn credits due to few service requests. The price offered by the nodes in the high-traffic region is normally higher than the price in the low-traffic region because the high service demand in the high-traffic area makes high-reputed nodes have higher prices based on Equation (1). Therefore, nodes also have fewer chances to buy high-QoS in the high-traffic region in MDR-w/o-Policy.

In order to show the effect of the individual market-based policy, we conducted experiments with only Policy 1 and with only Policy 2, respectively. Figure 11 shows the experimental results with the same metrics as in Figure 10. MDR-w/-Policy1 and MDR-w/-Policy2 represent MDR with only Policy 1 and with only Policy 2, respectively. Comparing each figure in Figure 11 with corresponding figure in Figure 10, we see that each policy is effective in encouraging cooperation and discouraging selfish behaviors, and the combination of the effect of both policies strengthen the final effectiveness.

6 Related Work

In recent years, extensive research has been conducted on hybrid wireless networks (i.e., multi-hop cellular networks). Lin *et al.* [3] proposed the first hybrid wireless network, in which the service infrastructure is constructed by fixed BSes and multi-hop wireless transmission in the MANET through MNs to BSes is used. Shin *et*

al. [4] developed an infrastructure using multi-antenna BSes to improve the throughput scaling in networks with randomly located wireless nodes. Asadi *et al.* [5] proposed a two-tier uplink forwarding scheme in hybrid wireless networks. Wu *et al.* [6] developed an analytical model to investigate the QoS of the hybrid wireless networks. Wang *et al.* [7] studied achievable multicast throughput for the hybrid wireless network. Shila *et al.* [8] established the same cell routing policy with multi-hop uplinks and studied the bounds on throughput and delay of this policy. The research in [9]–[11] tries to improve the capacity of conventional cellular networks by allowing ad-hoc communications between certain sources and destinations without the help of BSes so as to relieve their relay burden. Li *et al.* [12] attempted to explore the capacity of multi-hop cellular networks with all traffic going through BSes and ad hoc transmissions only acting as relay. Lorenzo *et al.* [13] presented an approach to optimize the throughput of multicast in multi-hop cellular networks by applying a hexagonal tessellation to partition the cell into smaller subcells.

However, most of the hybrid wireless networks simply combine the transmission modes of MANETs and infrastructure networks for routing. Thus, they inherit the drawbacks of ad-hoc transmission modes, such as congestion and a high overhead for route discovery and maintenance. MDR synergistically integrates the two data transmission modes by taking advantage of the widespread BSes while avoiding the drawbacks of ad-hoc routing. Wei and Gitlin [1] proposed a two-hop transmission scheme to eliminate multi-hop route maintenance overhead. However, their work focuses on one-cell networks while MDR is geared towards multi-cell networks. The single-relay feature of the MDR routing scheme also facilitates the effective reputation management and trading market management in MDR.

Cooperation incentives are needed to encourage cooperation between MNs in routing. Li *et al.* [44] proposed a self-enforcing incentive scheme in hybrid cellular networks, which comprises a global stimulating policy among coalitions and local allocating rule within each coalition. In multi-hop cellular networks, Kim [45] developed a trust model, in which the BSes appropriately react to selfish relay stations to maximize network performance. Reputation systems and price systems are two main methods to provide cooperation incentives. Many reputation systems [14]–[24] have been proposed for wireless networks. In most current reputation systems, each node periodically exchanges local reputation information with its neighbors and aggregates it to yield others' reputation values, which are referred for forwarder selection in routing. However, using local partial information for reputation evaluation may result in an insufficiently accurate reputation value. Also, this frequent information exchange generates high overhead. Furthermore, the reputation systems cannot avoid falsely reported reputation information and cannot effectively provide incentives for cooperation. MDR's novelty relies on a P2P structure to avoid frequent information exchange and provide more accurate reputation values based on globally collected information and nodes' actual relayed messages.

In the price-based systems [46]–[59], nodes are paid for offering packet forwarding service and pay for receiving forwarding service. The payments can be in money, stamps, points or similar objects of value. The previous price-based works focus on the payment method while MDR focuses on price determination based on supply and demand equilibrium, which can serve as a complement to these works. MDR novelly allows nodes to adaptively adjust their price to control their loads. It also exploits the integration of the market model and reputation system for fostering cooperation incentives. As far as we know, MDR is the first work that investigates the market policies in cooperation encouragement in hybrid wireless networks.

7 Conclusions

We propose a P2P-based Market-guided Distributed Routing mechanism (MDR) to improve the throughput of hybrid wireless networks, where channel resources are stringent and nodes may not cooperate in data forwarding. Current routing algorithms for hybrid networks do not fully exploit the BSes for efficient routing. Also, current reputation systems are not sufficiently efficient and effective for reliable routing. We fully utilize the BSes by forming them into a locality-aware P2P overlay (LP2P), on which we develop a distributed routing algorithm (DRA), efficient and accurate reputation system (EARM) and trading market model (TMM). DRA splits packet stream based on erasure coding, transmits data in a distributed manner, selects relay nodes guided by EARM and TMM, and relies on LP2P to collect distributed segments at the destination. EARM is superior to current reputation systems due to its efficient reputation information collection, querying based on LP2P, and more accurate reputation values calculated based on global information of actual relayed packets of relay nodes. TMM strengthens the incentives for node cooperation in routing by new market-based policies. These MDR components coordinately contribute to efficient and reliable routing for high throughput. In our future work, the impact between DRA, EARM and TMM will be further studied. Like other reputation systems, EARM in MDR is not completely bullet-proof though we briefly discussed the strategies to prevent misbehaviors. Misbehaviors to gain fraudulent benefits in EARM and corresponding strategies to prevent the misbehaviors will be investigated. Also, we will investigate how to adapt EARM and TMM to multi-hop routing.

Acknowledgements

This research was supported in part by U.S. NSF grants IIS-1354123, CNS-1254006, CNS-1249603, CNS-1049947, CNS-0917056, CNS-1025652 and Microsoft Research Faculty Fellowship 8300751. An early version of this work was presented in the Proceedings of SECON'12 [60].

References

[1] Y. Wei and D. Gitlin. Two-hop-relay architecture for next-generation WWAN/WLAN integration. *IEEE Wireless Communication*, 2004.

[2] S. Olariu and M. C. Weigle. vehicular networks from theory to practice. *Chapman and Hall/CRC*, 2009.

[3] Y. D. Lin and Y. C. Hsu. Multi-hop cell: A new architecture for wireless communications. In *Proc. of INFOCOM*, 2000.

[4] W. Shin, S. Jeon, N. Devroye, M. Vu, S. Chung, Y. Lee, and V. Tarokh. Improved Capacity Scaling in Wireless Networks With Infrastructure. *TIT*, 57(8):5088–5102, 2011.

[5] A. Asadi and V. Mancuso. Energy efficient opportunistic uplink packet forwarding in hybrid wireless networks. In *Proc. of e-Energy*, 2013.

[6] Y. Wu, G. Min, and L. Yang. Performance Analysis of Hybrid Wireless Networks Under Bursty and Correlated Traffic. *TVT*, 2013.

[7] C. Wang, C. Jiang, X. Li, and Y. Liu. On multicast throughput scaling of hybrid wireless networks with general node density. *Computer Networks*, 55(15):3548–3561, 2011.

[8] D. Shila, Y. Cheng, and T. Anjali. Throughput and delay analysis of hybrid wireless networks with multi-hop uplinks. In *Proc. of Infocom*, 2011.

[9] C. Zhang P. Li and Y. Fang. Capacity and delay of hybrid wireless broadband access networks. *IEEE JSAC*, 2009.

[10] P. Li and Y. Fang. Impacts of topology and traffic pattern on capacity of hybrid wireless networks. *IEEE TMC*, 2009.

[11] X. Wang G. Zhang, Y. Xu and M. Guizani. Capacity of hybrid wireless networks with directional antenna and delay constraint. *IEEE Transactions on Communications*, 2010.

[12] P. Li, X. Huang, and Y. Fang. Capacity scaling of multihop cellular networks. In *Proc. of Infocom*, 2011.

[13] B. Lorenzo and S. Glisic. Context-aware nanoscale modeling of multicast multihop cellular networks. *IEEE/ACM TON*, 2012.

[14] Y. Liu, K. Li, Y. Jin, Y. Zhang, and W. Qu. A novel reputation computation model based on subjective logic for mobile ad hoc networks. *FGCS*, 27(5):547–554, 2011.

[15] T. Chen, A. Bansal, and S. Zhong. A reputation system for wireless mesh networks using network coding. *JNCA*, 34(2):535–541, 2011.

[16] S. Buchegger and J.-Y. L. Boudec. Performance analysis of the confidant protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks. In *Proc. of Mobihoc*, 2003.

[17] B. Zong and F. Xu and J. Jiao and J. Lv. A Broker-Assisting Trust and Reputation System Based on Artificial Neural Network. In *Proc. of SMC*, 2009.

[18] M. T. Refaei and L. A. DaSilva and M. Eltoweissy and T. Nadeem. Adaptation of Reputation Management Sytems to Dynamic Network Conditions in Ad Hoc Networks. *IEEE TOC*, 2010.

[19] M. T. Refaei, L. A. DaSilva, M. Eltoweissy, and T. Nadeem. Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks. *TC*, 2010.

[20] T. Chen, F. Wu, and S. Zhong. FITS: A Finite-Time Reputation System for Cooperation in Wireless Ad Hoc Networks. *TC*, 2011.

[21] F. Li and J. Wu. Uncertainty Modeling and Reduction in MANETs. *TMC*, 9(7):1035–1048, 2010.

[22] R. Akbani, T. Korkmaz, and G. Raju. EMLTrust: An enhanced Machine Learning based Reputation System for MANETs. *Ad Hoc Networks*, 10(3):435–457, 2012.

[23] T. Lacey, R. Mills, B. Mullins, R. Raines, M. Oxley, and S. Rogers. RIPsec - Using reputation-based multilayer security to protect MANETs. *Computers & Security*, 31(1):122–136, 2012.

[24] P. Bedi, Aakanksha, and R. Sharma. Trust and context view-based knowledge sharing in MANETs. *TIE*, 1(1):85–103, 2013.

[25] Y. Wang, S. Jain, M. Martonosi, and K. Fall. Erasure-coding based routing for opportunistic networks. In *Proc. of SIGCOMM*, 2005.

[26] H. Shen and C. Xu. Locality-aware and churn-resilient load balancing algorithms in structured peer-to-peer networks. *TPDS*, 2007.

[27] Z. Xu, M. Mahalingam, and M. Karlsson. Turning heterogeneity into an advantage in overlay routing. In *Proc. of INFOCOM*, 2003.

[28] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier. Hierarchical Mobile IPv6 (HMIPv6) Mobility Management. *RFC 5380 (Proposed Standard)*, 2008.

[29] J. M. Perloff. Microeconomics: Theory and Applications with Calculus. *Addison Wesley*, 2007.

[30] Haiying Shen and Ze Li. Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 11(8):1287–1303, 2012.

[31] P. J. Welch and G. F. Welch. Economics: Theory and Practice. *Wiley, ISBN-10: 0471679461*, 2006.

[32] J. Katz and Y. Lindell. *Introduction to Modern Cryptography: Principles and Protocols*. Chapman and Hall/CRC, 2007.

[33] J. Grossschadl, A. Szekely, and S. Tillich. The energy cost of cryptographic key establishment in wireless sensor networks. In *Proc. of ASIACCS*, 2007.

[34] L. Lamport. Password authentication with secure communication. *Communication of ACM*, 1981.

[35] T. Ojanper and R. Mononen. Security and authentication in the mobile world. *Wireless Personal Communications*, 2004.

[36] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks. In *Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications*, WMCSA '02, pages 3–, Washington, DC, USA, 2002. IEEE Computer Society.

[37] Hamed Janzadeh, Kaveh Fayazbakhsh, Mehdi Dehghan, and Mehran S. Fallah. A secure credit-based cooperation stimulating mechanism for manets using hash chains. *Future Gener. Comput. Syst.*, 25(8):926–934, September 2009.

[38] A.S. Wander, N. Gura, H. Eberle, V. Gupta, and S.C. Shantz. Energy analysis of public-key cryptography for wireless sensor networks. In *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*, pages 324–328, March 2005.

[39] R. L. Freeman. *Fundamentals of Telecommunications*. Wiley-IEEE Press, 2005.

[40] S. Ross. A first course in probability, sixth edition. 2002.

[41] The network simulator ns-2. http://www.isi.edu/nsnam/ns/.

[42] E. Hyyti and J. Virtamo. Random waypoint model in n-dimensional space. *Operations Research Letters*, 2005.

[43] K. Chen and H. Shen. Global Optimization of File Availability Through Replication for Efficient File Sharing in MANETs. In *Proc. of ICNP*, 2011.

[44] C. Li, Z. Yang, and F. Tian. A Relaying Incentive Scheme for Multihop Cellular Networks Based on Coalition Game with Externalities. *Wireless Personal Communications*, 58(4):785–805, 2011.

[45] S. Kim. Reversed Stackelberg bandwidth-sharing game for cognitive multi-hop cellular networks. *IET*, 6(17):2907–2913, 2012.

[46] M. Mahmoud and X. Shen. FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Multihop Cellular Networks. *TMC*, 11(5):753 – 766, 2012.

[47] H. Janzadeh and K. Fayazbakhsh and M. Dehghan and M. S. Fallah. A Secure Credit-Based Cooperation Stimulating Mechanism for MANETs Using Hash Chains. *Elservier*, 2009.

[48] L. Chen, L. Libman, and J. Leneutre. Conflicts and Incentives in Wireless Cooperative Relaying: A Distributed Market Pricing Framework. *TPDS*, 22:758–772, 2011.

[49] M. Rasti, A.R. Sharafat, and B. Seyfe. Pareto-efficient and Goal-Driven Power Control In Wireless Networks: A Game-Theoretic Approach With A Novel Pricing Scheme. *TON*, 2009.

[50] F. Wu, T. Chen, S. Zhong, L. (E.) Li, and Y. R. Yang. Incentive-compatible Opportunistic Routing For Wireless Networks. In *Proc. of MOBICOM*, 2008.

[51] D. Yang, X. Fang, and G. Xue. Truthful Auction for Cooperative Communications. In *Proc. of MobiHoc*, 2011.

[52] L. Chen, B. K. Szymanski, and J. W. Branch. Auction-Based Congestion Management for Target Tracking in Wireless Sensor Networks. In *Proc. of PerCom*, 2009.

[53] S. Eidenbenz, G. Resta, and P. Santi. The COMMIT Protocol for Truthful and Cost-Efficient Routing in Ad Hoc Networks with Selfish Nodes. *TMC*, 7(1):19–33, 2008.

[54] Y. Cui, T. Ma, and X. Cheng. Multi-hop Access Pricing in Public Area WLANs. In *Proc. of INFOCOM*, 2011.

[55] X. Ai, V. Srinivasan, and C. K. Tham. Wi-sh: A Simple, Robust Credit Based Wi-Fi Community Network. In *Proc. of INFOCOM*, 2009.

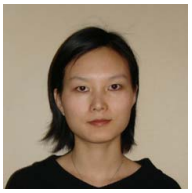
[56] R. Lu, X. Lin, H. Zhu, X. Shen, and B. Preiss. Pi: A Practical Incentive Protocol for Delay Tolerant Networks. *TWC*, 2010.

[57] B. B. Chen and M. C. Chan. MobiCent: a Credit-Based Incentive System for Disruption Tolerant Network. In *Proc. of INFOCOM*, 2010.

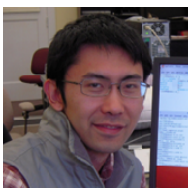
[58] U. Shevade, H. H. Song, L. Qiu, and Y. Zhang. Incentive-aware routing in DTNs. In *Proc. of ICNP*, 2008.

[59] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen. SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks. *TVT*, 58(8):4628–4639, 2009.

[60] Z. Li and H. Shen. MDR: A p2p-based market-guided distributed routing mechanism for high-throughput hybrid wireless networks. In *Proc. of SECON*, 2012.



Haiying Shen received the BS degree in Computer Science and Engineering from Tongji University, China in 2000, and the MS and Ph.D. degrees in Computer Engineering from Wayne State University in 2004 and 2006, respectively. She is currently an Associate Professor in the Department of Electrical and Computer Engineering at Clemson University. Her research interests include distributed computer systems and computer networks, with an emphasis on P2P and content delivery networks, mobile computing, wireless sensor networks, and cloud computing. She is a Microsoft Faculty Fellow of 2010, a senior member of the IEEE and a member of the ACM.



Ze Li received the BS degree in Electronics and Information Engineering from Huazhong University of Science and Technology, China in 2007, and the Ph.D. degree in Computer Engineering from Clemson University. His research interests include distributed networks, with an emphasis on peer-to-peer and content delivery networks. He is currently a data scientist in the MicroStrategy Incorporation.

Lei Yu received the PhD degree in computer science from Harbin Institute of Technology, China, in 2011. He currently is a post-doctoral research fellow in the Department of Electrical and Computer Engineering at Clemson University, SC, United States. His research interests include sensor networks, wireless networks, cloud computing and network security.