ON THE PERFORMANCE OF A MEDIUM ACCESS CONTROL SCHEME FOR THE RECONFIGURABLE WIRELESS NETWORKS

Zygmunt J. Haas

School of Electrical Engineering
Cornell University, Ithaca, NY 14853
`http://www.ee.cornell.edu/~haas/wnl.html`

Abstract

In this paper, we propose a MAC protocol for an ad-hoc network architecture, termed by us the Reconfigurable Wireless Networks*, and investigate its performance. We discuss the access synchronization and the construction of network connections features of the MAC protocol. Using event-driven simulation, we evaluate the throughput and the blocking probability of the scheme, demonstrating its behavior for different parameters of the mobility, traffic, and propagation models.*

Introduction

A *Reconfigurable Wireless Network* (RWN), which was introduced in [1], is an ad-hoc network architecture that can be rapidly deployed, without relying on a preexisting fixed network infrastructure. The nodes in a RWN can dynamically join and leave the network, frequently, often without warning, and without disruption to other nodes' communication. RWNs are a special case of the ad-hoc network architecture and distinguish themselves in the following features: large network span, large number of nodes, and highly mobile nodes. In particular, the node

---

Portions reprinted, with permission, from *Proceedings of MILCOM'97, Monterey, CA, November 2-5, 1997.*

constellation can change rapidly, and so is the presence or absence of links. Examples of the use of the RWNs are:

- military (tactical communication) - for fast establishment of a communication infrastructure during deployment of forces in a foreign and hostile terrain,
- rescue missions - for communication in areas without adequate wireless coverage,
- national security - for communication in times of national crisis, where the existing communication infrastructure is non-operational due to a natural disaster or a global war,
- law enforcement - similar to tactical communication,
- commercial use - for setting up communication in exhibitions, conferences, or sale presentations,
- education - for operation of virtual classrooms, and
- sensor networks - for communication between intelligent sensors (e.g., MEMS[1]) mounted on mobile platforms.

In contrast with the conventional cellular networks, in the RWNs, direct mobile-to-mobile (**peer-to-peer**) communication is allowed. Mobiles that cannot be reached directly, use other mobiles to relay their transmissions using **multi-hop** routing.

There is a number of central issues that need to be addressed to make the RWN a workable system: the mobility management, the routing protocol, and the Medium Access Control (MAC) scheme. In this paper, we deal with the MAC scheme. A routing protocol applicable to the RWN architecture – the *Zone Routing Protocol* - was introduced in [2] and further evaluated in [3]. Finally, we will report on the RWN mobility management scheme in a future publication.

In general, the MAC for wireless networks has been a subject of extensive studies, mostly concentrating on random access mechanisms. The traditional MAC schemes for radio networks, such as the Carrier Sense Multiple Access (CSMA), do not fully address the "hidden terminal problem." Newer schemes, such as *MACA* [4], *MACAW* [5], and *FAMA* [6] rely on low-level reservation mechanism. In these protocols, the RTS/CTS (Request-To-Send/Clear-To-Send) dialog precedes any communication between nodes. The MACAW protocol includes an additional feature of acknowledging, on the link layer, the received transmissions and, thus, provides fast recovery from collisions. In the FAMA protocol, the non-persistent CSMA scheme is used, which avoids repetitious collisions.

It should be noted that all these protocols do not resolve the hidden terminal problem and, therefore, do not prevent collisions. The notorious example is when a node, which did not hear the RTS/CTS dialog, migrates to within reception range of the already communicating nodes. A similar situation occurs when a node (due to transmission errors, for example) did not hear the CTS reply. In such cases, any transmission attempt of this node will most probably result in a collision. Additionally, because of the random access nature of these schemes, reservations of network capacity for real-time multimedia traffic cannot be easily accommodated.

---

[1] Micro Electro Mechanical Systems

As opposed to random access schemes, controlled-access schemes do not suffer from the above shortcomings. Controlled-access schemes have been considered before for multi-hop network environment; for example, the *Cluster TDMA* scheme [7]. The difficulty with these schemes, however, is that they require network-wide synchronization. This appears to be a significant problem, especially in a fast changing communication environment, such as the RWNs.

We propose here a hybrid of random- and controlled-access schemes, based on a local polling mechanism. It exhibits controlled-access behavior among neighbor nodes due to polling. Yet, the polls originating at different nodes are random and unsynchronized, and, thus, may lead to collisions. However, as the length of the polls is short compared with the actual data transmission and as the number of competing nodes is restricted to a subset of the neighbors only, the loss of capacity due to the random-access process is relatively small. The salient features of our scheme are that it requires local synchronization only (i.e., among the neighbors) and that it eliminates collisions of payload information. Additionally, it reduces the access time variance and inherently allows capacity reservation. Thus, it is applicable to multimedia traffic.

Medium Access Control (MAC) Protocol

The purpose of a MAC protocol is to synchronize access of mobiles to the shared communication medium. In the RWN, the span of the network is considerably larger than the transmission range of a single node transceiver. This necessitates multi-hop routing.

A MAC can be based on a single shared-channel[2] or multiple channels. Use of a single shared-channel MAC scheme requires each transceiver to operate at the maximum channel bit-rate. In addition, single shared-channel can lead to inefficient operation or to the need for network-wide access synchronization. Thus, a multi-channel solution, in which nodes are assigned individual channels, is a more viable option. Of course, in the multi-channel approach, channels can be reused in spatially separated areas and can be based on different multiple access schemes, such as TDMA or CDMA. Our work is independent of the actual multiple access scheme used. The determination of the actual multiple access scheme, as well as the channel/code allocation algorithm, are outside the scope of this work.

MAC-layer connections are established between neighbors.[3] With time, mobiles can become separated by large enough distance or by a radio propagation obstacle, so that connections will be broken. Likewise, mobiles can migrate close enough to each other to become neighbors and to establish new connections.

We assume the following elements of the MAC scheme:

- The transmission spectrum is divided into channels. For the sake of simplicity, we assume here that channels are created in time and frequency (FDMA/TDMA), rather than in code (i.e., CDMA). Nevertheless, the presented-here MAC scheme can be easily modified for CDMA-based transmission.

---

[2] In this work, we refer to a *channel* as a TDMA slot assignment on a particular frequency channel, or, in CDMA, as an assignment of one of the orthogonal codes. Note that this is not the traditional definition of a wireless channel.

[3] A mobile that can be reached directly by a mobile in question is referred to as the mobile's *neighbor*s.

- Each channel consists of two parts, which we call the *payload* and the *poll* portions of the channel. The bandwidth of the payload portion is larger than the bandwidth of the poll portion. The capacities of the payload and the poll depend on several factors and performance requirements. We label the payload portion of the k^{th} channel as Θ_k, and the poll portion as φ_k .
- Nodes are dynamically assigned channels. The reuse of channels is such that it corresponds to an acceptable Signal-to-Interference (SIR) ratio at the assigned nodes. Channel assignment schemes will not be discussed here.
- Each node maintains an updated list of who are its neighbors and what are their assigned channels (*neighbor-table*). This list is created and maintained as part of the *Neighbor Discovery* process, which will be explained later.
- Every node is equipped with two half-duplex transceivers. Although, this is not an essential assumption, as our MAC protocol will also operate with a single transceiver per node, our study indicates that a considerable advantage in reliability and network capacity can be achieved with two half-duplex transceivers. We term the two transceivers: an *in-transceiver* and an *out-transceiver.*

In reference to this last point: inclusion of two transceivers per station increases the reliability of the network. In a peer-to-peer routed network, such as the RWN, failures of a single-transceiver node can lead to network partitioning and to loss of connectivity with some network nodes. On the other hand, our MAC protocol is designed in such a way that a node can still continue to operate even when a failure of one of the two transceivers occurs (although the node's capacity is reduced).

Access Synchronization

Access synchronization is based on the operation of the two node's transceivers. Ordinarily, one node's transceiver (referred to here as *out-transceiver*) is assigned to traffic from the node in question to other nodes, while the other transceiver (the *in-transceiver)* is used for communication in the other direction.

The operation of the access synchronization is based on every node continuously polling its neighbors to determine whether they have any communication to send. The polling is performed on the poll portions of the channels. For illustration, assume that node-*k* is assigned the channel (Θ_k,φ_k) and its two neighbors, node-*i* and node-*j,* are assigned frequencies (Θ_i,φ_i) and (Θ_j,φ_j), respectively. Node-*k* tunes its in-transceiver to φ_i, polling the node-*i* for any data and immediately retunes its in-transceiver for reception on Θ_k. As the out-transceiver of node–*i* is ordinarily tuned to φ_i, it receives the poll and, assuming it has nothing to send to node-*k*, it responds with End-Of-Transmission (EOT) message on Θ_k. Node-*k* proceeds now to poll node-j on φ_j. Now assume that node-j has a number of packets to send to node-k. Node-j, after receiving the poll on its out-transceiver (ordinarily tuned to φ_j), tunes it to Θ_k and transmits the packets, ending with the EOT message. Node-k then starts a new poll cycle. The procedure is depicted in Figure 1, where the oval indicates tuning of the particular transceiver to the specified frequency.

Note that all the nodes perform the same procedure. Thus, at the same time as node-k polls its neighbors, the neighbor nodes (node-i and node-j) both poll node-k, which has his out-transceivers ordinarily tuned to its polling frequency, φ_k. In

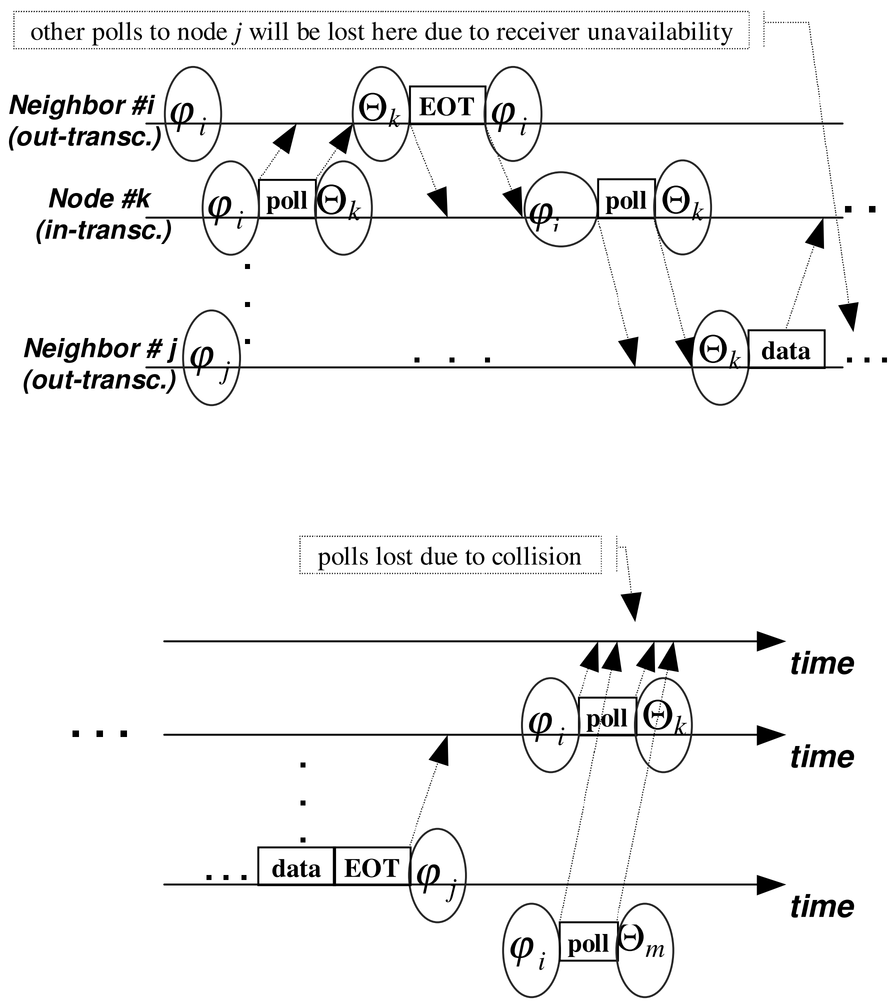

Figure 1: Access Synchronization Mechanism

summary, the process is as follows: In general, a node's out-transceiver is tuned to its own polling frequency. When a poll arrives, the node answers the poll (by either sending packets and/or EOT message) on the polling node's payload frequency. A node's in-transceiver is used for polling its neighbors by tuning to their polling frequency, sending a poll message and retuning to its own payload frequency to hear the polled node answer.

Of course, as the polling channels are unsynchronized, there is a possibility of polls collisions and of some of the polls being lost. (See Figure 1 for an example.) If a polling node gets no response to its poll within the specified time-out interval (*poll_time-out)*, it repeats the poll in the next cycles for up to maximum number of attempts (*max_poll_attempts).* If all the attempts fail, then the neighbor is placed on a watch-list. If no polls are received from the neighbor within *max_poll_cycle,* the link to the neighbor is considered lost and the neighbor identity is removed from the local *neighbor-table*.

A number of comments regarding the access synchronization scheme:

- As a node has full control over access to its payload portion of the channel, there are no collisions on the payload portion of the channel and, consequently, no packet transmission is lost due to collisions.
- While responding to a poll, a node can send only a limited number of packets. This number determines the maximum time a node can spend away from its frequency, *max_transmission_time*. The goal is to ensure that other nodes have a chance to communicate as well and to allow bandwidth reservations for multimedia traffic. However, when only few nodes want to communicate, the poll will return to the ready station sooner, allowing the station to capture larger portion of the channel.
- A possible modification is to allow a two-way traffic exchange, once a poll is answered. Such a modification increases reliability by preserving connectivity while loss of a single transceiver occurs.

Construction of network's connections

As the network nodes migrate, existing connections between adjacent nodes are broken and new connections are made possible. The *Network Construction* procedure is responsible for updating the connections' status. To accomplish this, each node maintains a list (*neighbor_table)* of all the nodes with which it can establish a direct link (referred to here as *neighbor*s*). Neighbor Discovery* is the process by which a node learns about its new neighbors. (Note that the reverse process, removal of out-of-reach nodes from the *neighbor_table*, is triggered by missing poll responses, as explained above.) The *Neighbor Discovery* process is performed by the in-transceivers, scanning the available channels and discovering polling messages from adjacent nodes.[4] (Note that when a node has no neighbors, it still periodically sends null polling messages.) In particular, when a message is received with "good enough quality" (e.g., sufficient Signal to Interference Ratio), the node starts the neighbor acquisition process by including the new neighbor in its next polling cycle. After one successful polling response from the neighbor, the

[4] This process is inspired by the search of control channels for handoff purpose in a cellular network. For example, this process is implemented by the "idle slot" in GSM.

neighbor is added to the *neighbor_table*. The principle of the process is shown in Figure 2.

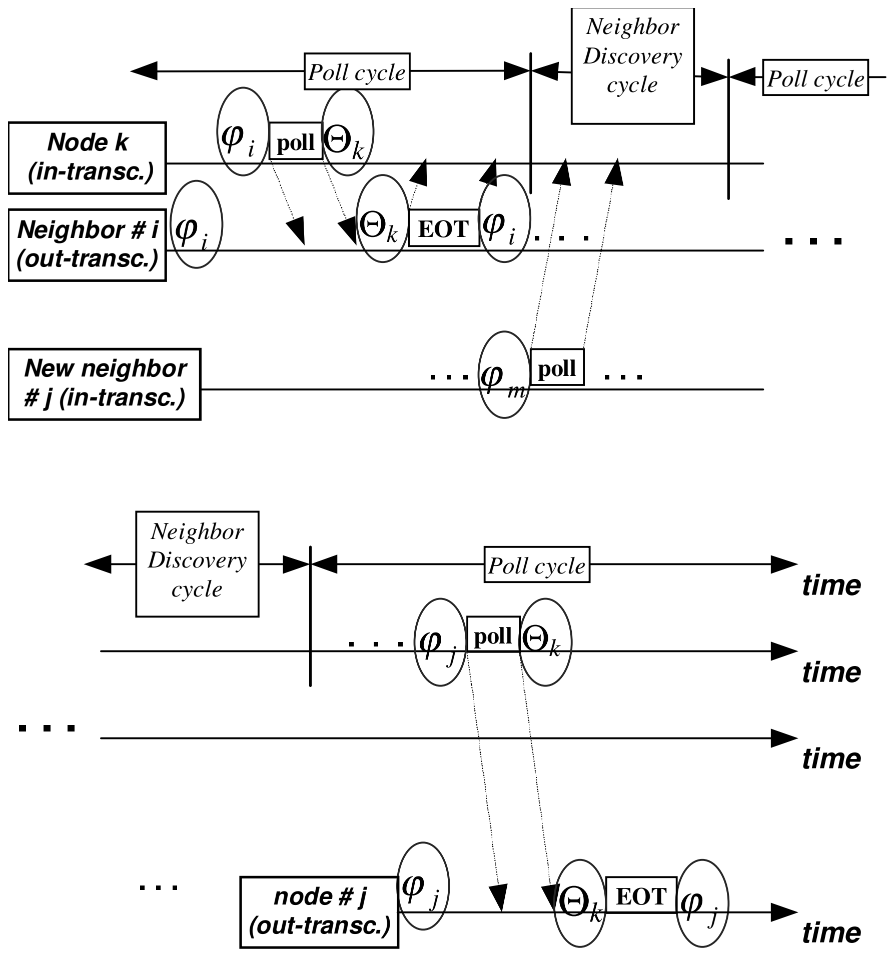

Fig 2: The Neighbor Discovery Mechanism

The Network, Traffic, and Radio Models

The coverage area of our network is a $1[km]\times 1[km]$ closed area (see [2] for the definition of a closed area). Initially, the mobiles are randomly distributed throughout this area. Each node is equipped with a transmitter/receiver pair, operating in the half-duplex mode. We assumed a narrowband system, in which the total spectrum is divided into channels through the FDM/TDMA technique. To make sure that the blocking is not spectrum- but system-limited, the system has large enough number of channels. The maximum transmission power of a mobile limits its connectivity to within an area of the radius r_{max}.

Each node can be in one of the four possible states: *idle, receive, transmit,* and *transmit/receive.* The transitions between the states are shown in Figure 3.

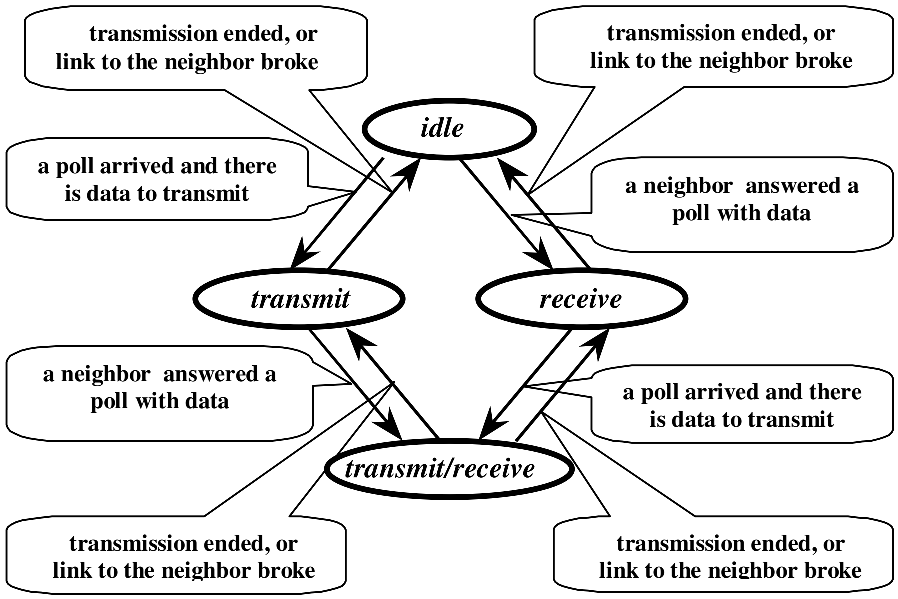

Fig 3: State transition diagram

Packets arrive to mobiles in a random manner with total inter-arrival time and the packet transmission time modeled as negative exponential distributions with parameters $1/\lambda$ [sec/packet] and $1/\mu$ [sec/packet], respectively. There is no distinction between the local and the to-be-forwarded traffic. Packets have to be fully received before they are forwarded to a neighbor node. Packets that arrive to a mobile while the mobile is already transmitting are considered blocked. Upon arrival of a packet, a destination is randomly chosen from the set of neighbors. If the node has no neighbors, the packet is considered blocked. If the destination neighbor is already receiving from another node, the packet is again blocked. Note that due to the dual-transceiver feature, the transmission and the receiving processes are decoupled. In other words and for example, if a packet is destined to a transmitting, but not receiving node, the packet is <u>not</u> blocked. A packet is considered *dropped* if during its transmission the link between the communicating nodes is broken due to mobility.

Blocked packets can be treated in several ways. The appropriate action depends on the reason for blocking the packet. In general, one possibility is to queue blocked packets. Another approach would be to discard blocked packets and alert the sending node (i.e., the previous node) or the local application (if the packet is locally generated) that the packet cannot be forwarded. The second choice might make sense in the highly versatile RWN environment, since a route to the destination might be broken while the packet is queued, effectively discarding the packet without notification. In such a case, a timeout mechanism and end-to-end retransmission would be necessary, at the expense of increased delay.[5] Discarding a packet with notification, on the other hand, might allow rerouting the packet through a different, available route. Possibly, a limited queue would be a better solution. In this paper, we assumed that a single buffer exists at each node and that blocked packets are discarded with notification. The treatment of blocked packets is still an open issue and we will not pursue it any further here.

The Mobility Model

Mobiles roam freely throughout the closed coverage area. At any point in time, mobile movement is characterized by two parameters, its velocity, $\vec{v}$, (value, v, and direction ϕ) and its current position, (x, y). The velocity is updated every time interval, Δt, according to the following formula:

$$v(t+\Delta t) = \min[\max(v(t)+\Delta v, 0), v_{\max}], \qquad (1)$$

where Δv is a uniformly distributed random variable in $[-\alpha \cdot \Delta t, \alpha \cdot \Delta t]$, $v_{\max}$ is the maximal mobile velocity, and α is the maximal mobile node acceleration/deceleration (assumed here to be of equal magnitude). The movement direction, ϕ , is also updated every Δt:

$$\phi(t+\Delta t) = \phi(t) + \Delta\phi, \qquad (2)$$

where $\Delta\phi$ is a uniformly distributed random variable in $[-\Delta\phi_{\max} \cdot \Delta t, \Delta\phi_{\max} \cdot \Delta t]$, and $\Delta\phi_{\max}$ represents the maximal angular change per unit time. This mobility model is an improvement on the previously used in the literature Brownian Motion model. The initial velocity $\vec{v}$ of the mobiles is assumed random, within the above-mentioned constraints.

The Simulation

We have simulated our MAC protocol with the above models by an event-driven simulation. The purpose of the simulation was to determine the effect of different parameter setting on the performance of the network. In particular, we evaluated the average system blocking and the total system throughput as a function of the number of mobiles in the system (M), maximal transmission radius ($r_{\max}$), maximal velocity ($v_{\max}$), the length of the Discovery Cycle (τ_{disc}), and the system loading (λ^{-1}).

---

[5] Of course, retransmission is not an option for real-time traffic and, thus, discarding packets without a notification to a previous node would result in reduced communications quality.

Numerical Results

Our simulation was tested for the range of parameters' values, as shown in the following Table. When the effect of a parameter was considered, all other parameters were assigned their respective default values.

Parameter	**Symbol**	**Default Values (Range)**
Coverage area	$S \times S$	1[km] X 1[km]
Discovery Cycle duration	τ_{disc}	100 [msec] (100[msec] - 300[msec])
Discovery Cycle deviation	$\Delta\tau_{disc}$	10 [msec]
Poll Cycle duration	τ_{poll}	900 [msec]
Poll Cycle deviation	$\Delta\tau_{poll}$	50 [msec]
Number of mobiles	M	40 [mobiles] (20 - 60)
Time increment	Δt	100 [msec]
Maximal transmission radius	$r_{\max}$	500 [meter] (100[m] - 300[m])
Maximal angular change	$\Delta\phi_{\max}$	$0.2 \cdot \pi$ [rad/sec]
Maximal velocity	$v_{\max}$	65 [mph] (15[mph] - 195[mph])
Acceleration/Deceleration	α	0.5 [m/sec^2]
Average packet transmission duration	μ^{-1}	100 [msec]
Average call inter-arrival time	λ^{-1}	0.5 – 10 [packets/sec]

The Discovery Cycle and Poll Cycle deviations were introduced to eliminate synchronized blocking phenomenon. Furthermore, in our simulations, we observed that the value of the time increment (Δt), has very little effect on the results of the simulation.

The results of the simulation are shown in Figures 4 - 11. The "Packet Arrival Rate" is the per-node total arrival rate. The "Throughput" is the aggregated per-node throughputs of all the network nodes[6]. Of course, to learn the effect of the various network's parameters, the relative, rather than the actual values of the throughput, are of most interest. The "Blocking probability" is the probability that an arrival packet cannot be immediately forwarded to the next node on its path. Note that this does not imply that these packets are necessarily lost, but it does indicate on how efficient the MAC is in forwarding packets.

[6] Note that this is not the traditional definition of network throughput. This definition was adopted because we are interested in the performance of the MAC scheme, rather than other network algorithms, such as the routing algorithm.

Figure 4 and 5 show the effect of changing the number of network nodes. With some number of nodes, the increase in the packet arrival rate results in smaller than linear increase in the throughput, due to the fact that the blocking probability increases as well with the increase in the packet arrival rate. From these figures, the throughput increases linearly with the number of mobiles and the blocking probability is not significantly affected by the number of users. This is the result of the fact that these figures were calculated under the assumption that the packet arrival rate per node is independent of the number of nodes. In general, increasing the number of nodes increases the per node arrival rate and this increase depends on the routing algorithm and on the average path length. That is, given the routing algorithm (and average path length), one could use these graphs to estimate the actual nodal throughput and blocking probability.

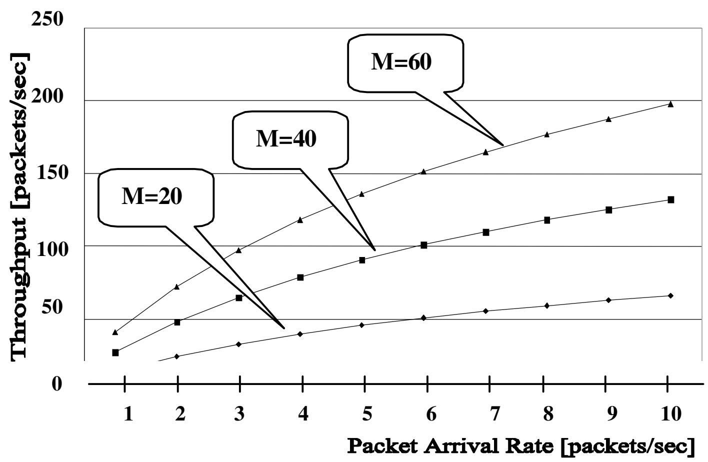

Fig 4: The effect of the number of users on throughput

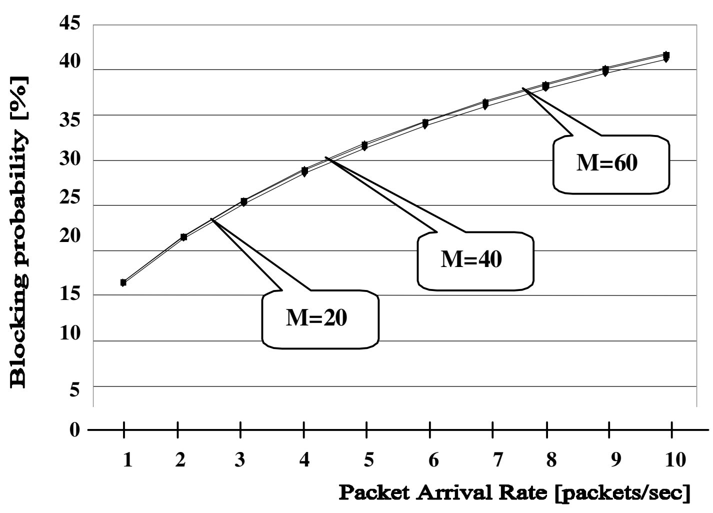

Fig 5: The effect of the number of users on blocking probability

Our conclusion from Figures 4 and 5 is that, with fixed per-node arrival rate, the nodal throughput and the blocking probability are independent of the number of network nodes.

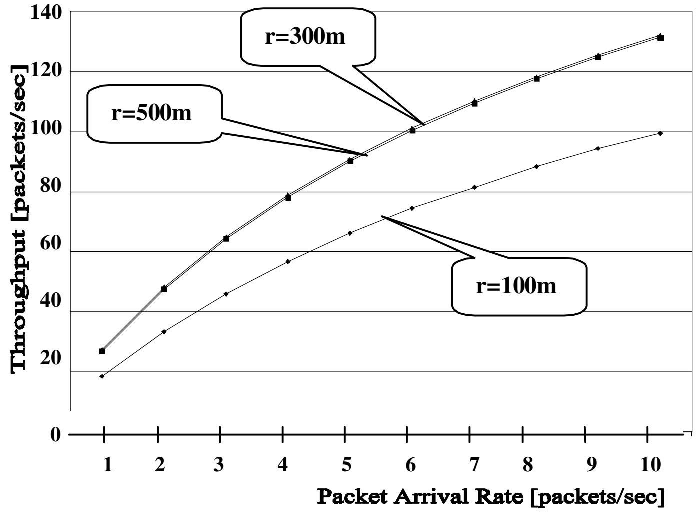

Fig 6: The effect of the transmission radius on throughput

Figures 6 and 7 show the effect of sizing the mobiles' transmission radius. The larger is the radius, the more neighbors each node has. Thus, the chance that a node has no neighbors (and, thus, blocks every packet) is minimized. Also, occupancy of

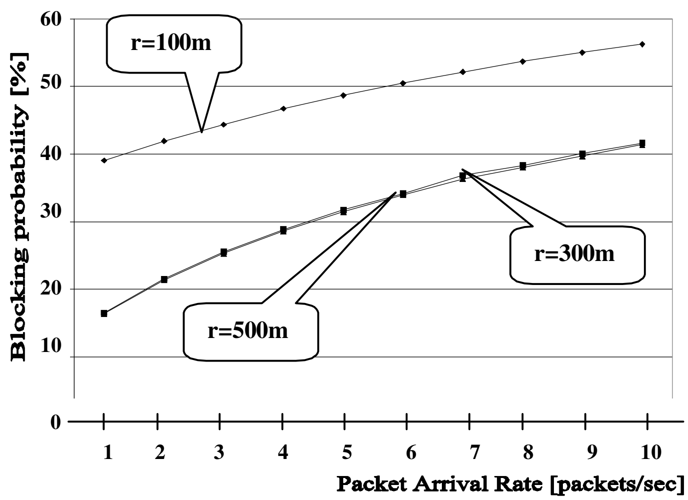

Fig 7: The effect of the transmission radius on blocking probability

the neighbor nodes tends to be more uniform. Consequently, the blocking probability decreases and the throughout increases. However, note that increasing the radius beyond the 100-200 [m] range has very little effect on the system performance. This reinforces and further qualifies our conclusion from Figures 4 and 5 that the number of network nodes has little effect on nodal throughput and blocking probability, as long as the number of nodes is larger than some minimum. (Or in other words, as long as each mobile has at least one neighbors that can be used to forward the received packets.)

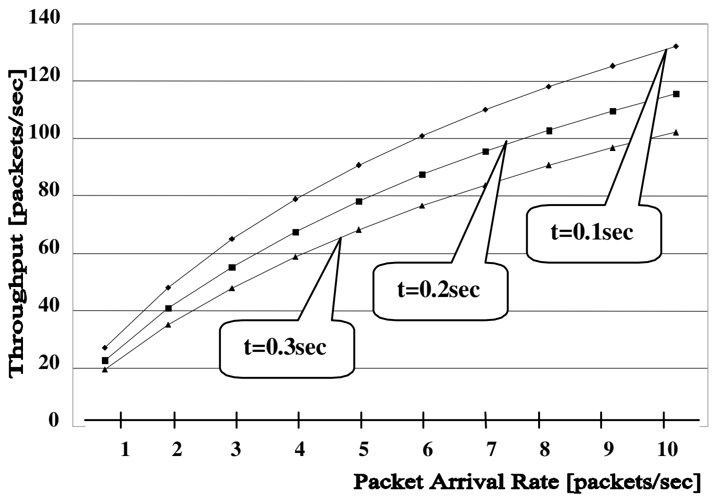

Fig 8: The effect of the Discovery Cycle length on throughput

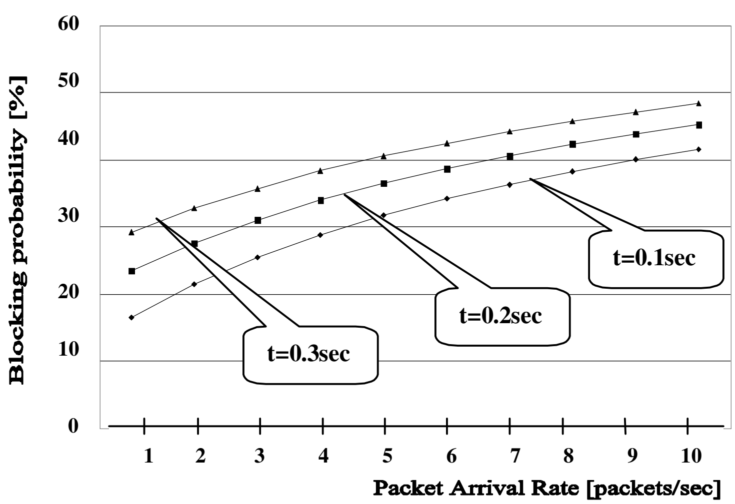

Fig 9: The effect of the Discovery Cycle length on blocking probability

Figures 8 and 9 depict the effect of the Discovery Cycle length. As anticipated, the longer the Discovery Cycle is, the lower is the throughput and the higher is the probability of blocking. However, longer Discovery Cycle does not correspond to proportionally smaller throughput. The blocking probability exhibits similar behavior. The reason is that the Discovery Cycle is responsible for only part of the blocked packets; other packets are blocked due to unavailability of the neighboring node transmitting or receiving from other nodes. This accounts for larger blocking probability, especially at higher loads, that could have been otherwise predicted from the portion of the total time that a node spends in the Discovery Cycle. The results in Figures 8 and 9 suggest that, if kept to a reasonable length, the Discovery Cycle does not carry prohibitively large overhead.

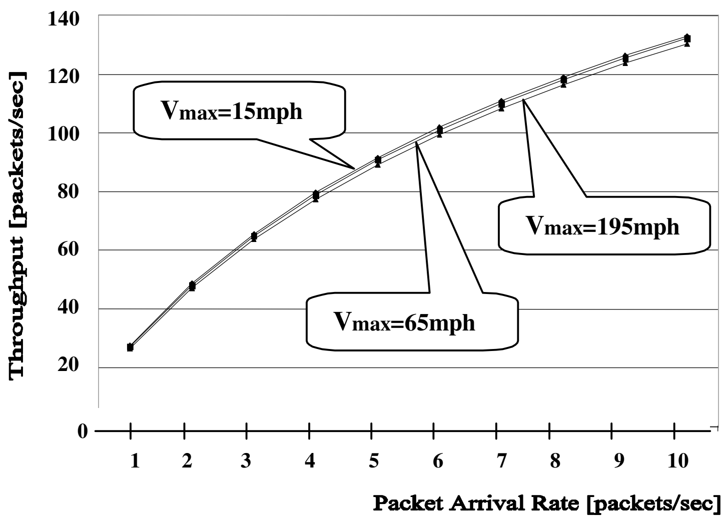

Fig 10: The effect of mobile velocity on throughput

Varying the user mobility (Figures 10 and 11) has only a small effect on the system performance. This can be explained by the fact that as the transmission time of the packets is so short, loosing the link in the middle of a packet transmission is rather a low-probability event. Connections do stay long enough not to affect majority of transmitted packets. Comparing this result with a connection-oriented transport ([1]) provides a strong indication that the preferred mode of operation of the RWNs is in connectionless communication.

Concluding Remarks

We have introduced here a novel MAC scheme, which is based on polling mechanism with local synchronization requirements only. Operation of the scheme relies on partitioning the channels (TDMA or CDMA) into two parts: the poll and the payload portions. The poll portions of the channel use random-access mechanism to perform the polling operation and are, thus, subject to collisions. However, because of the restricted number of neighbors and the short duration of the poll messages, the frequency of collisions is quite small in a practical network scenario. Transmission on the payload portion will not undergo collisions.

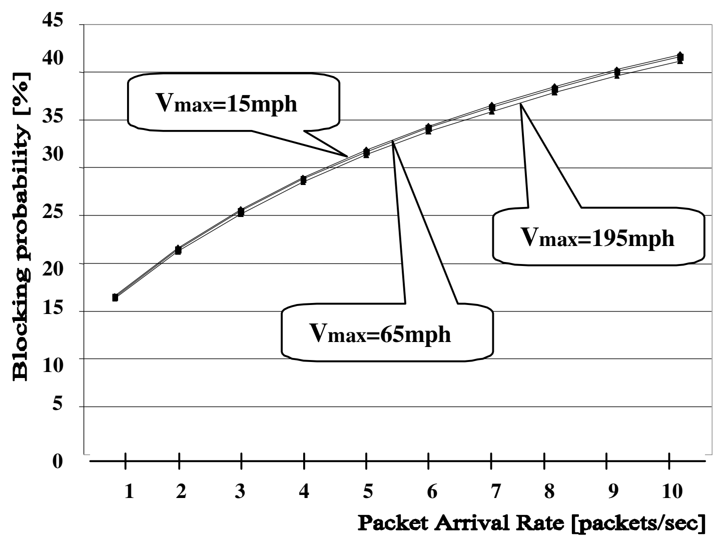

Fig 11: The effect of mobile velocity on blocking probability

Our evaluation of the proposed MAC scheme reveals that, for the set of parameter values considered, its performance in terms of nodal throughout and blocking probability is independent of the mobile population. This is correct as long as some minimal number of nodes are present, so that the probability that a node has no neighbors in small. This behavior translates to a minimum transmission radius, given some mobile density. Note that this conclusion addresses the MAC performance only and not the routing scheme. In fact, in another study, we have shown that the density of user population has a crucial effect on the probability of finding a route within a network [3]. However, from the MAC point of view, as long as there is at least one neighbor to which the packet can be forwarded, the performance of the MAC scheme is relatively invariant with the actual number of such neighbors.

Another conclusion that can be drawn from our study is that the Neighbor Discovery cycle is not a major source of blocking, as long as it is not excessively long. Further study is required to determine the required duration of the Neighbor Discovery cycle, which depends on the number of channels and mobile density.

Finally, we have demonstrated that the mobile's speed has only minor effect on the nodal throughput and blocking probability. This is an encouraging result as it indicates that, under the range of parameters considered, the dropping probability is not strongly affected by the mobility. It also suggests, as we have suspected, that connectionless mode of communication is the proper scheme for the RWN environment.

REFERENCES

[1] Z.J. Haas, "On the Relaying Capability of the Reconfigurable Wireless Networks," *VTC'97,* Phoenix, AZ, May 5-7, 1997.

[2] Z.J. Haas, "A New Routing Protocol for the Reconfigurable Wireless Networks," *ICUPC'97,* San-Diego, CA, Oct. 12-16, 1997.

[3] Z.J. Haas, "Providing Ad-Hoc Connectivity with the Reconfigurable Wireless Networks," in preparation.

[4] P. Karn, "MACA – a New Channel Access Method for Packet Radio," *ARRL/CRRL Amateur Radio 9th Computer Networking Conf.* ARRL, 1990

[5] V. Bharghavan *et al,* "MACAW: A Media Access Protocol for Wireless LANs," *ACM SIGCOMM'94.*

[6] C.L Fullmer and J.J. Garcia-Luna-Aceves, "Floor Equisition Multiple Access (FAMA) for Packet-Radio Networks," *ACM SIGCOMM'95.*

[7] M. Gerla and J.T.-C. Tsai, "Multicluster, Mobile, Multimedia Radio Network," *ACM/Baltzer Journal of Wireless Networks,* vol.1, no.3, 1995.