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

Ze Li and Haiying Shen
Department of Electrical and Computer Engineering
Clemson University, Clemson, SC 29631
{zel, shenh}@clemson.edu

***Abstract*—A hybrid wireless network combines a mobile ad-hoc network and an infrastructure network. Efficient and reliable data routing is important for high throughput in such networks. Existing routing schemes that simply combine ad-hoc and infrastructure routings inherit the drawbacks of ad-hoc routing and fail to take advantage of the infrastructure for high efficiency. Current reputation systems relying on local information exchange are not sufficiently effective and efficient in guiding reliable routing. This paper presents a peer-to-peer (P2P)-based Market-guided Distributed Routing mechanism (MDR) to increase the throughput of hybrid networks by achieving a high efficiency and reliability. Taking advantage of the high density of base stations, the packets from a source node are distributively transmitted to base stations directly or indirectly. The packet transmission in MDR is modeled as a market trading behaviors, in which source nodes pay credits to relay nodes. The service price is determined by the supply and demand equilibrium of the nodes in the system. MDR organizes base stations into a P2P structure to facilitate high efficient data operation for service price determination. An erasure coding-based distributed routing algorithm is also proposed to facilitate an efficient and reliable market trading. Theoretical analysis demonstrates the distinguishing features of MDR and simulation results show that MDR outperforms the traditional hybrid routing schemes and reputation systems.**

I. Introduction

A hybrid wireless network is a combination of a mobile ad-hoc network (MANET) and an infrastructure network. In a hybrid network, base stations (BSs) in the infrastructure act as relays for mobile nodes (MNs) in 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, Android and BlackBerry) are capable of seamlessly switching between MANET and 3G cellular network if they are configured properly. Mobile devices are quickly growing in their capabilities, their growth seems to be outpaced by the needs of sophisticated (e.g., multimedia) applications with requirements of a high throughput capacity. A recently released report shows that the mobile data traffic will grow at an annual rate of 40% between 2009 and 2014 and is expected to reach 40 billion gigabytes by 2014 [3]. Thus, an efficient and reliable routing scheme is increasingly needed to achieve high data throughput and support bandwidth-intensive applications. However, current routing schemes in hybrid networks are neither sufficiently efficient nor reliable.

Most of the routing schemes proposed in hybrid networks currently simply combine existing routing schemes in MANETs and infrastructure networks [1], [4]–[11]. As the nodes closer the base station normally has higher transmission rate as well as the WiFi link rate is higher than cellular link rate, a message is forwarded in MANET through WiFi links, then to the BS where the destination MN resides based on routing algorithm in cellular networks, and finally to the destination node. Such routing inherits the problems in ad-hoc routing, such as congestion generation and high overhead for route discovery and maintenance [1]. This prevents hybrid networks from achieving a high throughput. In a hybrid network, BSs are spread over the network. However, most proposed high-throughput routing algorithms are mainly focused on the routing in one single base station [1], [4]–[11] and fail to take advantage of the dispersed BSs for higher efficiency.

Reliable routing is faced with a severe challenge posed by selfish nodes, which tend to not forward data to save resources of their own. To avoid selfish nodes, a routing algorithm can choose high-reputed nodes as relay nodes by depending on reputation systems [12]–[17]. In most current reputation systems, node reputation is evaluated through reputation information exchanged between neighbors. This frequent information exchange generates high overhead and local partial information for reputation evaluation may result in an insufficiently accurate reputation value. Furthermore, the reputation systems cannot avoid falsely reported reputation information and cannot effectively provide incentives for cooperation.

We propose a peer-to-peer (P2P)-based Market-guided Distributed Routing mechanism (MDR) to increase the throughput of hybrid networks by achieving a high efficiency and reliability. Taking advantage of the high density of the base stations, the packet from source nodes are distributed transmitted to base stations through some selected neighbor nodes with higher transmission rate than itself [1]. In MDR, the packet forwarding by neighbors are modeled as a market trading behaviors. Source nodes pay credits to relay nodes and relay nodes charge source nodes for data forwarding services. The

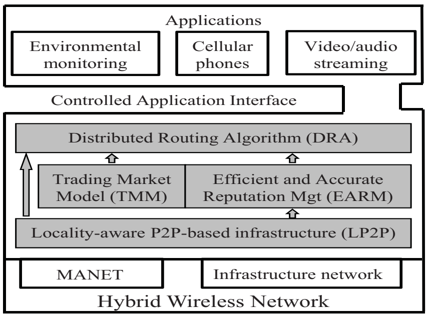


Fig. 1: A high-level view of the MDR.

price of the forwarding services is determined by the supply and demand equilibrium. MDR consists of four components: a trading market model (TMM) and three auxiliary models: a locality-aware P2P-based infrastructure (LP2P), a distributed routing algorithm (DRA) as well as an efficient and accurate reputation management system (EARM) to ensure the efficient and reliable operations of TMM. Figure 1 shows a high-level architecture of MDR. 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 load. TMM fosters the effectiveness in deterring selfish behaviors and providing cooperation incentives. In LP2P, by leveraging the dispersed BSs, LP2P constructs a locality aware structured P2P on the infrastructure component of a hybrid network to support efficient operations for TMM. In DRA, to enable a flexible trading market, DRA uses a erasure coding based distributed two hop routing helps to facilitate the source node to dynamically choose reliable trading partners. In EARM, EARM relies on LP2P to collect global information for more accurate reputation evaluation and efficient reputation querying.

The rest of this paper is organized as follows. Section II presents a review of representative hybrid network routing schemes and approaches for node cooperation. Section III details the MDR mechanism with descriptions of the different MDR components. Section IV shows the performance of MDR in experiments. Finally, Section V concludes the paper with remarks on our plans for future work.

II. Related Work

In order to increase the capacity of wireless networks, hybrid networks with different features have been proposed [1], [4]–[11]. In [4]–[7], the nodes in hybrid networks rely on ad-hoc network routing schemes such as DSDV [18] and AODV [19] in their MANET components. The routing algorithm proposed in [8] uses multi-hop transmission to transfer traffic from "hot" cells to "cold" cells. In the proposed schemes in [9], [10], a node communicates with another node by accessing a BS for routing information. Ioannidis *et al.* [11] proposed a scalable routing protocol for hybrid networks. It maintains a spanning tree of the network rooted at the BSs. Each node maintains an optimal path to a nearby BS through the tree structure. These schemes simply combine the transmission modes of MANETs and infrastructure networks. Thus, they inherit the drawbacks of ad-hoc transmission modes, such as congestion generation and a high overhead for route discovery and maintenance. MDR synergistically integrates the two data transmission modes by taking advantage of the widespread BSs while avoiding the drawbacks of ad-hoc routing. Wei *et al* [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.

Routing schemes can rely on reputation systems [12]–[17] or price systems [20]–[24] to enhance the routing reliability. In reputation systems [12]–[17], node frequent exchange local observation on other nodes to determine the reputation values of other nodes, which generates high overhead. Meanwhile, the local partial information for reputation evaluation may result in an insufficiently accurate reputation value. Furthermore, the reputation systems cannot avoid falsely reported reputation information and cannot effectively provide incentives for cooperation. MDR's novelty relies on P2P to avoid frequent information exchange and provide more accurate reputation values based on collected global information and nodes' actual relayed messages. The price system provide node cooperation incentives using credits or virtual currency payments [20]–[24]. These 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 load. It also exploits the integration of the market model and reputation system for fostering cooperation incentives.

III. MDR: P2P-based Market-guided Distributed Routing Mechanism

Since the packet trading behaviors of the nodes in TMM is based on the efficient and reliable operations of the three auxiliary models. In the sections below, we will firstly introduce the three auxiliary models: Locality-aware P2P-based Infrastructure (LP2P) (Section III-A), Distributed Two-hop Routing Algorithm (DRA) (Section III-B) and Efficient and Accurate Reputation Management (EARM) (Section III-C) before introduce the trading market model (TMM) (Section III-D).

A. Locality-aware P2P-based Infrastructure (LP2P)

As shown in Figure 2, MDR builds locality aware P2P (LP2P) overlay 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. In order to help BSs to communicate with their physically closest nodes, achieving a higher efficiency, In LP2P, we let logical proximity abstraction derived from the overlay network match the physical proximity information in reality.

In order to achieve it, we use the landmark method described in the work [25] 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

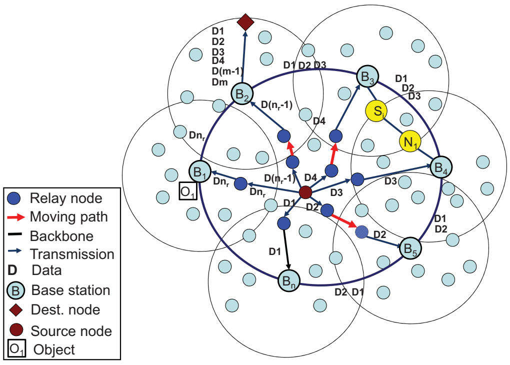


Fig. 2: MDR in a hybrid wireless network.

selected landmark nodes. Given $\tilde{m}$ landmark BSs 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 BSs have similar landmark vectors. A Hilbert space-filling curve [26] is a technique for dimension reduction of vectors while still preserving the relative distances among points in a multi-dimensional space. We then used the technique to map landmark vectors to real numbers, called Hilbert numbers. The closeness of the BSs' Hilbert numbers represents the physical closeness of the BSs on the network. Then a BS's Hilbert number is directly used as its ID for Distributed Hash Table Construction as well as P2P routing in the structured P2P network. Consequently, the LP2P is constructed. Based on the `Insert(ID,object)` and `Lookup(ID)` functions provided by the DHT, we can efficiently operate the information stored in the distributed base stations.

B. Distributed Two-hop Routing Algorithm (DRA)

DRA is comprised of three steps as shown in Figure 2. First, a source node divides a data stream into segments D_1 to D_{n_r}. Second, the source node sends the segments encoded by erasure code to some selected capable neighbors in a distributed manner based on the TMM model. The relay nodes forward the segments to BSs, which will forward the segments to the BS where the destination resides using mobile IP protocol [27]. Third, the segments are transmitted to and reassembled together in the destination MN.

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. In DRA, a source node divides the source message into n_r segments based on erasure coding and distributes the coded segments using different neighbors. DRA can tolerate $(1-\frac{1}{r})$ forwarding failures due to 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.

In a pure distributed routing scheme, when m segments of a message are sent out without using the erasure coding technique, the original message can be recovered only when all m segments arrive at the destination. Assuming that the nodes are independently and identically distributed (i.i.d) in the system and the probability of a segment being dropped is p, the probability of successful transmission of a message is $Pr(X = m) = (1-p)^m$ in the pure distributed routing scheme. Using the erasure coding to recode the m segments to n_r segments, the probability becomes

$$Pr(X \geq m) = \sum_{i=m}^{n_r} C_{n_r}^{m} p^{n_r - i}(1-p)^i > (1-p)^m. \quad (1)$$

Therefore, DRA leads to higher reliability than the pure distributed routing scheme.

Proposition 3.1: The expected transmission delay of a message in the erasure coding-based DRA is

$$E(T_r) = \bar{t} \cdot \sum_{i=0}^{m} \frac{1}{n_r - i}, \quad (2)$$

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

Proof: According to the Kleinrock independence approximation [28], the arrival interval of each segment is independent and exponentially distributed in DRA. Therefore, the probability that the i^{th} segment's transmission delay (T_i) is longer than t is

$$Pr(T_i > t) = e^{-t/\bar{t}} \ (1 \leq i \leq n_r).$$

Thus, the cumulative distribution function for the transmission delay of the shortest-delay segment (T_{min}) with delay less than t is

$$Pr(T_{min} = min(T_1, T_2, ...T_n) \leq t)$$
$$= 1 - Pr(min(T_1, T_2, ..., T_{n_r}) > t) = 1 - e^{-n_r \cdot t/\bar{t}}.$$

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

$$E(T_{min}) = \int_0^{\infty} t \cdot f(T_{min}) \cdot d(t) = \frac{\bar{t}}{n_r}.$$

If we use $\tilde{T}_i$ to denote the delay of the i^{th} arriving segment, then

$$E(\tilde{T}_i) = \frac{\bar{t}}{n_r - i}. \quad (3)$$

The expected transmission delay of the first m arriving segments is

$$E(T_r) = E(\tilde{T}_1 + \tilde{T}_2 + ... + \tilde{T}_m) = \bar{t} \sum_{i=0}^{m} \frac{1}{n_r - i}.$$

■

Replication [29] is another method used to increase the transmission reliability. Next, we will analyze the delay of erasure coding-based DRA compared to replication-based DRA. To keep the same transmission overhead as erasure coding-based DRA, replication-based DRA replicates $(1/r - 1) \cdot m = n - m$ segments and distributively transmits them to the destination. Thus, it needs to transmit m *different* segments to the destination for a successful message transmission. We use *hit* to represent the arrival of a new segment that has never been received by the destination.

Proposition 3.2: With the same amount of transmission overhead, erasure coding-based DRA incurs shorter transmission delay than replication-based DRA.

Proof: Let n_i denote the number of received segments during the time after the $(i-1)^{th}$ hit and upon the i^{th} hit. Then,

$$E[n_i] = \frac{m}{m - i + 1}.$$

Hence, the expected number of segments n_p that need to arrive at the destination for a successful message transmission is

$$E[n_p] = \sum_{i=1}^{m} \frac{m}{m-i+1} \approx m \cdot \ln m.$$

Based on Equ. (3), the expected transmission delay T_p is

$$E(T_p) = E(\tilde{T}_1 + \tilde{T}_2 + ... + \tilde{T}_{m\cdot\ln m}) = \bar{t} \sum_{i=0}^{m\cdot\ln m} \frac{1}{n_r - i}. \quad (4)$$

Comparing Equations (2) and (4), we get $E(T_p) > E(T_r)$. ■

DRA employs distributed routing with erasure coding to enhance the throughput of a hybrid network. To select neighbors to transmit a segment, a source node first broadcasts a request message with the segment length. Its neighbors with sufficient capacity and higher transmission rate for the forwarding reply to the source node. The source node relies on EARM and TMM for reliable and trustworthy relay node selections.

After receiving a segment from a relay node, a P2P BS transmits the segment to the destination. It is important for the BS to locate the destination, especially when it moves between coverage regions of different BSs. Mobile IP protocol [27] can be used to keep track of the locations of MNs during node region switching.

Proposition 3.3: With the assumption that nodes are i.i.d, MDR achieves $O(1)$ system average throughput in a hybrid wireless network.

Proof: In the two-hop routing, the throughput between a S-D in MDR equals the product of the probability that S meets other relay nodes and the probability that relay nodes meet BSs. The former is $O(1/n)$ and the latter is 1. By summing the throughput of communication pairs in the network, the average throughput of the network is $O(1)$. ■

DRA's short path length (2-hop) help it to generate a higher throughput and reliability by adaptively selecting relay nodes based on EARM and TMM. Meanwhile, as for each segment, there is only one forwarding node between source node and a base station, the transmission can be easily monitored by the base station to ensure high transmission reliability. Unlike current ad-hoc routing schemes, DRA neither requires route acquisition nor route maintenance by periodical information exchanges in the MANET component of a hybrid network. Therefore, DRA significantly reduces resource consumption. By distributed routing, DRA enable the source dynamically choose reliable neighbors for packet trading. More importantly, erasure coding based segmentation enables DRA to tolerate a number of forwarding failures and delay in the distributed packet trading process.

C. Efficient and Accurate Reputation Management (EARM)

A challenge in reliable data routing is how to avoid selfish nodes in routing. EARM helps to achieve this objective while offering incentives for node cooperation in routing. As explained in Section I, traditional reputation systems for MANETs are not sufficiently effective and efficient for guiding reliable routing. 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 and incurs a high overhead, EARM relies on LP2P to efficiently collect global reputation information and 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 access. Based on the accurate global reputation value of a node, TMM can evaluate the QoS provided by the node and determine the price of service provided by the nodes. We will introduce the details of TMM in Section III-D

a) Reputation value calculation: As in this paper, we focus on how to encourage the mobile nodes to be cooperative to improve the throughput of hybrid wireless networks, we assume the BSs serve as authorities to supervise the transactions between source nodes and relay nodes, as the BSs are maintained by authorized telecommunication companies or government which are generally trustworthy. In EARM, every node is initially considered to be untrustworthy. The reputation value of a node is increased with a good encounter. A BS increases the reputation value of a relay node when receiving a forwarding segment from the node. That is, $R = R+\beta\cdot l$, where R is a node's reputation value, β denotes a constant, and l denotes the length of the segment. In order to reflect the recent behaviors of nodes, like current reputation systems, BSs 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 awarding relay nodes, a BS assigns more bandwidth to higher-reputed MNs by $BW = \eta R$ ($\eta > 1$), where BW denotes the assigned bandwidth. This algorithm provides incentives for node cooperation in data forwarding while improving a system's throughput.

b) Reputation value collection and querying: A BS calculates local reputation value of N_i in its own range and periodically reports the value to LP2P by using `Insert(`ID_{N_i}, R_{N_i}`)`. Based on the P2P object assignment policy, each node's local reputation values are collected in its owner BS which calculates the average of the local reputation values of each relay node as its global reputation value. As a result, a MN's global reputation value is stored in its owner BS. When node N_i queries for N_j's reputation value, it asks its closest BS. If the BS does not have the reputation value, it sends `Lookup(`ID_{N_j}`)`. Using the P2P routing algorithm, the request will be forwarded to N_j's owner BS having its 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 information 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.

c) Avoiding misbehavior and countering security threat: Threat 1: A relay node forges messages. Since R of a node is determined by the size and number of forwarded segments, a selfish node may forges segment from source nodes by itself to earn a higher R. To prevent such behavior, each BS keeps a log for recent forwarding activities of its MNs and periodically reports the log along with reputation values. A source node also keeps a log of its message transmission history. Once it enters the range of a BS, it sends its log to the BS. The BS parses the log information according to MN IDs and executes `Insert(ID,log)`. Consequently, the logs of source nodes and BSs about a specific relay's activities will be gathered and compared in the relay's owner BS. If the owner observes that a relay node forge segments from the source node for fraudulent benefits, the relay node's reputation will be decreased.

Threat 2: Collusion attack. In the traditional reputation systems, in order to increase the reputation of each other, two nodes may collude by falsely reporting the other's forwarding activities. In EARM, since R is calculated based on actual forwarding activities recorded by BSs, such collusion misbehavior is avoided.

Threat 3: Packet dropping. Similar to the first attack, after a node's BS gathers the logs reported from the source node and BSs, the node's BS can determine whether a forwarding node drops a packet from the source node by comparing the forwarding node's activity information in the logs.

D. Trading Market Model (TMM)

TMM manages data transmission operations between source nodes and relay nodes for reliable and efficient data transmission. Basically, 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 based on the supply and demand equilibrium. Particularly, a node considers two factors: its quality of service (QoS) and the business competition between nodes. For the former, higher-QoS nodes tend to claim higher prices and vice versa. A node with high reputation value is regarded as the node can provide high QoS. For the latter, in order to attract more business to earn more credits and higher reputations, nodes compete to be relay nodes. The autonomous price determination provides nodes a flexible way to control their load and reputations. For example, if a node has a very low reputation, it can lower its service price in order to encourage others to choose it as relay node to have its own reputation value increased. If a node fails to be selected as a relay node for a certain period of time, it could gradually decrease its prices to meet the balance of the request and supply. On the other hand, if a node receives a large amount of forwarding requests and already has a high reputation, it could raise its price to avoid being overloaded. In this way, a node temporary with low reputation will not suffer from traffic starvation, as some nodes may like low price service, if they cannot afford the price of high reputed node.

The 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 still has sufficient capacity to offer a high QoS and receive more requests to increase its reputation. In this case, the node should decrease its price to attract more requests. Leveraging the polynomial price function in the economics area [30] that keeps the supply and demand equilibrium, we propose a price determination function:

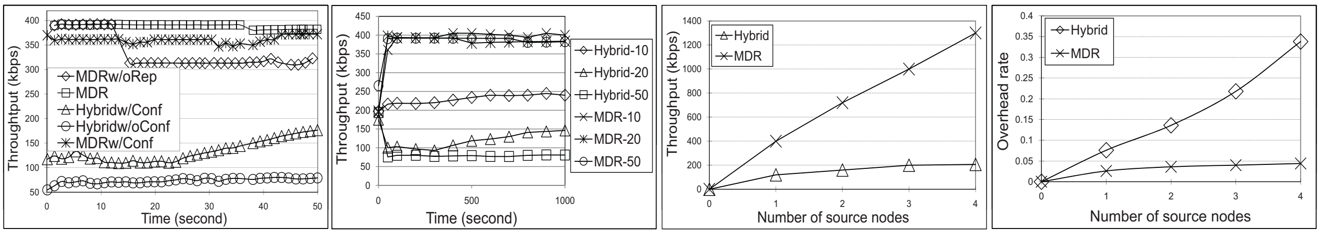
$$P = \bar{p} + \sum_{i=1}^{\beta} \alpha \cdot (\frac{l_q}{L_q})^i, \tag{5}$$

where P is a node's forwarding service price, 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 β are the scaling parameters for the price.

As described in Section III-B, a source node broadcasts a forwarding request to its neighbors. After receiving responses from its neighbors, the source queries the reputation values of the neighbors from the EARM if it does not have the values. Then, the source selects a relay node for each segment. Higher priority is given to the higher-reputed nodes because such nodes help to achieve higher routing reliability. The source then chooses the neighbors whose service charges it can afford. For two neighbors with the same reputation, the source selects the one with the lower price. Therefore, $P_a \geq \sum_{i=1}^{n_r} P_i \cdot l_i$, where P_a is the amount of credits owned by the source, and P_i and l_i are the service price of selected neighbors and data length for the i^{th}segement, respectively. The source node pays the selected relays by including credits into the heads of the segments which is similar to [20]–[22]. 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. TMM also balances node load by enabling nodes to automatically adjust their service price based on the supply and demand equilibrium.

IV. Performance Evaluation

This section demonstrates the distinguishing properties of MDR through simulations built using ns-2 [31]. We used the Distributed Coordination Function (DCF) of IEEE 802.11 as the MAC layer protocol and two-way propagation model in the physical layer. We employed the constant bit rate traffic model in ns-2 for all connections. The default settings are presented below unless otherwise indicated. The total number of MNs and BSs were set to 50 and 5, respectively. The transmission range of BSs and MNs were set to 500m and 250m, respectively. The BSs were uniformly distributed in a 1000×1000 square area. We used the Random Way Point model [32] to simulate the mobility of the nodes. In this model, each MN randomly selects and moves toward a destination point with a speed randomly selected from [1-20]m/s. One S-D pair is randomly chosen every 10 seconds. The Bandwidth was set to 54Mbit/s. The data generating and forwarding rate was set to 1Mbit/s and the time period that a source node transmits a data stream was set to 50 seconds. We randomly assigned a reputation value $\in [0, 1]$ to each node and the percent of the



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

Fig. 3: Performance of MDR, *Hybrid* and *Confidant* in a hybrid network.

selfish node was set to 20%. Selfish nodes always drop their received messages. The warm up time was set to 100s.

We compared MDR with a routing scheme proposed in [9], denoted by *Hybrid*, which directly combines the ad-hoc routing with infrastructure routing. We also compared MDR with the *Confidant* [14]. In *Confidant*, each node evaluates the reputation of its neighbors based on their packet forwarding and receiving rates and exchanges reputation information with its neighbors. 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.

A. 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/o Conf*). Figure 3(a) demonstrates the throughput of different methods over a time period. We can see from the figure that the throughput of MDR remains almost constant over time. The experimental result is consistent with Proposition 3.3 that MDR achieves $O(1)$ system throughput. The throughput of MDR 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, some source nodes move closer to the destinations and the interference on transmissions lessens.

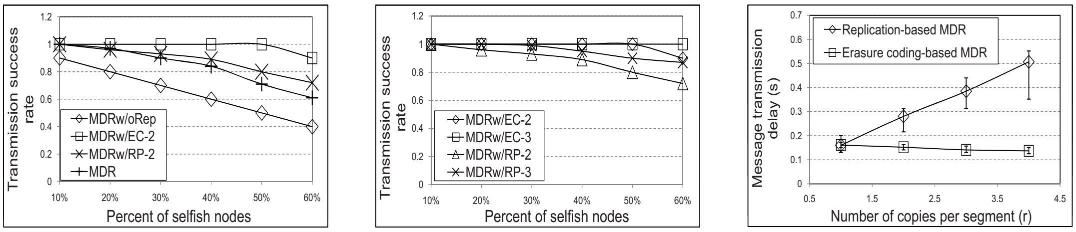
We can also observe that MDR generates a higher throughput than *MDRw/oRep*. In *MDRw/oRep*, source nodes cannot avoid selfish nodes. In contrast, MDR enables source nodes to choose highly-reputed nodes to forward segments. Therefore, the throughput of MDR is much higher. This figure also shows that 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. 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* without a reputation system. This is because some messages were not successfully forwarded due to broken links in multi-hop transmission. This result implies that the higher performance of DRA over multi-hop routing is because of its fewer routing hops and shorter path lengths in transmission.

B. 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 were set to 10, 30 and 50. Figure 3(b) illustrates that with the growth of nodes, 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. This leads to many transmission failures.

Figure 3(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 (i.e., P2P 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 3(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 grow. 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* suffers from an increasing burden to discover and maintain routes, which generate many control messages. These results confirm that MDR produces much less overhead than *Hybrid*.



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

Fig. 4: Effectiveness of the erasure coding-based DRA in MDR.

C. Evaluation of the Erasure Coding-based DRA

In this experiment, we compare the effectiveness of erasure coding with replication in routing reliability enhancement. 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. We define the *success rate* as the percent of the received non-duplicated segments used for message recovery among all original segments. Figure 4(a) compares the success rate of different methods versus the percent of selfish nodes in the system. The figure shows that the success rate of the methods follow *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. As the figure shows, 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 less than *MDRw/EC-2*, especially when selfish nodes constitute a large portion of the network. Using the replication technique, *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 grow. This is because more selfish nodes lead to more dropped messages.

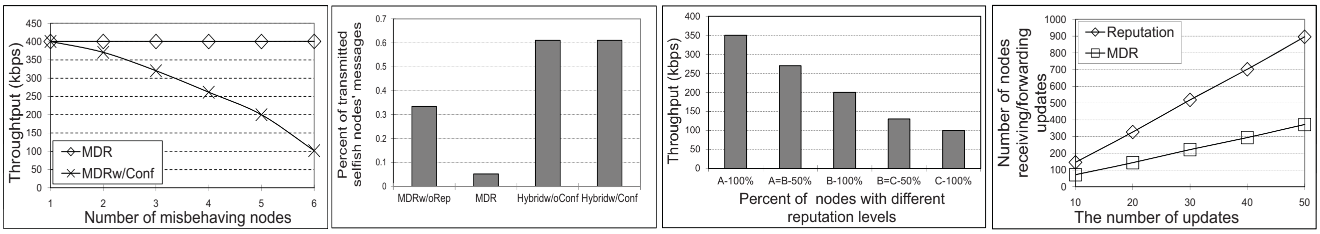
To evaluate the effect of the number of segment copies on the effectiveness of erasure coding and replication, we varied the value of the replication factor r and tested the success rate accordingly. Figure 4(b) shows that *MDRw/EC-2* and *MDRw/EC-3* exhibit approximately the same performance except 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 to enhance the reliability of routing. The figure also shows that *MDRw/RP* leads to less 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 to achieve a higher success rate.

Figure 4(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 leads to a higher queuing delay of the messages in the nodes. Since *MDRw/RP* requires for 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. Therefore, more copies help the destination receive m segments earlier even though the rest of the segments may reach the destination later due to queuing delays. This is also the reason why *MDRw/EC* has a smaller variance in delay than *MDRw/RP*. These experimental results are in line with Proposition 3.2.

D. 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 choose a number of misbehaving nodes that always report a high reputation value for their low-reputed neighbors in an attempt to increase their reputation. Figure 5(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 neighbor information exchanges. 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. It also compares the source nodes' reported activities to the BSs' reported activities to further avoid false information. Thus, EARM provides a more accurate reputation.

In this experiment, one selfish source node continuously sends out messages while two other high-reputed source nodes periodically send out messages. The selfish node initially only has 100 credits and the high-reputed nodes have sufficient credits to support their data transmission. Figure 5(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



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

Fig. 5: Effectiveness and efficiency of the EARM reputation management system.

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 dropped message. MDR's distributed routing avoids generating congestions.

The next experiment investigates how a node's reputation level impacts the throughput in MDR. We assigned four reputation levels, A, B, C and D, to a certain percentage of nodes in the system. Nodes with A, B, C and D levels have possibilities randomly generated in [1, 0.9], [0.9, 0.8], [0.8, 0.7] and [0.7, 0.6] to forward a received segment, respectively. We use "A-100%" to represent the scenario that 100% nodes have reputation level A. Figure 5(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 get more bandwidth from BSs and low-reputed nodes tend to drop transmission data. Therefore, more high-reputed nodes in the system helps to increase the throughput. These results imply that the throughput of a system will be enhanced by choosing relay nodes with high reputation levels.

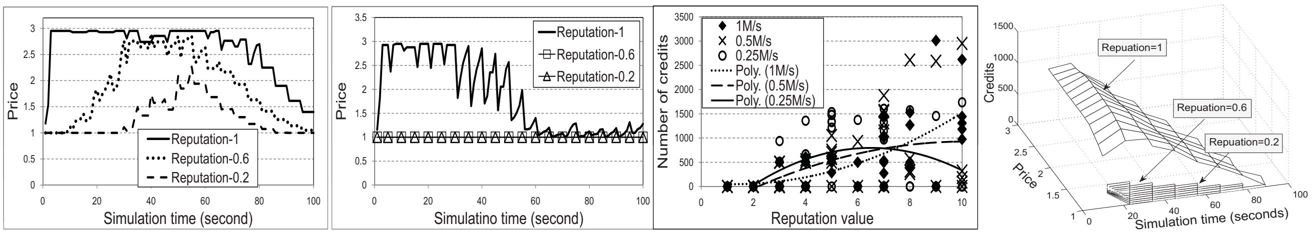
In *Confidant*, neighbors exchange reputation information. After node N_i locally updates the reputation of its neighbor N_j, it sends the update to N_i's neighbors, which update N_j's reputation and notify their neighbors. This process is then repeated. In EARM, BSs that have received messages from N_j send its updated local reputation to N_j's owner BS, which calculates N_j's global reputation. In order to evaluate the overhead of both methods, we varied the number of initiated updates from 10 to 50 with an increment step of 10 and recorded the total number of nodes that have received or forwarded the updates. We set the number of hops for update forwarding in *Confidant* to 3. Figure 5(d) shows that the total number of nodes increases as the initiated updates grow. Also, the number of nodes 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. The update is forwarded to its destination with an average path length of $\log n$, where n is the number of BSs. Message exchange in *Confidant* generates many more messages. The result implies that by taking advantage of the BSs in a hybrid network, EARM leads to a much lower overhead than *Confidant*.

E. Evaluation of the TMM Trading Market Model

In the price determination Formula (5), we set $\beta = 4$, $\alpha = 0.5$ and $\bar{p} = 1$. We assigned each node 500 credits initially and chose 7 source nodes every second for message transmission. We set the forwarding rate of nodes to 0.2M/s. Figure 6(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 (5), 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 less 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 to 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, a node gradually reduces its price to attract more requests if it has not received requests for 60 seconds.

Figure 6(b) shows the change of the service price of the selected three nodes when the forwarding rate is 1M/s. 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. A higher forwarding rate 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 price. Comparatively, a reasonable price and a high QoS of the high-reputed node attracts 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 6(c) plots the credits of each node when the simulation run 100 seconds versus the node's reputation. *Poly. (1M/s)* denotes the linear regression curve for the experimental results with forwarding rate 1M/s based on the Polynomial distribution model. The same applies to the other denotations. The figure shows that the credits of a node increase as the node reputation increases when the forwarding rate is 1M/s and 0.5M/s. A higher-reputed node receives more requests, which leads to higher price. Therefore, a higher-reputed node earns more credits. The figure also shows that higher



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

Fig. 6: Effectiveness of the TTM trading market model.

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 6(d) shows the change of price and credits versus the simulation time when the forwarding rate is 1M/s. The figure shows that there is a positive correlation between price and credits in the nodes with reputation equal to 1. The reason is the same as explained in Figure 6(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.

V. 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. We fully utilize the BSs by forming them into a locality-aware P2P overlay (LP2P), based 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. TMM strengthen the incentives for node cooperation in routing. These MDR components contribute to efficient and reliable routing for a higher throughput.

ACKNOWLEDGEMENTS

This research was supported in part by U.S. NSF grants OCI-1064230, CNS-1049947, CNS-1156875, CNS-0917056 and CNS-1057530, CNS-1025652, CNS-0938189, CSR-2008826, CSR-2008827, Microsoft Research Faculty Fellowship 8300751, and Oak Ridge Award 2008833.

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] Global mobile data traffic growth forecast. http://techcrunchies.com.
[4] H Luo and et al. Ucan: A unified cell and ad-hoc network architecture. In *Proc. of MOBICOM*, 2003.
[5] P. K. McKinley, H. Xu, and et al. Unicast-based multicast communication in wormhole direct networks. *TPDS*, 1992.
[6] H. Wu, C. Qiao, S. De, and O. Tonguz. Integrated cell and ad hoc relaying systems: iCAR. *J-SAC*, 2001.
[7] J. Zhou and Y. R. Yang. PAR CelS: Pervasive ad-hoc relaying for cell systems. In *Proc. of Med-Hoc-Net*, 2002.
[8] 3GPP. pportunity Driven Multiple Access (ODMA). Technical report, Technical Specification Group, 1999.
[9] Y. D. Lin and Y. C. Hsu. Multi-hop cell: A new architecture for wireless communications. In *Proc. of INFOCOM, Vol3*, 2000.
[10] H. Y. Hsieh and R. Sivakumar. Performance comparison of cell and multi-hop wireless network: A quantitative study. In *Proc. of SIGMETRICS*, 2001.
[11] I. Ioannidis, B. Carbunar, and C. Nita-Rotaru. High Throughput Routing in Hybrid Cellular and Ad-Hoc Networks. In *Proc. of WOWMOM*, 2005.
[12] Q. He, D. Wu, and P. khosla. Sori: A secure and objective reputation-based incentive scheme for ad-hoc networks. In *Proc. of WCNC*, 2004.
[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proc. of MobiCom*, 2000.
[14] 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.
[15] N. Li and et al. Design of a Role-based Trust Management Framework. In *Proc. of the IEEE Symposium on Security and Privacy*, 2002.
[16] J. Mundinger and J. Le Boudec. Analysis of a reputation system for mobile ad-hoc networks with liars. *Performance Evaluation*, 2008.
[17] J. Luo, X. Liu, and M. Fan. A trust model based on fuzzy recommendation for mobile ad-hoc networks. *Computer Network*, 2009.
[18] E. P. Charles and P. Bhagwat. Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers. In *Proc. of SIGCOMM*, 1994.
[19] C. Perkins, E. Belding-Royer, and S. Das. Rfc 3561: Ad hoc on demand distance vector (AODV) routing, 2003.
[20] M. Jakobsson, J. Hubaux, and L. Buttyan. A micropayment scheme encouraging collaboration in multi-hop cellular networks. In *Proc. of Financial*, 2003.
[21] L. Buttyan and J. Hubaux. Enforcing service availability in mobile ad-hoc wans. In *Proc. of MobiHoc*, 2000.
[22] L. Buttyan and J. P. Hubaux. Stimulating cooperation in self-organzing mobile ad hoc network. *ACM J. of MONET*, 2002.
[23] J. Chen S. Zhong, Y. R. Yang. Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks. In *Proc. of INFOCOM*, 2003.
[24] 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.
[25] H. Shen and C. Xu. Locality-aware and churn-resilient load balancing algorithms in structured peer-to-peer networks. *TPDS*, 2007.
[26] Z. Xu, M. Mahalingam, and M. Karlsson. Turning heterogeneity into an advantage in overlay routing. In *Proc. of INFOCOM*, 2003.
[27] Ed. C. Perkins. Ip mobility support for ipv4. *Network Working Group, RFC3344*, 2002.
[28] D. Bertsekas and R. Gallager. Data network. In *Prentice Hall*, 1992.
[29] H. Weatherspoon and J. D. Kubiatowicz. Erasure coding vs. replication: A quantitative comparison. In *Proc. of IPTPS*, 2002.
[30] J. M. Perloff. Microeconomics: Theory and applications with calculus.
[31] The network simulator ns-2. http://www.isi.edu/nsnam/ns/.
[32] E. Hyyti and J. Virtamo. Random waypoint model in n-dimensional space. *Operations Research Letters*, 2005.