CHAPTER 1

A Simulation Study of Location- and Power-aware Wireless Networks with Asymmetric Links

Guoqiang Wang, Yongchang Ji, Dan C. Marinescu

School of Computer Science
University of Central Florida
Orlando, FL 32816-2450, USA
E-mail: {gwang, yji, dcm}cs.ucf.edu

Damla Turgut, Ladislau Bölöni

Department of Electrical and Computer Engineering
University of Central Florida
Orlando, FL 32816-2450, USA
E-mail: {turgut, lboloni}cpe.ucf.edu

Asymmetric links are common in wireless networks for a variety of physical, logical, operational, and legal considerations. An asymmetric link supports unidirectional communication between a pair of mobile stations and requires a set of relay stations for the transmission of packets in the other direction. We evaluate m-limited forwarding, a technique to disseminate information in location- and power-aware networks with symmetric and/or asymmetric links. Then we introduce a network and a MAC layer protocol for wireless networks with asymmetric links. The network layer protocol takes advantage of the location information to reduce the number of retransmissions and thus reduces the power consumption via the *m*-limited forwarding technique. The MAC layer protocol requires fewer nodes to maintain silence during a transmission than the protocols proposed in [1,2]. We present a set of metrics characterizing the ability of a medium access control protocol to silence nodes which can cause collisions.

1. Introduction and Motivation

In a wireless environment, at any given time, an asymmetric link supports unidirectional communication between a pair of mobile stations and requires a set of relay stations for the transmission of packets in the other direction. Throughout this paper the term "asymmetric" is related to the transmission range of a node at time t and a communication channel linking two nodes. Two nodes linked by an asymmetric link at time t may find themselves in close proximity, or may be able to increase their transmission range and to reach each other at time $t + \tau$ and thus be connected by a bi-directional link. Thus we feel compelled to make a distinction between unidirectional and asymmetric links in wireless networks. We shall drop this distinction whenever the context allows us to. Asymmetric links are common in wireless networks for a variety of physical, logical, operational, and legal considerations; several scenarios contribute to the asymmetry of communication links in a wireless environment:

(a) Transmission range limited by the node hardware. The hardware properties of the node (for instance, the antenna or the radio circuits) determine the maximum transmission range. This can be different for different nodes, leading to asymmetric links, which can not be avoided except by physically changing the nodes hardware components, for instance by installing a different antenna.

(b) Power limitation. Two nodes have different power constraints, e.g., A has sufficient power reserves and a transmission range enabling it to reach B; however, B has limited power, and either (i) cannot reach A, or (ii) may choose not to reach A to save power. The two scenarios lead to different protocol design. In the second scenario, B is capable to reach A and we could exploit this capability for short transmissions when necessary, e.g., during a network setup phase and thus avoid setting up a bidirectional overlay[a].

(c) Interference. A can reach B and B can reach A, but if B would transmit at a power level sufficient to reach A, it would interfere with C who might be a licensed user of the spectrum. This scenario is critical for transmitters which attempt to opportunistically exploit unused parts of the licensed spectrum (such as unused television channels). Even if operating in the un-licensed bands, dynamic spectrum management arrangements might have given the priority to node C, thus B needs to refrain from sending at a power level above a given threshold.

(d) Stealth considerations. A and B attempt to communicate and wish to hide the existence or the exact location of B from O. One way to achieve

[a] Some approaches use network layer tunneling to enable the transmission of ACK packets at the MAC layer. However, a working network layer requires a working MAC layer.

this is to restrict the transmission power of node B to the minimum and/or transmit on frequencies which make location detection more difficult (low probability of detection (LPD) systems). This is especially important in military/battlefield applications [3,4].

(e) Unidirectional links required by dynamic spectrum management. In the emerging field of software defined radios, the nodes can transmit virtually in any band across the spectrum, but they need to share the spectrum with devices belonging to licensed operators as well as devices with limited flexibility. Once any of the reasons discussed previously force a link to be unidirectional additional constraints, e.g., the need for a reverse path between some pairs of nodes may cause other links to change their status and operate in a unidirectional mode even when there is no explicit reason for unidirectionality.

We discuss briefly two potential applications of the network and MAC layer protocols for location- and power-aware networks with asymmetric links discussed in this paper: software radios and ad hoc grids.

Software radios can sense their RF environment and modify their frequency, power, and/or modulation, allowing for real-time spectrum management. A software radio has *distinctive* advantages over a traditional one: (a) it covers a wide operational frequency spanning multiple bands of the spectrum, (b) can support multiple networking protocols, (c) a single hardware unit can be programmed to work with multiple waveforms and (d) a software radio can be updated to work with new protocols, designed after the radio hardware.

An *ad hoc grid* consists of a hierarchy of mobile systems with different hardware, software, and communication capabilities [6]. The processor speed, amount of main memory, secondary storage, speed of communication devices, and sophistication of the software support increase as we move from one class to another in this hierarchy. Informally, we call the four classes of systems: disposable or `C4`, wearable or `C3`, portable or `C2`, and back-end or `C1`. There are many potential applications of ad hoc grids for sporting events, discovery expeditions, natural resource exploration, disaster management, and battlefield management [6].

The contributions of this paper are: an evaluation of m-limited forwarding, a technique to disseminate information in location- and power-aware networks with symmetric and/or asymmetric links. We also introduce a routing and a MAC layer protocol for wireless networks with asymmetric links. The network layer protocol exploits the location information to reduce the number of retransmissions and thus reduces the power consumption.

The MAC layer protocol requires fewer nodes to maintain silence during a transmission than the protocols proposed in [1,2]. We introduce a set of metrics characterizing the ability of a medium access control protocol to silence nodes which can cause collisions.

2. Related Work

Ad hoc routing protocols are: (i) *table-driven*, or *proactive*, such as DSDV[8], CGSR[9], DREAM[10], and OLSR[11]; (ii) *on-demand*, *reactive*, or *source-initiated*, such as DSR[12], AODV[13], LAR[14], and TORA[15]. In case of proactive routing protocols, nodes periodically propagate routing update advertisements with their neighbors in order to maintain up-to-date routing information. Routes are immediately available upon a node's request. In reactive routing protocols, a route is found on demand when the source needs to send a packet to a destination. Routes are valid only for a limited period, after which routes are considered to be obsolete. No periodical route information propagation is required. Reactive protocols require less bandwidth and power than proactive ones, but discovering routes on demand leads to higher latency. *Hybrid protocols*, such as Zone Routing Protocol (ZRP) [16] combine the features of proactive and reactive protocols. In a hybrid protocol, routes for a subset of nodes are maintained in a routing table proactively while routes for the remaining nodes are discovered when needed. *Location-aware protocols* use location information provided by an attached GPS to improve the performance. LAR[14] and DREAM[10] are examples of such protocols.

Reducing power consumption is critical for wireless communication protocols [17,?]. *Power-aware* routing protocols take into account power consumption when determining a route [19,?].

MAC-layer protocols specify the rules for contending users to access a shared wireless medium in a fair, stable and efficient way. A MAC-layer protocol for wireless ad hoc networks should take into account additional considerations: (i) Mobility - the connection between nodes can become unstable because of the independent movement of the nodes; (ii) Quality of channel - a wireless channel has a higher *Bit Error Rate* (BER) than a wired network; (iii) Collisions - wireless transceivers work in a half-duplex mode; nodes do not "listen" when "talk" and do not "talk" when "listen". The sender is unable to detect the collision and the receiver is unable to notify the sender of the collision during the transmission of a packet. *Collision avoidance* is almost mandatory.

In Carrier Sensing Multiple Access (CSMA) [26] every node senses the carrier before transmitting its data, it defers transmission if it detects the medium is busy. CSMA reduces the possibility of collisions at the vicinity of the sender. Multiple Access Collision Avoidance (MACA) [27] and its variant MACAW [28] are alternative medium access schemes for wireless ad hoc networks that aim to solve the hidden node problem by reducing the possibility of collisions in the vicinity of the receiver. The Floor Acquisition Multiple Access (FAMA) [29] protocol consists of both carrier sensing and a collision avoidance handshake between sender and receiver of a packet. Once the control of the channel is assigned to one node, all other nodes in the network should become silent. Carrier Sensing Multiple Access based on Collision Avoidance (CSMA/CA), the combination of CSMA and MACA, is considered a variant of FAMA protocols. The IEEE 802.11 Standard [30] is a the best-known instance of CSMA/CA.

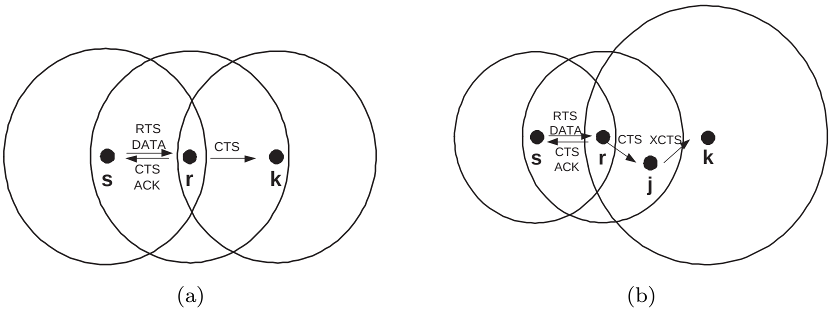


Fig. 1. (a) Hidden node problem in a “classical” wireless network with mobile nodes. All links are assumed to be bidirectional. A hidden node is a node out of the range of the source and in the range of the receiver node. k is a hidden node for a transmission from node s to node r. (b) Hidden node problem in a heterogeneous wireless network with mobile nodes. A hidden node is a node out of the range of the sender and whose range covers the receiver. k is a hidden node as for a transmission from node s to node r.

In a wireless network with symmetric links only, a *hidden node* is generally defined as *a node out of the range of the sender and in the range of the receiver* [31]. According to this definition such a node is hidden from the sender but exposed from the receiver (See Figure 1(a)). The hidden node problem can be solved by a `RTS-CTS` handshake mechanism proposed by MACA [27] (`RTS` stands for *Request to Send* and `CTS` for *Clear to Send*).

However, in a heterogeneous wireless ad hoc network, a *hidden node* should be defined as *a node out of the range of the sender and whose range covers the receiver* (See Figure 1(b)). According to this definition, a hidden node is hidden from the sender and possibly hidden from the receiver as well. The RTS-CTS handshake mechanism is not a solution for such networks since a CTS packet may not be able to reach hidden nodes.

Several solutions to the hidden node problem in a heterogeneous wireless ad hoc network exist. [1] proposes that a node rebroadcasts a CTS packet if it is received from a low-power node. To decrease the probability of collisions, each node waits a random number $(1 \ldots 6)$ of SIFS (Short Inter-Frame Spacing) periods before transmitting a CTS packet. [2] made several improvements relative to [1]: (i) not only CTS but also RTS packets are rebroadcasted; (ii) nodes with a CTS packet to rebroadcast, first sense the medium and transmit only if the medium is not busy; and (iii) only high-power nodes rebroadcast RTS or CTS packets. The solutions proposed by [1] and [2] can lead to inefficient use of the channel if nodes are *misclassified* as hidden nodes. In such situations, nodes that could have been active are silenced due to misclassification, severely degrading the channel utilization. [1] and [2] routinely assume routing over symmetric links so that the sender is able to receive both CTS and ACK packets. In the presence of asymmetric links, however, the sender might not receive the CTS or ACK packets, thus the sender cannot trigger the transmission of DATA packets, and does not know whether a transmission was successful or not. The MAC protocol to be presented in Section 6 is designed to handle these situations as well.

The Sub Routing Layer (SRL) project [32,33] adds an intermediary layer between the MAC and network layers. This layer partially isolates the routing protocol from the MAC layer, although it still allows the routing protocol to directly contact the MAC layer. For unidirectional links, reverse paths are computed using the Reverse Distributed Bellman-Ford algorithm. Another approach is to tunnel packets by encapsulating them at higher level protocols, thus creating virtual reverse links [34]. Although the details of implementation differ, both approaches create a virtual reverse link by substituting it with a reverse path. Even though a bidirectional abstraction is created, the reverse link has a significantly higher latency, and possibly, lower bandwidth.

3. The Model of the System

Let $\mathcal{N}$ be the set of nodes. We assume that:

a. The number of nodes is relatively small, say $| \mathcal{N} | \leq 10^4$.

b. The mobility of individual nodes is limited and differs from one node to the other.
c. Nodes are able to adjust their transmitting power according to their residual power so that their lifetime is extended.

Every node $i \in \mathcal{N}$ is characterized by a minimal set of attributes:
1. *Id*, Id_i; unique string used for node identification.
2. *Class*, C_i; the nodes of a heterogeneous mobile network are classified in several classes based on the hardware and software resources. Throughout this paper we assume a four level hierarchy.
3. *Location* at time t, $L_i(t)$; the geographical coordinates of the position of node i at time t, and
4. *Residual power* at time t, $P_i^{res}(t)$; the amount of power available at time t.

Other attributes can be derived from the ones in the minimal set.
5. *Transmission range* at time t, $R_i(t)$; a function of the residual power and possibly other factors including the configuration of the terrain, atmospheric conditions, and so on.

The *distance* between two nodes $i, j \in \mathcal{N}$ at time t, $d_{ij}(t)$ is a function of the position of the two nodes

$$d_{ij}(t) = d_{ji}(t) = f(L_i(t), L_j(t)).$$

6. *Average velocity* over an interval $\Delta t = t_2 - t_1 > 0$, $v_i^{\Delta t}$; $v_i^{\Delta t} = f(L_i(t_2), L_i(t_1))/\Delta t$.
7. *Mobility region* over an interval $\Delta t = t_2 - t_1 > 0$, $M_i^{\Delta t}$; a circle of radius $v_i^{\Delta t} \times \Delta t$, centered at $L_i(t_1)$.

The Boolean *reachability function* $\mathcal{R}_{ij}(t)$ is defined as

$$\begin{array}{lcl} \mathcal{R}_{ij}(t) = \text{true} & \Longleftrightarrow & R_i(t) \geq d_{ij}(t); \\ \mathcal{R}_{ij}(t) = \text{false} & \Longleftrightarrow & R_i(t) < d_{ij}(t). \end{array}$$

Definition 1: Two nodes $i, j \in \mathcal{N}$ are in *neighbor* relationship at time t if there is a direct communication link between them. We recognize several types of neighbors:
1. *Out-bound neighbor:* j is the out-bound neighbor of i, if i can reach j but j cannot reach i. In this case the link L_{ij} between the two nodes is unidirectional

$$\mathcal{R}_{ij}(t) = \text{true} \qquad \text{and} \qquad \mathcal{R}_{ji}(t) = \text{false}.$$

Call $Out_i(t) \subset \mathcal{N}$ the set of Out-bound neighbors of i at time t.

2. *In-bound neighbor:* j is the In-bound neighbor of i, if j can reach i but i cannot reach j. In this case the link L_{ji} between the two nodes is unidirectional

$$\mathcal{R}_{ij}(t) = \text{false} \qquad \text{and} \qquad \mathcal{R}_{ji}(t) = \text{true}.$$

Call $In_i(t) \subset \mathcal{N}$ the set of In-bound neighbors of i at time t.

3. *In/Out-bound neighbor:* j is the In/Out-bound neighbor of i, if i and j can reach each other. In this case the link L_{ij} between the two nodes is bidirectional

$$\mathcal{R}_{ij}(t) = \text{true} \qquad \text{and} \qquad \mathcal{R}_{ji}(t) = \text{true}.$$

Call $InOut_i(t) \subset \mathcal{N}$ the set of In/Out-bound neighbors of i at time t.

Definition 2: If node i is an Out-bound neighbor of node j, we call i the *high-range node* (H-node) and j the *low-range node* (L-node) of the asymmetric link L_{ij}.

Definition 3: A set of m nodes $i_1, i_2, \dots i_m \in \mathcal{N}$ are in an *m-party proxy set* if each node can reach the other $m-1$ nodes either directly or through a subset of the other $m-2$ members.

Proposition 4: *At least one of the links of an m-party proxy set must be bidirectional.*

Proof: Suppose Proposition 1 is false, that is, there exists an m-party proxy set with no bidirectional link. Let the m nodes in the m-party proxy relationship be $i_1, i_2, \cdots, i_m \in \mathcal{N}$ and arbitrarily pick up an asymmetric link (i_u, i_v) where $1 \leq u, v \leq m, u \neq v$. Thus, node i_u can reach node i_v directly, but the reciprocal is not true, $\mathcal{R}_{i_u i_v}(t) = true$ and $\mathcal{R}_{i_v i_u}(t) = false$, which is equivalent to

$$R_{i_u}(t) \geq d_{i_u i_v}(t) > R_{i_v}(t).$$

By the definition of m-party proxy set, there exists at least a path for node i_v to reach node i_u. Let us choose the shortest path from node i_v to node i_u. There are no duplicate nodes on this path, otherwise a shorter path can be obtained by removing the sub-path consisting of all the nodes connecting the two duplicate nodes. Call the set of nodes on the shortest path $(i_v, i_{N_1}, i_{N_2}, \cdots, i_{N_p} \cdots, i_{N_k}, i_u)$, where $N_p \neq N_q, N_p \neq u, N_p \neq$

$v, 1 \leq p, q \leq k \leq m-2, p \neq q$. Similarly, we have

$$\begin{aligned} R_{i_v}(t) &\geq d_{i_v i_{N_1}}(t) > R_{i_{N_1}}(t) \\ &\geq d_{i_{N_1} i_{N_2}}(t) > R_{i_{N_2}}(t) \\ &\geq \cdots > R_{i_{N_p}} \geq d_{i_{N_p} i_{N_{p+1}}}(t) > R_{i_{N_{p+1}}}(t) \\ &\geq \cdots > R_{i_{N_k}} \geq d_{i_{N_k} i_u}(t) > R_{i_u}(t). \end{aligned}$$

The above inequalities are contradictory, thus, Proposition 1 must be true. □

Figure 2(a) and 2(b) show two possible configurations of a three-party proxy set with unidirectional links only. The configuration in Figure 2(a) is infeasible according to Proposition 1, while the configuration in Figure 2(b) is infeasible because k cannot reach either i or j.

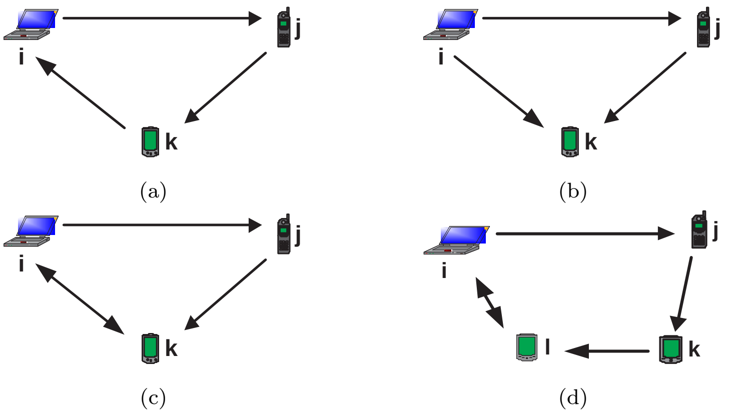


Fig. 2. Three-party and four-party proxy sets. (a) An infeasible scenario for a three-party proxy set involving three unidirectional links. (b) A second infeasible scenario for a three-party proxy set involving three unidirectional links. (c) A feasible scenario for a three-party proxy set with one bidirectional link. (d) A feasible scenario for a four-party proxy set with one bidirectional link.

Proposition 5: *There is at least one configuration of an m-party proxy set with one bidirectional link.*

The configuration in Figure 2(c) and any configuration obtained by a permutation of the nodes in the set has one bidirectional link. In this configuration i can reach j and k directly, j can reach k directly and i via

k, and finally k can reach i directly and j via i. The ranges and distances among the nodes of the configuration in Figure 2(c) are:

$$R_j < d_{ij} \leq R_i, \quad R_k < d_{jk} \leq R_j; \quad d_{ik} \leq R_i, \quad d_{ki} \leq R_k.$$

To show that there is at least one configuration of four-party proxy set with one bidirectional link we consider the configuration in Figure 2(d). Since there is a loop $i \rightarrow j \rightarrow k \rightarrow l \rightarrow i$, every node can reach the other nodes in the set.

The ranges and distances among the nodes of the configuration in Figure 2(d) must satisfy the following constraints:

$$\begin{cases} R_j < d_{ij} \leq R_i, \quad R_k < d_{jk} \leq R_j, \quad R_l < d_{kl} \leq R_k; \quad d_{li} \leq R_i, \quad d_{li} \leq R_l; \\ d_{ik} > R_i, \quad d_{jl} > R_j, \quad d_{ki} > R_k, \quad d_{lj} > R_l. \end{cases}$$

In the general case of an m-party proxy set consider the nodes $i_1, i_2, \ldots i_m \in \mathcal{N}$ connected as follows: nodes i_k and i_{k+1} $(1 \leq k \leq m-2)$ are connected by unidirectional links from node i_k to node i_{k+1}, and nodes i_1 and i_m are connected by a bidirectional link. The ranges and distances among nodes must satisfy the following constraints

$$\begin{cases} R_{k+1} < d_{k,k+1} \leq R_k, \quad 1 \leq k \leq m-2; \quad d_{1m} \leq R_1, \quad d_{m1} \leq R_m; \\ d_{k,(k+j) \mod m} > R_k, \quad 2 \leq j \leq m-1, \; 1 \leq k \leq m. \end{cases}$$

Definition 6: Define the *average number of neighbors* for a bidirectional ad hoc network given a mobility area S, at time t, $\omega(S, \mathcal{N}, t)$, as $\frac{\Sigma_{i \in \mathcal{N}}(\omega_i(t))}{|\mathcal{N}|}$, where $\omega_i(t)$ is the number of neighbors of node i at time t.

Proposition 7: *Assume (i) the set of nodes $\mathcal{N}$ is uniformly distributed throughout the area S and (ii) all the nodes have the same transmission range R. Let S be a rectangle with length X and width Y, $X, Y \geq 2R$. We can approximate the average number of neighbors of a node as:*

$$\omega(S, \mathcal{N}, t) \approx \mid \mathcal{N} \mid (\frac{R^4}{(XY)^2} - \frac{3}{4}(\frac{1}{X^2Y} + \frac{1}{XY^2})R^3 + \frac{\pi R^2}{XY}) - 1.$$

Corollary 8: *If $X = Y$, $\omega(S, \mathcal{N}, t) \approx \mid \mathcal{N} \mid (\frac{R}{X})^4 - 1.5(\frac{R}{X})^3 + \pi(\frac{R}{X})^2] - 1.$*

Corollary 9: *If $X = Y = mR, m \geq 2$, $\omega(S, \mathcal{N}, t) \approx \mid \mathcal{N} \mid (\frac{1}{m^4} - \frac{1.5}{m^3} + \frac{\pi}{m^2}) - 1.$*

4. m-Limited Forwarding

m-limited forwarding is a technique to reduce the cost of disseminating information in a power-constrained environment by limiting the cardinality of the subset of nodes which will retransmit a packet. In case of flooding in an ad hoc network, when node j transmits a packet at time t the nodes in the set $H_j(t)$, the set of all neighbors within the transmission range of node j, retransmit the packet. There are $n_j(t) =| H_j(t) |$ nodes in this set. We wish to limit the size of the subset of nodes which forward the packet to at most $m < n$. The nodes in this subset, called *m-forwarding subset*, $F_j(t) \subset H_j(t)$ should be the ones optimally positioned vis-a-vis the packet destination and with the most favorable balance of power. The parameter m should be chosen to satisfy a subset of sometimes contradictory requirements, e.g., minimize the power consumption, ensure some stability of the routes when the nodes move within a certain area, minimize error rates, minimize retransmission, and so on.

Informally, in the method discussed in this paper the sender of a packet, node j provides a "hint", we call this value a *forwarding cutoff*, $\kappa_j(t)$, and sends it to all its neighbors together with the original information. Each node $i \in H_j(t)$ determines if it belongs to the selected subset, $i \in F_j(t)$, by evaluating a function, the *forwarding priority* function, $\varphi_i(t)$, and then compares the value of this function with the *forward cutoff*. Node i forwards the packet if and only if $\varphi_i(t) \geq \kappa_j(t)$. Obviously, the destination recognizes its own `nodeID` and does not further forward the packet. If the location of the destination is not known, the sender sets $\kappa_j(t) = -1$ and all nodes in H_j retransmit the packet. If $| F_j(t) |< m$ then $\kappa_j(t) = 0$ and in this case individual nodes in H_j make their own decision whether to forward or not.

Note that information regarding the position and the residual power of each node in the set $H_j(t)$ may, or may not, be very accurate, due to node mobility and to node activity which affects the residual power. As a result, $\kappa_j(t)$ may allow fewer than m nodes to forward, if some have moved away from their location known to node j, or may have further depleted their power reserves. The actual number of nodes forwarding the packet may be larger than m if new nodes have moved into the optimal forwarding area, or recharged their batteries.

A forwarding fitness function measures the fitness of a node as the next hop. Different heuristics can be used when designing a forwarding fitness function.

One example of a forwarding fitness function is:

$$\tau_k(i,j) = \frac{1}{d_{ik} + c}, \tag{1}$$

where j is the sender, i is the destination, k is the next hop candidate, d_{ik} is the distance between node i and node k, and c is a positive constant.

Another instance of a forwarding fitness function is proposed in [35],

$$\eta_k(i,j) = \begin{cases} 0 & \text{if } R_k \leq d_{ik} - r_{ij}; \\ \pi \cdot r_{ij}^2 & \text{if } R_k \geq d_{ki} + r_{ij}; \\ \frac{1}{2}[r_{ij}^2(\varphi - sin\varphi) + R_k^2(\theta - sin\theta)] & \text{otherwise}; \end{cases} \tag{2}$$

where $r_{ij} = d_{ij} - R_j$, $\theta = 2 \arccos \frac{R_k^2 + d_{ik}^2 - r_{ij}^2}{2 \cdot R_k \cdot d_{ki}}$, and $\varphi = 2 \arccos \frac{r_{ij}^2 + d_{ik}^2 - R_k^2}{2 \cdot r_{ij} \cdot d_{ik}}$.

If we assume that the number of nodes in a given area is proportional to the size of the area, this fitness function based upon geometric considerations, favors nodes which have more neighbors who could possibly either reach the destination, or reach other nodes best positioned to reach the destination.

4.1. *Simulation Study*

M-limited forwarding can be used for wireless networks with symmetric/bidirectional links as well as wireless networks with asymmetric/unidirectional links. We choose to study the first type of networks because we wanted to clearly distinguish the advantages and the drawbacks of the algorithm in a traditional setting, without the additional effects due to asymmetric links.

We use NS-2 [36,?], an object-oriented event-driven simulator developed at the Lawrence Berkeley National Laboratory as part of the VINT project, with the CMU wireless extensions [38]. To describe the movement of nodes in the system we use the "random waypoint" model [39,?]. In our simulations we use traffic patterns generated by *constant bit rate* (CBR) sources sending UDP packets. We are concerned with the impact of network load, node mobility, and network density upon power consumption, packet loss ratio, and latency. We run several simulation experiments and vary the number of nodes, the speed in the "random waypoint" model, and the number of CBR sources. Table 1 illustrates the default settings and the range of the parameters for our simulation experiments. To construct 95% confidence intervals, we repeat each experiment 10 times for a pair of scenario and traffic pattern, the two elements affecting the results of a performance study.

Field	**Value**	**Range**
simulation area	$500 \times 500(m^2)$	
number of nodes	80	30 - 100
transmission range	100 (m)	
average number of neighbors	8.22	2.46 - 10.53
speed	1 (m/s)	2 - 20 (m/s)
pause time	15 (s)	
simulation time	800 (s)	
number of CBR sources	30	5 - 40
CBR packet size	64 (bytes)	
CBR sending rate	512 (bps)	

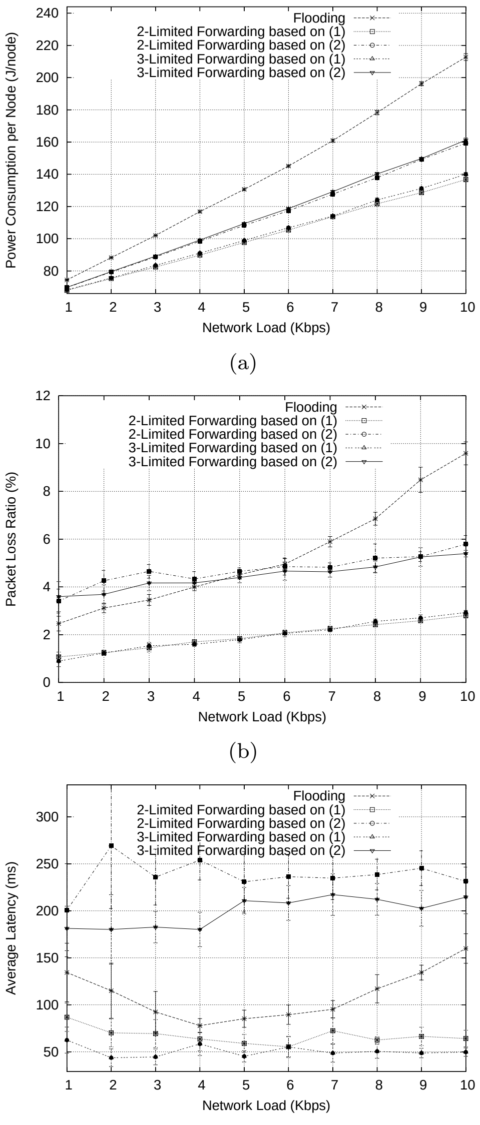
The Effect of the Network Load. We expect the network load to affect differently the power consumption, the packet loss ratio, as well as the average packet delay of the five routing schemes, flooding and 2- and 3-limited forwarding with $\tau_k(i,j)$ and $\eta_k(i,j)$ fitness functions. Figure 3(a) illustrates average power consumption versus network load. As expected, flooding needs more power than routing with m-limited forwarding schemes.

Figure 3(b) illustrates packet loss ratio versus network load. Packet loss could be due to several factors: (i) the forwarding set calculated by the forwarding fitness function excludes nodes on the critical path from source to destination; (ii) packets are dropped due to collisions or excessive retransmission failures at MAC layer; (iii) nodes move fast and the routing tables become outdated frequently. When the traffic load is light, the major cause of packet loss is exclusion of nodes on the path from source to destination, while for heavy traffic the collisions become the major source of traffic loss. Node movement is a minor factor affecting the packet loss as the node speed is relatively low in this experiment.

As a general rule flooding causes more collisions than m-limited forwarding. When network load is relatively heavy, routing schemes using m-limited forwarding outperform flooding as collisions become a major concern.

Figure 3(c) illustrates average latency versus network load. The average latency is calculated based solely on delivered packets. Higher latency is due to heavy traffic and/or paths with a large number of hops. To avoid collisions, the binary exponential backoff algorithm of the MAC layer protocol requires that packets are retransmitted after timeouts lasting increasingly longer after subsequent collisions.

Not surprisingly, the average latency of flooding is lower than that of



(a)

(b)

(c)

Fig. 3. The impact of network load on power consumption, packet loss ratio, and latency. (a) Average power consumption versus network load. (b) Packet loss ratio versus network load. (c) Average latency versus network load.

routing with m-limited forwarding using $\eta_k(i,j)$. Flooding tends to find routes with the shortest latency while routing with m-limited forwarding scheme using $\eta_k(i,j)$ may exclude nodes on the shortest path. However, when the network load is high, flooding may experience higher average latency than routing with m-limited forwarding using $\tau_k(i,j)$.

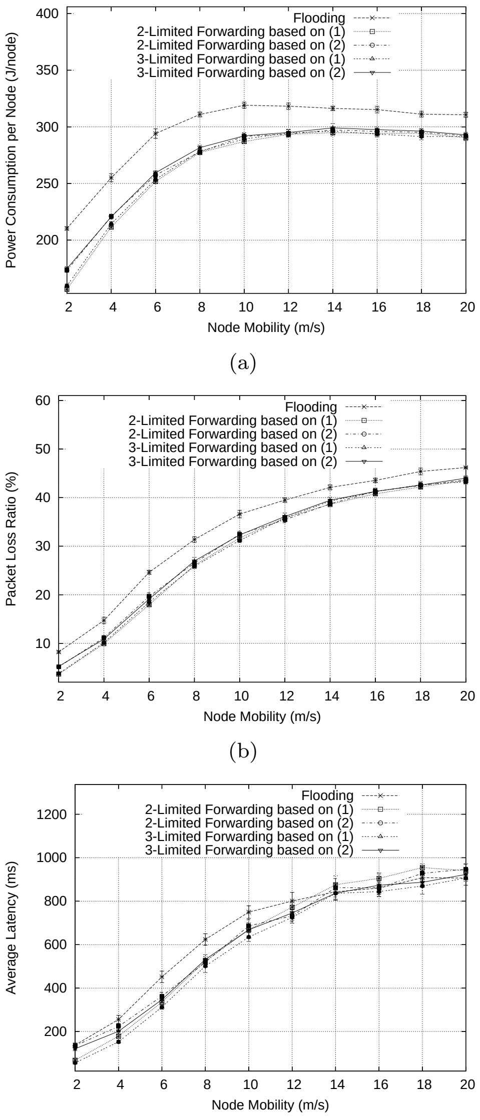
The Effect of Node Mobility. Node mobility is measured by the speed of the node movement. Figure 4(a) illustrates the average power consumption versus node mobility. When node mobility is high the routing table become outdated quickly and the average power consumption of all routing schemes increases, as additional power is dissipated to find new routes. As expected, m-limited forwarding requires less power than flooding. For example, 2-limited forwarding using $\tau_k(i,j)$ is 20.55% at 2 m/s and 10.01% at 20 m/s better than flooding.

Figure 4(b) presents packet loss ratio versus node mobility. In all routing schemes packet loss ratio increases sharply when node mobility increases due to outdated routing tables. All routing schemes are very sensitive to node mobility, for example, for flooding the packet loss ratio increases from 6.07% at 2 m/s to 26.56% at 20 m/s.

Figure 4(c) illustrates average latency versus node mobility. When the node speed increases the routing table become outdated frequently and the path discovery process, which is very demanding in terms of network bandwidth, is initiated frequently. For all routing schemes the average latency increases with the node mobility due to congestion caused by frequent retransmissions and the need to discover new routes.

The Effect of Network Density. We expect node density to affect network performance and study its effects on power consumption, packet loss ratio, and average delay. In Figure 5(a), as the network density increases, the power consumption of routing based upon m-limited forwarding increases nearly linearly, while for flooding the increase is nearly exponential. The 2-limited forwarding using $\tau_k(i,j)$ is more efficient than flooding; the savings in power consumption range from 19.50% for 30 nodes (average number of neighbors is 2.46) to 46.08% for 100 nodes (average number of neighbors is 10.53).

Figure 5(b) illustrates packet loss ratio versus network density. The packet loss ratio of all routing schemes is relatively low when network density is small. When the number of nodes is larger than 70, the packet loss ratio for flooding increases sharply due to excessive congestion and the col-

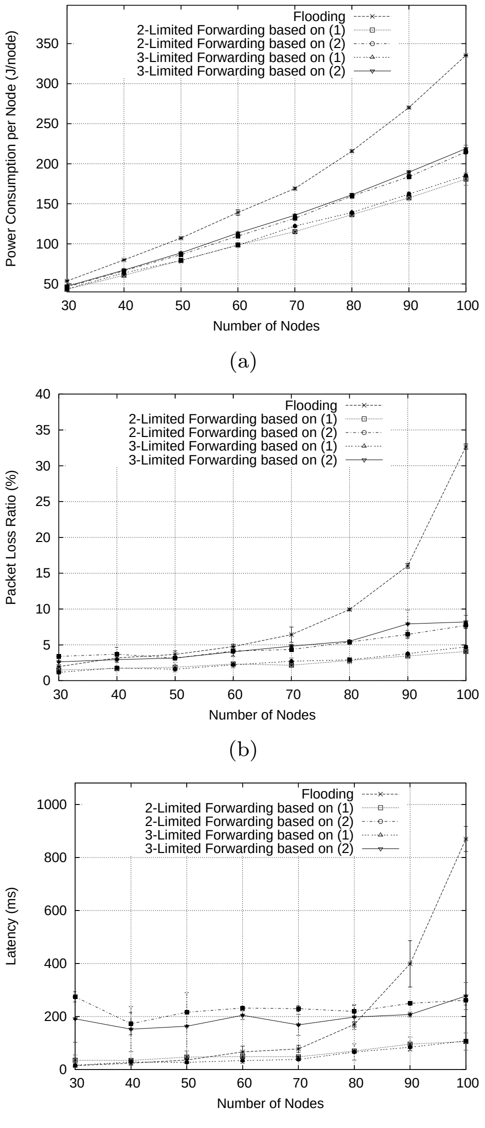


(a)

(b)

(c)

Fig. 4. The impact of node mobility on power consumption, packet loss ratio, and latency. (a) Average power consumption versus node mobility. (b) Packet loss ratio versus node mobility. (c) Average latency versus node mobility.



(a)

(b)

(c)

Fig. 5. The impact of network density on power consumption, packet loss ratio, and latency. (a) Average power consumption versus network density. (b) Packet loss ratio versus network density. (c) Average latency versus network density.

lisions. The packet loss ratio of flooding increases from 1.96% for 30 nodes to 32.67% for 100 nodes.

Figure 5(c) illustrates average latency versus network density. The average latency of all routing schemes is relatively low when the number of nodes is relatively small. When the number of nodes is larger than 70 the average latency for flooding increases sharply due to excessive collisions.

In terms of power dissipation m-limited forwarding outperforms flooding when network load, node mobility, and node density increase. Among the four m-limited forwarding schemes, the 2-limited forwarding with $\tau_k(i,j)$ performs the best. When network load increases, the power dissipation of flooding increases faster than that of m-limited forwarding schemes. The power consumption increases almost linearly with the node density for m-limited forwarding while the increase is faster for flooding.

The packet loss ratio is another aspect of network performance where m-limited forwarding is at par if not better than flooding. For a light network load flooding performs slightly better than m-limited forwarding using $\eta_k(i,j)$ but worse than m-limited forwarding using $\tau_k(i,j)$. All routing schemes are very sensitive to node mobility and the packet loss ratio increases sharply when node mobility increases. Flooding is only slightly worse than m-limited forwarding. In terms of node density m-limited forwarding fares better than flooding. The packet loss ratio for flooding at high node density increases exponentially due to excessive collisions.

Finally, the packet delay increases due to heavy traffic and/or paths with a large number of hops. Flooding is slightly better than routing with m-limited forwarding at light network load using $\eta_k(i,j)$ but worse than m-limited forwarding using $\tau_k(i,j)$ at heavy network load. For all routing schemes the average latency increases with the node mobility due to congestion caused by frequent retransmissions and the need to discover new routes. The average latency for flooding increases sharply due to excessive collisions when the network density increases.

It is possible that the ongoing evaluation of m-limited forwarding for heterogeneous wireless ad hoc networks with asymmetric links will led to slightly different conclusions, e.g., it is likely that $\eta_k(i,j)$- may prove to be better than $\tau_k(i,j)$-based policies.

5. Routing Protocol

The A^4LP protocol [35] consists of an initialization phase when each node discovers its In-, In/Out-, and Out-bound neighbors, a path discovery phase using m-limited forwarding, and a path maintenance phase.

Information Maintained by a Node and Packet Types. A node $i \in \mathcal{N}$ maintains several data structures, a routing table (see Table 2), a path request sequence number and a node sequence number.

(1) *Routing Table at node j (RT_j)*: caches information for all neighbors and for most recently used destination (Table 2). The field *dstNeighborType* takes one of the following values: In-bound, Out-bound, In/Out-bound, or Not-neighbor. *expTime* records the expiration time for an entry after which it is no longer valid.
(2) *Request Sequence Number* (`reqSeq`): a counter, uniquely identifies a path request packet sent by the the node with nodeId. The `reqSeq` is incremented every time a route request is sent.
(3) *Node Sequence Number* (`seq`): a counter revealing the freshness of a node, incremented when the node detects the change of location, residual power, transmission range, routing table, and so on.

Field	**Description**
dstId	Destination node id
dstLoc	Destination location information
dstClass	Destination class
dstPower	Destination residual power
dstRange	Destination transmission range
dstSeq	Destination sequence number
dstNeighborType	Neighbor type of destination
nextHop	Next hop to forward a packet
expTime	Expiration time

5.1. *Neighbor Discovery*

In-bound Neighbor Discovery. In-bound neighbor discovery (which, incidentally, leads also to the discovery of neighbors which will later turn out to be In/Out-bound) is initiated when a node joins the network. Each node broadcasts periodically a `Hello` packet to inform all the neighbors in its range of its current location, residual power, and transmission range. The time between two such transmissions is called a *hello interval.*

Upon receiving a `Hello` packet a node either updates an existing entry in its routing table or creates a new one. Acknowledgements are not required (actually not possible for In-bound neighbors). A node deletes the entries of Out- and In/Out-bound neighbors if it does not receive their `Hello` packets for several hello intervals. A `Hello` packet is a broadcast packet with a life time of one hop. The `Hello` packet provides the location, the class, the residual power, and the range of the sender.

Out-bound Neighbor Discovery. Due to the nature of asymmetric links, Out-bound neighbors are not detected directly as their signals cannot be heard. For example, in the three-party proxy set in Figure 2(c), the `Hello` packet from node j cannot reach node i, thus node i cannot know that node j is an Out-bound neighbor. However, node k, which is an In/Out-bound neighbor of node i and an Out-bound neighbor of node j, is aware that link L_{ij} is asymmetric with i as the H-node and j as the L-node. Thus, node k sends a `Convey` packet to node i with the information of node j, and, at the same time, records node i as the next hop to reach node j.

In the Out-bound neighbor discovery, a node periodically checks the link relationship between its neighbors, sets up the route to its In-bound neighbor if a three-party proxy set is detected, and informs the H-node of an asymmetric link, when it detects one. The time between two Out-bound neighbor discovery is called a *convey interval.* The `Convey` packet contains the Id of the sender and of the destination (the H-node of an asymmetric link), the Id, the location, the class, the residual power, the range, and the sequence number of the L-node of the asymmetric link.

5.2. *Location and Power Update*

Dissemination of the approximate node location as well as its residual power are critical for any location-aware and power-aware routing scheme, yet it is not the focus of this paper. It can be achieved by (i) gossiping algorithms, (ii) a broadcast scheme, in which updates are sent infrequently and locally. (iii) a hierarchical scheme - nodes form clusters around *head of a cluster*, who covers a relative large area and is able to exchange information collected from members of the cluster, or some other scheme.

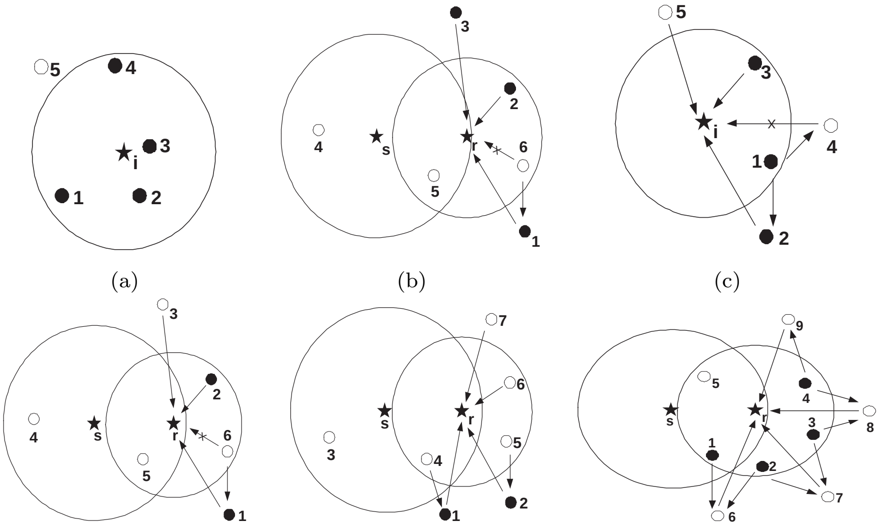
In A^4LP a node sends location and power updates only when (i) it joins the network, (ii) has moved significantly since the last reported location, (iii) its residual power goes below *low water mark.*

6. MAC Protocol

6.1. *Topological considerations*

The handling of the hidden nodes is an essential problem for wireless MAC protocols operating in the presence of asymmetric links. In the following, we introduce a series of topological concepts and attempt to classify hidden nodes. The following definitions are necessary to introduce the MAC layer protocol.

We call the proxy node through which an *L*-Node can reach an *H*-node a *P-node.* A *tunnel* is defined as the *reverse route* from an *L*-Node to an *H*- through a *P*-node. Call T_{sr} a transmission from sender s to receiver r.



(a) (b) (c)

(d) (e) (f)

Fig. 6. An illustration for topology concepts. (a) The vicinity of a node i, $V_i = \{1, 2, 3, 4\}$. (b) The set of hidden nodes for the transmission from s to r: $H_{sr} = \{1, 2, 3\}$. (c) Example of the three-party proxy set coverage of node i: $P3_i = \{1, 2, 3\}$. (d) The $H3_{sr}$ set for a transmission T_{sr}: $H3_{sr} = \{1, 2\}$. (e) The extended hidden nodes set $XH3_{sr}$: $XH3_{sr} = \{1, 2\}$. (f) The extended hidden nodes relay set $XHR3_{sr}$ for a transmission T_{sr}. In the illustrated scenario, $XHR3_{sr} = \{1, 2, 3, 4\}$, $mXHR3_{sr} = \{2, 4\}$ or $\{1, 3, 4\}$, $MXHR3_{sr} = \{2, 4\}$.

Definition 10: Call V_i the *vicinity* of node i. V_i includes all nodes that could be reached from node i (see Figure 6(a)).

$$V_i = \{j|\mathcal{R}(i, j)\}.$$

Definition 11: Call H_{sr} the set of *hidden nodes of a transmission* T_{sr}. H_{sr} includes nodes that are out of the range of the sender and whose range covers the receiver (see Figure 6(b)).

$$H_{sr} = \{k | \neg\mathcal{R}(s,k) \wedge \mathcal{R}(k,r)\}.$$

Note that H_{sr} are the hidden nodes for the transmission of the `DATA` packets, while H_{rs} are the hidden nodes for the transmission of `ACK` packets.

Definition 12: Call $P3_i$ the *three-party proxy set coverage* of node i. $P3_i$ is the set of nodes nodes reachable either by node i directly, or participate in a three-party proxy set with node i and a third node (see Figure 6(c)).

$$P3_i = \{k | \mathcal{R}(i,k) \vee \exists_j \ (\mathcal{R}(i,j) \wedge \mathcal{R}(j,k) \wedge \mathcal{R}(k,i))\}.$$

Definition 13: Call $H3_{sr}$ the *hidden nodes* of a transmission T_{sr} in the three-party proxy set coverage of node r. The set $H3_{sr}$ includes hidden nodes covered by $P3_r$ (see Figure 6(d)).

$$H3_{sr} = H_{sr} \cap P3_r.$$

Definition 14: Call $XH3_{sr}$ the *extended hidden nodes* of a transmission T_{sr} in three-party proxy set coverage of node r. The set $XH3_{sr}$ includes nodes in $H3_{sr}$ covered by V_r (see Figure 6(e)).

$$XH3_{sr} = H3_{sr} - V_r.$$

Definition 15: Call $XHR3_{sr}$ the *extended hidden nodes relay set* of a transmission T_{sr} in three-party proxy set coverage of node r. $XHR3_{sr}$ includes *all* nodes in $P3_r$ that could relay traffic from node r to nodes belonging to $XH3_{sr}$ (see Figure 6(f)).

$$XHR3_{sr} = \{j \ | j \in V_r \wedge \exists_{k \in XH3_{sr}} (\mathcal{R}(j,k))\}$$

Definition 16: Call $mXHR3_{sr}$ the *minimal extended hidden nodes relay set* of a transmission T_{sr} in three-party proxy set coverage of node r. $mXHR3_{sr}$ includes a set of nodes in $XHR3_r$ ($mXHR3_r \subseteq XHR3_r$) such that (i) the node r can relay traffic to any node in $XH3_{sr}$ through some nodes from $mXHR3_{sr}$; (ii) the removal of any nodes in $mXHR3_{sr}$ makes some nodes in $XH3_{sr}$ unreacheable from node r (see Figure 6(f)).

$$\forall_{k \in XH3_{sr}} \exists_{j \in mXHR3_{sr}} (\mathcal{R}(j,k))$$

and

$$\forall_{j\prime \in mXHR3_{sr}} \exists_{k \in XH3_{sr}} \nexists_{j \in mXHR3_{sr} - \{j\prime\}} (\mathcal{R}(j,k)).$$

Note that $mXHR3_{sr}$ may not be unique, and different minimal extended hidden nodes relay sets could contain a different number of nodes.

Definition 17: Call $MXHR3_{sr}$ the *minimum extended hidden nodes relay set* of a transmission T_{sr} in three-party proxy set coverage of node r. $MXHR3_{sr}$ is the subset of $mXHR3_{sr}$ with the smallest number of nodes (see Figure 6(f)).

$$MXHR3_{sr} \in mXHR_{sr}$$

and

$$\forall r \in mXHR3_{sr}(|MXHR3_{sr}| \leq |r|).$$

Finally, we introduce a set of metrics characterizing the ability of a MAC protocol to silence nodes which can cause collisions.

Definition 18: Let $\mathcal{F}$ be an algorithm of a MAC protocol that silences proper nodes during a transmission. Call the set of nodes silenced by $\mathcal{F}$ during a transmission T_{sr}, $\mathcal{S}_{sr}(\mathcal{F})$. Ideally, an algorithm should silence all nodes that have the potential to be hidden nodes, as well as nodes that could potentially be affected by the transmission T_{sr}. Assume there exists an algorithm $\mathcal{I}$ which classifies all the nodes that should be silenced during a transmission T_{sr}, thus,

$$\mathcal{S}_{sr}(\mathcal{I}) = H_{sr} \cup H_{rs} \cup V_s \cup V_r.$$

Definition 19: Call $Misc_{sr}(\mathcal{F})$ the *misclassification ratio* of an algorithm $\mathcal{F}$ for a transmission T_{sr}. $Misc_{sr}(\mathcal{F})$ measures the ratio of nodes that are incorrectly silenced by $\mathcal{F}$.

$$Misc_{sr}(\mathcal{F}) = \frac{|\mathcal{S}_{sr}(\mathcal{F}) - \mathcal{S}_{sr}(\mathcal{I})|}{|\mathcal{S}_{sr}(\mathcal{I})|}.$$

Definition 20: Call $Miss_{sr}(\mathcal{F})$ the *miss ratio* of an algorithm $\mathcal{F}$ for a transmission T_{sr}. $Miss_{sr}(\mathcal{F})$ measures the ratio of nodes which are not silenced by the algorithm $\mathcal{F}$, although they should be.

$$Miss_{sr}(\mathcal{F}) = \frac{|\mathcal{S}_{sr}(\mathcal{I}) - \mathcal{S}_{sr}(\mathcal{F})|}{|\mathcal{S}_{sr}(\mathcal{I})|}.$$

Definition 21: Let $\overline{Misc(\mathcal{F})}$ and $\overline{Miss(\mathcal{F})}$ be the *average misclassification* ratio and *average miss ratio* of an algorithm $\mathcal{F}$, respectively. The averages are computed over a network $\mathcal{N}$.

$$\overline{Misc(\mathcal{F})} = \frac{\sum_{\forall_{s,r \in \mathcal{N}} \mathcal{R}(s,r)} |\mathcal{S}_{sr}(\mathcal{F}) - \mathcal{S}_{sr}(\mathcal{I})|}{\sum_{\forall_{s,r \in \mathcal{N}} \mathcal{R}(s,r)} |\mathcal{S}_{sr}(\mathcal{I})|},$$

and

$$\overline{Miss(\mathcal{F})} = \frac{\sum_{\forall_{s,r \in \mathcal{N}} \mathcal{R}(s,r)} |\mathcal{S}_{sr}(\mathcal{I}) - \mathcal{S}_{sr}(\mathcal{F})|}{\sum_{\forall_{s,r \in \mathcal{N}} \mathcal{R}(s,r)} |\mathcal{S}_{sr}(\mathcal{I})|}.$$

6.2. *A solution to the hidden node problem*

A heterogeneous wireless ad hoc network of mobile devices is composed of devices with different computation and communication capabilities. Asymmetric links dominate routing in such a network [35] and the sender may not be able to receive the CTS or ACK packets from the receiver. In such a case a DATA packet, or the next frame cannot be sent. The IEEE 802.11 protocol assumes that all the connections are symmetric. Our protocol relaxes this assumption, asymmetric links can be used provided that they are part of a *three-party proxy set* [35].

Our protocol retains the use of RTS, CTS, DATA and ACK frames defined in IEEE 802.11 standard. In addition to these, we have four additional frames: XRTS (Extended RTS), XCTS (Extended CTS), TCTS (Tunneled CTS), and TACK (Tunneled ACK).

An ideal MAC layer protocol should be based upon a scheme which delivers the RTS and CTS packets to all hidden nodes in H_{rs} and H_{sr}, respectively. Such a scheme however can be impractical because (i) a node may not have knowledge of all its In-bound neighbors; (ii) the number of hops needed to reach an In-bound neighbor might be large, thus the time penalty and the power consumption required for the RTS/CTS diffusion phase might outweigh the benefits of a reduced probability of collision.

Our solution is to send RTS and CTS packets to the nodes in $H3_{rs}$ and $H3_{sr}$ respectively. In this way, a considerable number of nodes that are misclassified as "hidden" nodes by [1], referred to as protocol A, and [2], referred to as protocol B, are allowed to transmit (see Figure 7). Note that our approach does not identify all hidden nodes, but neither methods A or B are able to identify all hidden nodes.

6.3. *Node Status*

In IEEE 802.11, when a node overhears an RTS or a CTS packet, it becomes *silent* and cannot send any packet from then on until its NAV expires. In this way, nodes in the relay set cannot send XRTS/XCTS as they should be in a *silent* state after overhearing the RTS/CTS packet. To resolve this dilemma, we replace the *silent* state with a *quasi silent* state, in which a node is allowed to send control packets, except RTS and CTS.

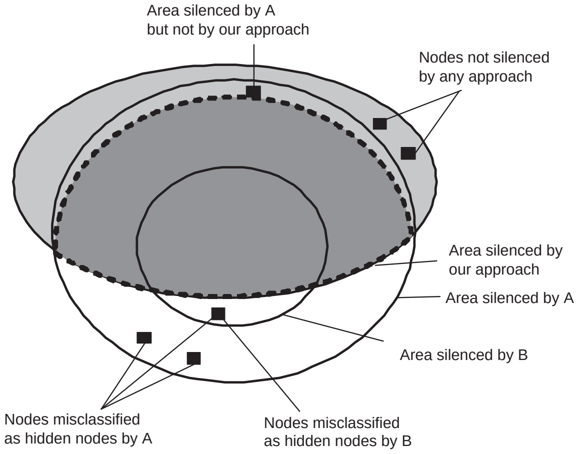


Fig. 7. The ability of three MAC layer protocols, A, B, and the one introduced in this paper, to correctly classify "hidden" nodes. A protocol may incorrectly require nodes to be silent ("missclassify" them) and miss nodes which should be silent.

In the medium access model proposed in this paper, a node is either in an *idle* state, *active* state, *quasi silent* state, or *silent* state. When a node is in an *idle* state, it is able to send or receive any type of packets. When a node is in *active* state, the node is either sending or receiving a packet. When a node is in *quasi silent* state, the node can either receive packets or send any packet type except `RTS`, `CTS`, or `DATA` packet. When a node is in *silent* state, the node can receive packets but cannot send any packet.

6.4. *Medium Access Model*

The medium access model of our protocol is an extended four-way handshake. (see Figure 8)For short data frames, there is no need to initiate an `RTS-CTS` handshake. For long data frames we recognize several phases:

(1) Sensing phase. The sender s senses the medium. If it does not detect any traffic for a DIFS period, the sender starts the contention phase; otherwise, it backs off for a random time before it senses again.
(2) Contention phase. The sender s generates a random number $\gamma \in$ [0, contention window] slot time. The sender s starts a transmission if it does not detect any traffic for γ slot time.
(3) `RTS` transmission phase. The sender s sends an `RTS` packet to the receiver r. The `RTS` packet specifies the NAV(RTS), *link type* of L_{sr} and

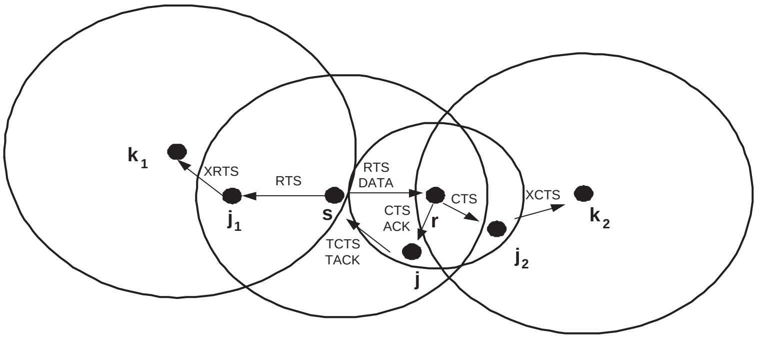


Fig. 8. Routing over asymmetric links in a heterogeneous wireless ad hoc network. Node s is the sender, r is the receiver, the link from node s to r is asymmetric, and node j is the proxy node that can relay traffic to s for r. Nodes k_1 and k_2 are hidden nodes for transmissions T_{rs} and T_{sr}, respectively. Nodes j_1 and j_2 are the proxy nodes that can relay traffic from s to k_1 and from r to k_2, respectively.

$MXHR3_{rs}$. The *link type* field is used to determine whether symmetric or asymmetric medium access model is used.

(4) CTS transmission phase. The receiver r checks whether the link is symmetric or not. If link L_{sr} is symmetric, node r sends a CTS packet back to node s; otherwise, node r sends a TCTS packet to node s. A TCTS packet specifies both the proxy node and the receiver s. The proxy node forwards the TCTS packet to the original sender s after receiving it. A CTS/TCTS packet can be sent only after sensing a free SIFS period. Instead of $MXHR3_{sr}$, $MXHR3_{rs} - MXHR3_{sr}$ is specified in the CTS/TCTS packet so that every extended hidden node relay is included only once thus the duration of XCTS/XRTS diffusion phase can be reduced.

(5) XRTS/XCTS diffusion phase. All nodes that overhear a RTS/CTS/TCTS packet enters a *quasi silent* state. After the CTS transmission phase, all extended hidden node relays that are either specified in RTS or CTS/TCTS starts contention for broadcasting XRTS/XCTS to its neighbors. When a node captures the medium, all other nodes backs off for a random number of (1, 4) SIFS period, and continue the contention until the XRTS/XCTS diffusion phase finishes. An XRTS/XCTS diffusion phase lasts for δ SIFS periods, after which all nodes except the proxy node becomes *silent.*

(6) Data transmission phase. When the XRTS/XCTS diffusion phase finishes, the sender s starts sending DATA packets to the receiver r after sensing

a free SIFS period.

(7) Acknowledgement phase. Once the receiver r successfully received the DATA packet from the sender s, it replies with an ACK if link L_{sr} is symmetric, or a TACK packet if link L_{sr} is asymmetric. An ACK/TACK packet can be sent only after sensing a free SIFS period. When the sender s receives an ACK/TACK packet, it starts contending the medium for the next frame. Meanwhile, the NAVs that are reserved for this transmission should expire.

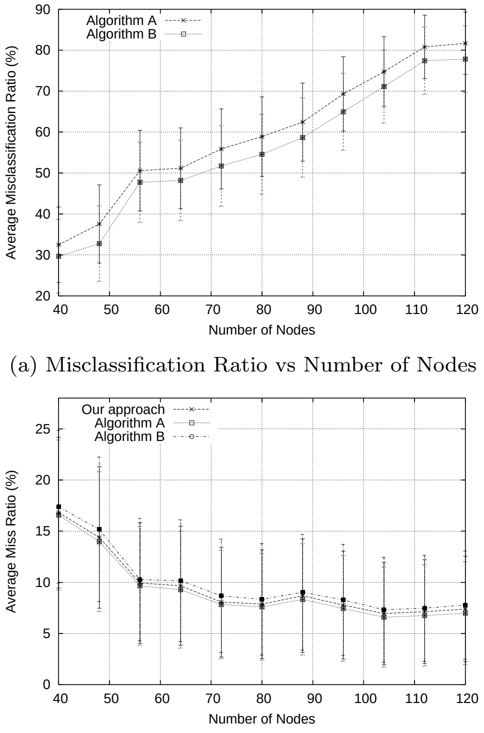
6.5. *A Simulation Study*

To evaluate the performance of the MAC layer protocols which support asymmetric links we conducted a simulation study. We compared the protocols in [1,2], and the one presented in this paper. We assume that the nodes are immobile and wish to study the number of nodes which are silenced by the RTS-CTS protocol as well as nodes which should be silenced but are not. In this experiment we do not consider other characteristics of devices, such as power reserve. We plan to expand these studies for the case when the nodes are mobile and assume that the nodes in the same class have a slight variation in their power reserve.

A node is *misclassified* as a hidden node and it is silenced by an algorithm while it should not have been. A node is *missed* if it should be considered a hidden node and silenced by an algorithm but it is not. We measure the average misclassification and the average miss ratio of the protocols under several scenarios and construct 95% confidence intervals for these averages. The scenario involves a rectangular simulation area of 500 × 500 meters. The transmission range for the four class of nodes [6,?], $C1$, $C2$, $C3$, and $C4$ are random variables normally distributed with the mean $25, 50, 75$, and 100 meters, respectively; the standard deviations for each class is 5 meters. The simulation scenario is created using a set of 40 to 100 nodes, which belong to one of the 4 classes. The initial positions of the nodes are uniformly distributed in the area, while the number of nodes in each class is equal.

For each generated scenario, we repeat the experiment 100 times. For each replica of the experiment, the nodes are in slightly different position. The displacement is normally distributed around an initial position and the standard deviation is 20% of its transmission range.

Figure 9(a) illustrates the average misclassification ratio of protocols A [1] and B [2] as a function of the number of nodes. A and B perform



(a) Misclassification Ratio vs Number of Nodes

(b) Miss Ratio vs Number of Nodes

Fig. 9. (a) The average misclassification ratio of protocols A and B as a function of the number of nodes. As an artifact of node immobility in our simulation study, the protocol introduced in this paper has a zero average misclassification ratio. A node is misclassified if it is required to be silent unnecessarily. (b) The average miss ratio of protocols A, B, and our approach, as a function of the number of nodes. Missed nodes should be required to be silent but are not.

similarly; the average misclassification ratio ranges from 34.10% to 70.42%, and increases with the number of nodes. As an artifact of node immobility, in our simulation the algorithm introduced in this paper has a zero average misclassification ratio.

Figure 9(b) illustrates the average miss ratio of protocols A, B, and the one introduced in this paper as a function of the number of nodes. The protocols perform similarly; the average miss ratio ranging from 5.55% to 16.36%. The average miss ratio for our approach is slightly larger than that of protocol A but smaller than the average miss ratio of protocol B. The average miss ratio decreases as the number of nodes increases. Protocol A achieve slightly better performance but requires more power consumption and generates additional collisions, compared to protocol B and our approach.

7. Cross-Layer Architecture

There is a growing consensus that cross-layer communication is necessary to fully exploit the possibilities offered by wireless networks. The complex nature of a heterogeneous wireless networks with asymmetric links requires information flow across several layers of the protocol stack. For example, software radio requires dynamic spectrum management. The goal of dynamic spectrum management is to determine the rights of nodes to transmit on a certain channel, at a specific power, time interval and geographic location. There is a strong interdependency between the spectrum management and the MAC and routing protocols. The spectrum allocation determines the possible topologies which can be achieved by the MAC and network layers. Conversly, we want the minimum spectrum allocation which makes a given topology feasible. The ability of the MAC and routing protocols to handle asymmetric links allows spectrum management to determine the transmission rights of the nodes independently; the pairing requirements, inevitable for bidirectional links, are not applicable. This allows for a more efficient spectrum allocation.

One of the consequences of operating in the context of a MANET with asymmetric links is that the information of three-party proxy sets needs to be maintained both at the MAC and the network layer. With the knowledge of three-party proxy sets, reverse routes (for upper routing protocol) or tunnels (for underlying MAC protocol) for an asymmetric link can be computed.

In our approach, the required information is maintained by the MAC layer protocol `TPSDM` (Three-party Proxy Set Discovery and Maintenance). `TPSDM` stores information of three-party proxy sets at a shared module, which could be fetched by the routing module of network layer.

In `TPSDM`, each node maintains a *neighbor table* that contains six fields: node id, location, transmission range, neighbor type, P-node list, and timestamp list. Each node periodically broadcasts a 1-hop limited *Hello* message which encloses the node id, location and transmission range of its neighbors along with its own. When a node receives a *Hello* message, it applies a `TPSDM` Algorithm on the incoming *Hello* message and its own neighbor table. The algorithm first identifies the neighbors of the current node for each entry of the incoming *Hello* message and stores them into the neighbor table along with the neighbor type. For each entry of the incoming message a three-party proxy set is found if a directed circle is formed by the links connecting the current node, the node of the incoming *Hello* message, and the node of an entry. If a node detects a three-party proxy set in which it plays the role of L-node or H-node of an asymmetric link, the proxy node and the current time are appended onto the *P-node list* and the *timestamp list* of H-node entry in the neighbor table, respectively. In case the current node is an L-node, the P-node is the node through which the current node can reach the H-node, thus one or more tunnels to the H-node is established; in case the current node is the H-node, the *Hello* message of the P-node carries the information of the L-node, which notifies or renews the information of the L-node at the current node.

The maintenance of three-party proxy sets is achieved by periodically checking the *timestamp list* field. When TPSDM detects the expiration of a timestamp, the associated P-node is purged; when the *P-node list* becomes empty, the entry of the node is purged from the neighbor table in case it is an out-bound neighbor.

8. Work in Progress

We have implemented the network and MAC layer protocols in NS2 and we are conducting experiments to assess their advantages over protocols based upon IEEE 802.11 and their performance. We discuss briefly an example when the A4LPprotocol uses asymmetric links to route messages from node 0 to node 4 while protocols for symmetric links fail to find a route. In our simulation we use FTP as the transport layer protocol.

The initial position of nodes is depicted in Figure 10, which shows also the transmission range and the distance between the nodes. The nodes do not move during the simulation. The forward and reverse routes are found and established by A4LP, and MAC layer acknowledgements are assured by our MAC protocol. For instance, node 5 is a proxy node that forwards CTS and ACK packets for a unidirectional transmission from node 1 to node 4 at MAC layer. The packets are successfully delivered and acknowledged.

9. Summary

In this paper we argue that asymmetry of the transmission range in wireless networks is a reality and should be treated as such. This asymmetry makes

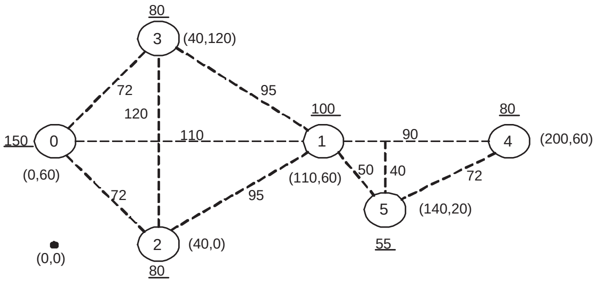


Fig. 10. The topology of a network when the A4LP protocol routes messages from node 0 to node 4 over asymmetric links, while protocols for symmetric links fail to find a route. The initial position, range, and distance between nodes are shown.

reliable communication more difficult and complicates medium access control as well as network layer protocols. In some instances, e.g., in case of software radio, we should be able to take advantage of this asymmetry.

The models of traditional multiple access networks assume that all nodes share a single communication channel and have access to the feedback (success, idle slot, collision) from any transmission. In this case splitting algorithms allow sharing of the communication channel in a cooperative environment with reasonable efficiency and fairness. This is no longer the case for wireless networks with symmetric or bidirectional links, where the sender and the receiver do not share the feedback channel and hidden nodes may interfere with a transmission. In case of networks with asymmetric links hidden nodes are out of the reach of the sender and the receiver, but their transmissions may interfere with the reception of a packet by the intended destination. The problem of hidden nodes is further complicated in this case because the feedback from the receiver in an RTS - CTS exchange may have to pass through several relay stations before reaching all the nodes which are supposed to be silent. Some of the solutions proposed in the literature reduce the probability of a collision by requiring a larger than necessary set of nodes to be silent. In turn, this has negative effects upon the communication latency and the overall network throughput. We propose a MAC layer protocol which reduces the number of nodes that have to be silent but as all the other schemes proposed may miss some of the nodes which should have been classified as "hidden".

MAC layer and routing protocols are further complicated by the need to minimize the number of retransmissions to reduce the power consumption and collisions. We propose a technique to address this concern; m-limited forwarding was conceived to reduce the cost of disseminating information in a power-constrained environment by limiting the cardinality of the subset of nodes which retransmit a packet.

While more studies are necessary to confirm our results that m-limited forwarding with $\tau_k(i,j)$ fitness function and $m = 2$ is a serious contender to flooding for disseminating control information in a power-constrained, location-aware ad hoc network with bidirectional links. Ongoing evaluation of m-limited forwarding for wireless networks with asymmetric links may led to slightly different conclusions, e.g., it is likely that $\eta_k(i,j)$- may prove to be better than $\tau_k(i,j)$-based policies.

There is a growing consensus that cross-layer communications is necessary to fully exploit the possibilities offered by wireless networks. The complex nature of a heterogeneous wireless networks with asymmetric links requires information flow across several layers of the protocol stack. In this paper we sketch a possible architecture which allows information about network status to flow across layers.

Our future work is dedicated to the applications of m-limited forwarding to MAC and network layer protocols for heterogeneous ad hoc networks with asymmetric links. We have reported only on partial results; further simulation and possibly analytical studies are needed to provide conclusive proofs that the protocols presented in this paper offer a viable alternative and perform better than existing solutions.

Acknowledgments

The research reported in this paper was partially supported by National Science Foundation grants MCB9527131, DBI0296035, ACI0296035, and EIA0296179.

References

1. N. Poojary, S. V. Krishnamurthy, and S. Dao, "Medium access control in a network of ad hoc mobile nodes with heterogeneous power capabilities," in *Proceedings of IEEE ICC 2001*, vol. 3, 2001, pp. 872–877.
2. T. Fujii, M. Takahashi, M. Bandai, T. Udagawa, and I. Sasase, "An efficient MAC protocol in wireless ad-hoc networks with heterogeneous power nodes," in *The 5th International Symposium on Wireless Personal Multimedia Communications (WPMC '2002), Hawaii*, vol. 2, 2002, pp. 776–780.
3. "DARPA Advanced Technology Office - FCS Communications program," URL `http://www.darpa.mil/ato/programs/fcs_comm.htm`.
4. "Joint Tactical Radio System (JTRS)," URL `http://jtrs.army.mil`.

5. "Federal Communications Commission Notice of Inquiry FCC 03-289 regarding the interference temperature model," URL `http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-289A1.pdf`.
6. D. C. Marinescu, G. M. Marinescu, Y. Ji, L. Bölöni, and H. Siegel, "Ad hoc grids: Communication and computing in a power constrained environment," in *Proceedings of the Workshop on Energy-Efficient Wireless Communications and Networks (EWCN)*, 2003, pp. 113–122.
7. Y. Afek and E. Gafni, "Distributed algorithms for unidirectional networks," *SIAM Journal on Computing*, vol. 23, no. 6, pp. 1152–1178, 1994. [Online]. Available: citeseer.ist.psu.edu/afek93distributed.html
8. C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *ACM SIGCOMM '94*, 1994, pp. 234–244.
9. C.-C. Chiang, H.-K. Wu, W. Liu, and M. Gerla, "Routing in clustered multihop, mobile wireless networks with fading channel," in *Proceedings of IEEE SICON'97*, 1997, pp. 197–211.
10. S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A. Woodward, "A distance routing effect algorithm for mobility (DREAM)," in *Proceedings of the ACM MOBICOM '98*, 1998, pp. 76–84.
11. T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in *Proceedings of IEEE INMIC*, December 2001, pp. 62–68.
12. D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, Imielinski and Korth, Eds. Kluwer Academic Publishers, 1996, ch. 5, pp. 153–181.
13. C. Perkins and E. Royer, "Ad hoc On-demand Distance Vector Routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1999, pp. 99–100.
14. Y. Ko and N. Vaidya, "Location-Aided Routing (LAR) in mobile ad hoc networks," in *Proceedings of the Fourth Annual ACM International Conference on Mobile Computing and Networking (MobiCom 1998)*, 1998, pp. 66–75.
15. V. Park and M. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in *Proceedings of INFOCOM '97*, vol. 3, 1997, pp. 1405–1413.
16. Z. Haas and M. Pearlman, "The zone routing protocol (ZRP) for ad hoc networks," in *Internet Draft*, 1998.
17. C. E. Jones, K. Sivalingam, P. Agrawal, and J. C. Chen, "A survey of energy efficient network protocols for wireless networks," *Wireless Networks*, vol. 7, pp. 343–358, 2001.
18. M. Maleki, K. Dantu, and M. Pedram, "Power-aware source routing protocol for mobile ad hoc networks," in *Proceedings of the 2002 international symposium on Low power electronics and design*, 2002, pp. 72–75.
19. S. Singh, M. Woo, and C. Raghavendra, "Power-aware routing in mobile ad hoc networks," in *Proceedings of Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM '98)*, 1998, pp. 181–190.

20. J. H. Y. Xu and D. Estrin, "Geography-informed energy conservation for ad hoc routing," in *Proceedings of 7th Annual International conference on Mobile Computing and Networking (Mobicom '01)*, 2001, pp. 70–84.
21. D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," in *Ad Hoc Networking*, C. E. Perkins, Ed. Addison-Wesley, 2001, ch. 5, pp. 139–172.
22. Z. Haas, M. Pearlman, and P. Samar, "The intrazone routing protocol (IARP)," in *Internet Draft, draft-ietf-manet-zone-iarp-02.txt*, 2002.
23. Z. Haas, M. Pearlman, and P. Samar, "The interzone routing protocol (IERP)," in *Internet Draft, draft-ietf-manet-zone-ierp-02.txt*, 2002.
24. P. Sinha, S. Krishnamurthy, and S. Dao, "Scalable unidirectional routing using ZRP extensions for wireless ad-hoc networks," in *Proceedings of IEEE WCNC 2000*, September 2000, pp. 1329–1339.
25. S. Corson, S. Papademetriou, P. Papadopoulos, V. Park, and A. Qayyum, "An Internet MANET Encapsulation Protocol (IMEP)," IETF," Internet Draft, August 1999.
26. L. Kleinrock and F. Tobagi, "Packet switching in radio channels: Part i - carrier sense multiple-access modes and their throughput-delay characeteristics," *IEEE Transactions on Communications*, vol. COM-23, no. 12, pp. 1400–1416, 1975.
27. P. Karn, "Maca - a new channel access method for packet radio," in *Proceedings of the 9th ARRL Computer Networking Conference*, 1990, pp. 134–140.
28. V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, "MACAW: A media access protocol for wireless lan's," in *Proceedings of ACM SIGCOMM '94*, 1994, pp. 221–225.
29. C. Fullmer and J.J.Garcia-Luna-Aceves, "Floor Acquisition Multiple Access (FAMA) for packet-radio networks," in *Proceedings of ACM SIGCOMM '95*, 1995, pp. 262–273.
30. "IEEE std 802.11b-1999. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," Tech. Rep., August 1999.
31. V. Bharghavan, "A New Protocol for Medium Access in Wireless Packet Networks," Urbana, IL: Timely Group, Tech. Rep., 1997.
32. V. Ramasubramanian and D. Moss, "Statistical analysis of connectivity in unidirectional ad hoc networks," in *Proceedings of the International Workshop on Ad Hoc Networking 2002, Vancouver*, 2002, pp. 109–115.
33. V. Ramasubramanian, R. Chandra, and D. Mosse, "Providing a bidirectional abstraction for unidirectional ad-hoc networks," in *Proceedings of INFOCOM 2002*, vol. 3, 2002, pp. 1258–1267.
34. S. Nesargi and R. Prakash, "A tunneling approach to routing with unidirectional links in mobile ad-hoc networks," in *Proceedings of Ninth International Conference on Computer Communications and Networks*, 2000, pp. 522–527.
35. G. Wang, Y. Ji, D. C. Marinescu, and D. Turgut, "A routing protocol for power constrained networks with asymmetric links," in *Proceedings of the ACM Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN)*, 2004, pp. 69–76.
36. L. Breslau, D. Estrin, K. Fall, S. Floyd, J. Heidemann, A. Helmy, P. Huang,

S. McCanne, K. Varadhan, Y. Xu, and H. Yu, "Advances in network simulation," *IEEE Computer*, vol. 33, no. 5, pp. 59–67, 2000.

37. "VINT project. the ucb/lbnl/vint network simulator-ns (version 2)," URL `http://www.isi.edu/nsnam/ns`.
38. "CMU Monarch extensions to ns," URL `http://www.monarch.cs.cmu.edu`.
39. J. Broch, D. A. Maltz, D. B. Johnson, Y. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in *Proceedings of Mobile Computing and Networking*, 1998, pp. 85–97.
40. V. Kawadia and P. Kumar, "A cautionary perspective on cross layer design," University of Illinois, Tech. Rep., June 2003.