A Simulation Study of a MAC Layer Protocol for Wireless Networks with Asymmetric Links

Guoqiang Wang, Damla Turgut, Ladislau Bölöni, Yongchang Ji, Dan C. Marinescu
School of Electrical Engineering and Computer Science
University of Central Florida
Orlando, FL 32816
{gwang, turgut, lboloni, yji, dcm}@cs.ucf.edu

ABSTRACT

Asymmetric links are common in wireless networks for a variety of physical, logical, operational, and legal considerations. An asymmetric link supports uni-directional communication between a pair of mobile stations and requires a set of relay stations for the transmission of packets in the other direction. We introduce a MAC layer protocol for wireless networks with Asymmetric links (`AMAC`). The MAC layer protocol requires fewer nodes to maintain silence during a transmission exchange than the protocols proposed in [1, 2]. We present a set of concepts and metrics characterizing the ability of a medium access control protocol to silence nodes which could cause collisions.

Categories and Subject Descriptors: C.2.1 [COMPUTER-COMMUNICATION NETWORKS]: Network Protocols

General Terms: Algorithms

Keywords: Asymmetric link, `AMAC`, Heterogeneous MANET

1. INTRODUCTION

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. The transmission range of a node might be limited by the capabilities of the hardware or by power limitations. A node might need to limit its transmission power to avoid interference with a licensed user of the spectrum, or because of dynamic spectrum management considerations. In military applications, considerations of stealth might require some nodes to reduce their transmission power. In addition to these, [3] mentions some schemes have been proposed recently to maintain optimum network topology by tuning the transmission range of individual nodes [4–6], which leads to possible unidirectional links.

In this paper we introduce a MAC layer protocol for wireless networks with Asymmetric links (`AMAC`). 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 MAC protocol to silence nodes which can cause collisions.

The paper is organized as follows. Related work is presented in Section 2. Section 3 presents `AMAC` protocol in every aspects. Section 4 describes the simulation environment and presents the results of the simulation study with a discussion of the effect of network load and number of nodes. We conclude in Section 5.

2. RELATED WORK

Several potential problems and issues of wireless ad hoc networks with unidirectional links have been addressed in [7] and [8]. One of the important issue is the hidden node problem, which becomes more complicated with the existence of unidirectional links. 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* [9]. According to this definition such a node is hidden from the sender but exposed from the receiver. The hidden node problem can be solved by a `RTS-CTS` handshake mechanism proposed by MACA [10] (`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*. 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 all hidden nodes.

Several solutions to the hidden node problem in a heterogeneous wireless ad hoc network exist. Poojary et al. [1] proposes that a node rebroadcasts a `CTS` packet if it is received from a low-power node. To decrease the probability

IWCMC'06, July 3–6, 2006, Vancouver, British Columbia, Canada.

of collisions, each node waits a random number (1 ... 6) of SIFS (Short Inter-Frame Spacing) periods before transmitting a CTS packet. Fujii et al. [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 the 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 3 is designed to handle these situations as well.

Bao et al. [11] propose a collision-free dynamic channel access scheduling algorithm PANAMA. Two scheduling algorithms are proposed for networks with unidirectional links, NAMA-UN that is node activation oriented and supports broadcast traffic efficiently, and PAMA-UN that is link activation oriented and is more suitable for relaying unicast traffic. The channel access is allocated for NAMA-UN and PAMA-UN alternatively, with each scheduling algorithm lasting for a fixed amount of time. In PANAMA, the sender node is able to detect the hidden node that also attempts to relay traffic to the receiver. The winner of a contention is based on priority values, however, if the link from the hidden node to the receiver is unidirectional, in which case the hidden node may not be aware of the sender, the hidden node always wins the contention. In this way, the hidden node problem involving unidirectional links is solved.

The Sub Routing Layer (SRL) project [12, 13] 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. The SRL implementation also signals the detection of new neighbors and the loss of (unidirectional) links. The place of the SRL in the network stack is analogous to the IMEP protocol in the TORA routing algorithm.

In the following sections, we are going to introduce a new MAC layer protocol for ad hoc networks with Asymmetric links (AMAC). Though we have the intention to design AMAC as the underlying MAC protocol for any routing protocols, AMAC currently works with A^{4}LP [14], a routing protocol for power-constrained networks.

3. MAC PROTOCOL

3.1 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.

Assuming at time t, the distance between two nodes i and j is $d_{ij}(t)$, and the transmission range of node i is $R_i(t)$. Then, the Boolean *reachability function* $\mathcal{R}_{ij}(t)$ is defined as

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

DEFINITION 1. *A set of m nodes $i_1, i_2, \ldots i_m \in \mathcal{N}$ 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. [14]*

DEFINITION 2. *Call V_i the vicinity of node i. V_i includes all nodes that could be reached from node i.*

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

DEFINITION 3. *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.*

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

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 4. *Call $P3_i$ the three-party proxy set coverage of node i. $P3_i$ is the set of nodes reachable either by node i directly, or participate in a three-party proxy set with node i and a third node.*

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

DEFINITION 5. *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 $P3_r$.*

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

DEFINITION 6. *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.*

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

DEFINITION 7. *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 $XH3_{sr}$.*

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

DEFINITION 8. *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.*

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

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 9. *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.*

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

and

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

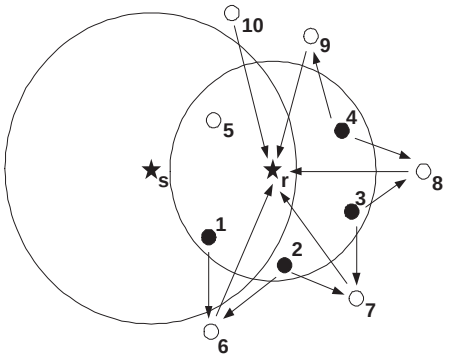


Figure 1: An illustration for topology concepts. The transmission ranges of the sender s and the receiver r are reflected by the circles centered at them. The partial reachability information of other nodes is shown by directed lines.

Figure 1 illustrates the above topology concepts. The transmission ranges of the sender s and the receiver r are reflected by the circles centered at them. The reachability information of other nodes is shown by directed lines. Notice we describe only *partial* reachability information that is necessary for the description of the scenario. In Figure 1, the known three-party proxy sets are {r, 1, 6}, {r, 2, 6}, {r, 2, 7}, {r, 3, 7}, {r, 3, 8}, {r, 4, 8}, and {r, 4, 9}. $V_r = \{1, 2, 3, 4, 5\}$. $H_{sr} = \{2, 3, 4, 6, 7, 8, 9, 10\}$. $P3_r = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. $H3_{sr} = \{2, 3, 4, 6, 7, 8, 9\}$. $XH3_{sr} = \{6, 7, 8, 9\}$. $XHR3_{sr} = \{1, 2, 3, 4\}$. $mXHR3_{sr} = \{2, 4\}$ or $\{1, 3, 4\}$. $MXHR3_{sr} = \{2, 4\}$.

In our current design, the topology information is maintained by the routing protocol A^{4}LP [14].

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

DEFINITION 10. *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 11. *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 12. *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 13. *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

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

3.2 A solution to the hidden node problem

In a heterogeneous ad hoc network with asymmetric links 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* [14].

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

Our solution is to relay `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. Note that our approach does not identify all hidden nodes, but neither methods A or B are able to identify all hidden nodes.

3.3 Node Status

In `IEEE 802.11`, when a node overhears a `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`.

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.

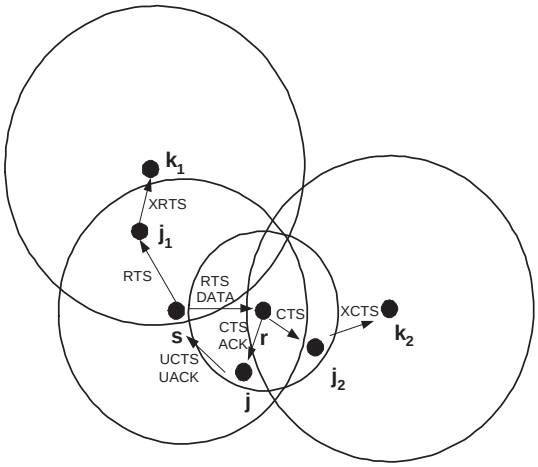


Figure 2: Routing over asymmetric links in a heterogeneous wireless ad hoc network. Node s is the sender, r is the receiver, the link from node s to r is asymmetric, and node j is the proxy node that can relay traffic to s for r. Nodes k_1 and k_2 are hidden nodes for transmissions T_{rs} and T_{sr}, 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.

3.4 Medium Access Model

The medium access model of our protocol is an extended four-way handshake. (see Figure 2) 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 $MXHR3_{rs}$. 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 6 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.

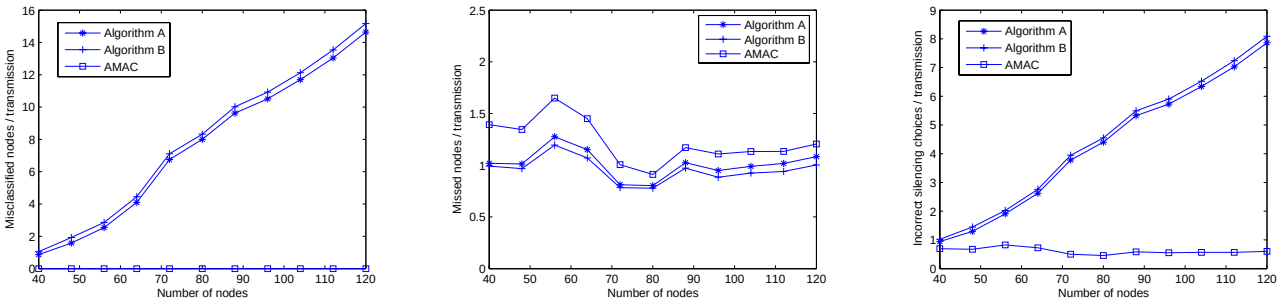
We note that when a node overhears a packet containing new NAV information, it compares the current NAV with the new NAV, and updates it with the NAV that expires later.

4. SIMULATION STUDY

4.1 The accuracy of hidden node classification

A node is *misclassified* as a hidden node if it is silenced by the algorithm mistakenly. Misclassification leads to unnecessary silencing of nodes which could have been transmitting, reducing bandwidth utilization. A node is *missed* by the algorithm if it was not silenced although it should have been. Missed nodes lead to collisions. The better the accuracy of the protocol in classifying the nodes, the better the bandwidth utilization. A useful measure of the global performance of an algorithm is the number of incorrect silencing decisions per transmission - which we define as the sum of the misclassified and missed nodes.

We compare the accuracy of the classification of our proposed AMAC protocol with the accuracy of two well known protocols which are performing the same classification [1,2]. As a note, the basic IEEE 802.11 MAC protocol does not perform any classification of nodes. The simulation environment is an area of 500×500 meters. We populate our environment with a heterogeneous collection of nodes belonging to the four main classes of wireless nodes $C1$, $C2$, $C3$, and $C4$ (see [14, 15]). The transmission ranges are random variables with the mean $100, 75, 50$, and 25 meters, respectively and the standard deviations for each class is 5 meters. The simulation scenarios are created using a set of 40 to 120 nodes including an even number of nodes for each class. The positions of the nodes are uniformly distributed in the area. For each generated scenario, we repeat the experiment 1000



(a) Misclassified nodes (b) Missed nodes (c) Incorrectly classified nodes

Figure 3: (a) The average misclassified nodes / transmission as a function of the number of nodes. The AMAC protocol does not misclassify nodes in a static network. (b) The average missed nodes / transmission for protocols A, B, and our approach, as a function of the number of nodes. (c) The average number of incorrect silencing decisions per transmission for protocols A, B, and our approach.

times. The displacement of nodes are distributed around an initial position and the standard deviation is 20% of its transmission range.

The results of the simulation are shown in Figure 3. The graph (a) shows the number of misclassified nodes per transmission. The AMAC algorithm does not misclassify nodes, because in the process of 3-party proxy set formation, the nodes whose transmission range does not reach the current node are filtered out. However, misclassified nodes can appear with the AMAC protocol if the nodes are highly mobile and the current configuration does not reflect the one detected when the 3-party proxy set was established. The graph (b) shows the missed nodes per transmission. Here the AMAC protocol performs worse than the other two protocols considered, as it is considering only the 3-party proxy sets, and ignores possible higher order proxy sets. However, the number of missed nodes is very small for all the three protocols. Figure 3 shows the number of incorrect silencing decisions per transmission. Here the AMAC protocol emerges with the lowest number of incorrect decisions, as its better performance at misclassification compensates for the lower performance in regards to missed nodes.

4.2 Comparison in realistic scenarios

The main benefit in using a MAC protocol capable of handling asymmetric links is that it can provide the adequate functionality to routing protocols which can take advantage of asymmetric connections. Therefore, the benefits of the MAC protocol can be visualized only if we compare it in a complete routing stack. In this section we present a series of experiments where we compare the pairing of AMAC with A^{4}LP [14] as the upper layer protocol, against two well established protocols pairs: AODV/IEEE 802.11 and OLSR/IEEE 802.11.

We use NS-2 [16,17], an object-oriented event-driven simulator developed at the Lawrence Berkeley National Laboratory, with the CMU wireless extensions [18]. To describe the movement of nodes in the system we use the "random waypoint" model [19]. Each node randomly picks a destination on the map, moves to the destination at a *constant speed*, and then pauses for certain time, the *pause time*. After the pause time, it continues the movement following the same pattern.

In our simulations we use traffic patterns generated by *constant bit rate* (CBR) sources sending UDP packets. Each CBR source is active for a time interval called *CBR duration*. Our simulation allows a *setup time* to allow nodes gather certain routing information before generating any traffic. After the *setup time*, The simulation time is divided into equal time slices, called *switching intervals*. During each switching interval, we generate CBR sources for different pairs of senders and receivers. Table 1 illustrates the default settings and the range of the parameters for our simulation experiments.

Table 1: The default values and the range of the parameters for our simulation studies.

Field	Value	Range
simulation area	$500 \times 500(m^2)$	
num of nodes	8(C1), 16(C2), 24(C3), 32(C4)	30-110
ratio of nodes	C1:C2:C3:C4 = 1:2:3:4	
transmission ranges	200(C1),150(C2), 100(C3),50(C4)(m)	
speed	1 (m/s)	1-10 (m/s)
pause time	15 (s)	
simulation time	200 (s)	
setup time	20 (s)	
switching interval	10 (s)	
num of CBR sources	10	4-40
CBR packet size	64 (bytes)	
CBR sending rate	512 (bps)	
CBR duration	5 (s)	

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.

We are concerned with the impact of node mobility, network load, and network density upon packet loss ratio, and latency. For each randomly generated scenario and traffic patterns, we run simulation experiments covering AODV over IEEE 802.11, OLSR over IEEE 802.11, A^{4}LP using 3-limited forwarding with distance metric (A^{4}LP-M3-F1) over AMAC, and

A4LP using 3-limited forwarding with the metric proposed in [14] (A4LP-M3-F2) over AMAC.

The influence of network load

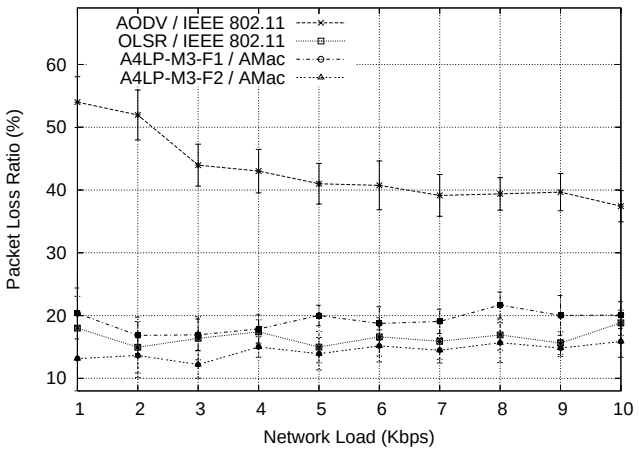


Figure 4: Packet loss ratio vs network load. The ratio of packets lost by AODV/IEEE 802.11 is roughly twice the ratio of packets lost by the other protocols. Among the other protocols, A4LP-M3-F2/AMAC performs best, followed by OLSR/IEEE 802.11, which delivers more packets than A4LP-M3-F1/AMAC for similar scenarios and traffic patterns.

Figure 4 illustrates average latency versus network load. AODV/IEEE 802.11 is the worst. The ratio of packets lost by AODV/IEEE 802.11 is roughly twice the rate of packets lost by the other protocols. The major reason is that flooding, an inefficient broadcast solution, is used in AODV/IEEE 802.11 for finding a route. Among the other protocols, A4LP-M3-F2/AMAC performs best, followed by OLSR/IEEE 802.11, which delivers more packets than A4LP-M3-F1/AMAC for similar scenarios and traffic patterns. OLSR/IEEE 802.11 is able to deliver packets only via symmetric links, thus packets are dropped if at least one asymmetric link is on the *critical* path, however, in which case A4LP/AMAC is able to deliver those packets. The case study in the previous section is the right instance. Our experiment also proves the metric we proposed in [14] (A4LP-M3-F2), a combined metric with distance, power level and class information, is a better metric than the distance only metric (A4LP-M3-F1) in heterogeneous mobile ad hoc networks.

Figure 5 illustrates the average latency versus the network load. The average latency of AODV/IEEE 802.11 is much higher than that of the other protocols. AODV is an reactive protocol which finds routes only when needed. A4LP is a hybrid protocol, routes to non-neighbors are still discovered when needed, however, routes to certain In-, Out-, and InOut-bound neighbors are maintained proactively in a routing table; this fact contributes to the reduction of the average packet delivery latency.

Figure 5 shows that OLSR/IEEE 802.11 has the lowest average packet delivery latency. It is followed by A4LP-M3-F2/AMAC, A4LP-M3-F1/AMAC. The average packet delivery latency is only based on delivered packets. OLSR/IEEE 802.11 drops more packets than A4LP-M3-F2/AMAC; these are the packets

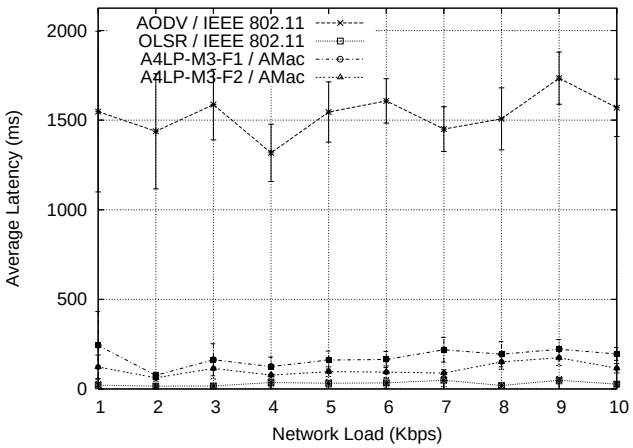


Figure 5: Average latency vs network load. The average latency of AODV/IEEE 802.11 is much higher than the other protocols. Among the other protocols, OLSR/IEEE 802.11 delivers packets with the shortest latency. However, the results cannot prove that OLSR/IEEE 802.11 has a better performance than A4LP-M3-F2/AMAC.

which require a protocol able to deal with asymmetric links. The packets that could be delivered by A4LP-M3-F2/AMAC but not by OLSR/IEEE 802.11 generally have higher latency, and this explains why the average packet delivery latency of A4LP-M3-F2/AMAC is higher than that of OLSR/IEEE 802.11.

The influence of number of nodes

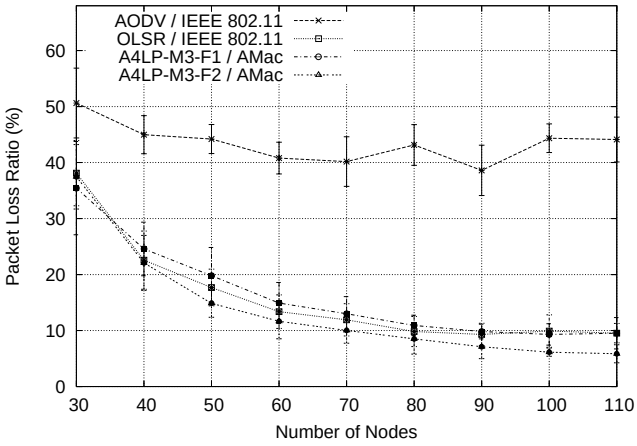


Figure 6: Packet loss ratio vs number of nodes. A4LP-M3-F2/AMAC delivers most packets, followed by OLSR/IEEE 802.11, A4LP-M3-F1/AMAC and AODV/IEEE 802.11 for similar scenarios and traffic patterns. The packet loss ratio decreases when the number of nodes increases.

Figure 6 illustrates the average latency versus the number of nodes. For similar scenarios and traffic patterns, A4LP-M3-F2/AMAC delivers most packets, followed by OLSR/

IEEE 802.11, A^{4}LP-M3-F1/AMAC, and AODV/IEEE 802.11. As the number of nodes in the network increases, the network connectivity increases as well, thus the packet loss ratio decreases. Figure 6 shows that the packet loss ratio decreases from roughly 40% to about 10% as the number of nodes increases from 30 to 110.

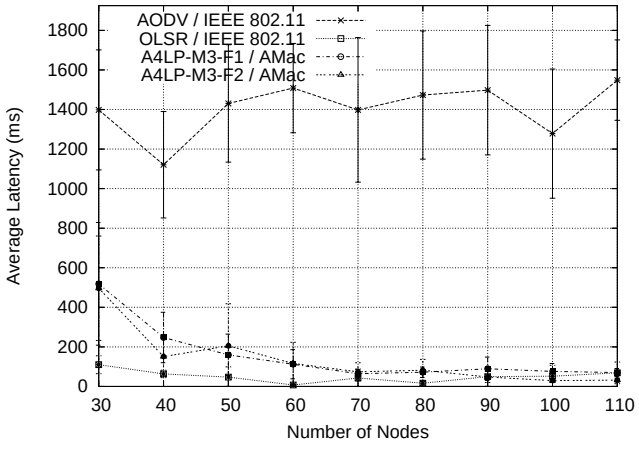


Figure 7: Average latency vs number of nodes. The average latency of AODV/IEEE 802.11 is much higher than the other protocols. The packet latency tends to decrease as the number of nodes increases for A^{4}LP/AMAC and OLSR/IEEE 802.11.

Figure 7 shows the average packet delivery latency versus the number of nodes. The average latency of AODV/IEEE 802.11 is much higher than the other protocols. For A^{4}LP/AMAC and OLSR/IEEE 802.11 the packet latency tends to decrease as the number of nodes increases. As the number of nodes in the network increases, more neighbors and routes are found during the neighbor information exchange process, thus the packet delivery latency decreases.

5. CONCLUSIONS

In this paper, we argue that asymmetry of the transmission range in wireless networks is a reality and should be treated as such. We proposed a MAC layer protocol, AMAC, 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". IEEE 802.11 assumes symmetric links between each pair of nodes while AMAC does not. For traffic over unidirectional links, AMAC relies on a proxy node in three-party proxy set to relay acknowledgements back to the sender so that the reliability is assured. Our MAC protocol reduces average packet loss ratio and average latency as asymmetric links are comprehensively utilized which dominate routing in heterogeneous ad hoc networks.

Our future work is dedicated to remove the dependency of AMAC from A^{4}LP, and provide transparent interface to routing protocols so that it could be the underlying MAC protocol for any routing protocol in heterogeneous wireless ad hoc networks.

Acknowledgment

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

6. 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] S. Kumar, V. S. Raghavan, and J. Deng, "Medium access control protocols for ad hoc wireless networks:a survey," *Ad Hoc Networks Journal, Elsevier*, vol. 4, pp. 326–358, 2006.

[4] R. Ramanathan and R. Hain, "Topology control of multihop wireless networks using transmit power adjustment," in *Proceedings of INFOCOM*, 2000, pp. 404–413.

[5] R. Wattenhofer, L. Li, P. Bahl, and Y.-M. Wang, "Distributed topology control for wireless multihop ad-hoc networks," in *Proceedings of INFOCOM*, 2001, pp. 1388–1397.

[6] P. C. Gurumohan, T. J. Taylor, and V. R. Syrotiuk, "Topology control for manets," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC'04)*, 2004, pp. 600–604.

[7] R. Prakash, "Unidirectional links prove costly in wireless ad-hoc networks," in *Proc. of DIMACS Workshop on Mobile Networks and Computers*, 1999, pp. 15–22.

[8] S. Agarwal, "Handling unidirectional links in ad-hoc wireless networks," University of California, Berkeley, Tech. Rep., December 2000.

[9] V. Bharghavan, "A New Protocol for Medium Access in Wireless Packet Networks," Urbana, IL: Timely Group, Tech. Rep., 1997.

[10] P. Karn, "MACA - a new channel access method for packet radio," in *Proceedings of the 9th ARRL Computer Networking Conference*, 1990, pp. 134–140.

[11] L. Bao and J. Garcia-Luna-Aceves, "Channel access scheduling in ad hoc networks with unidirectional links," in *Proceedings of Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIALM)*, 2001, pp. 9–18.

[12] V. Ramasubramanian and D. Mosseé, "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.

[13] 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.

[14] 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.

[15] 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.

[16] 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," vol. 33, no. 5, pp. 59–67, 2000.

[17] "VINT project. the ucb/lbnl/vint network simulator-ns (version 2)," URL http://www.isi.edu/nsnam/ns.

[18] "CMU Monarch extensions to ns," URL http://www.monarch.cs.cmu.edu.

[19] 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.