EUDA: Detecting and Avoiding Unidirectional Links in Ad Hoc Networks*

Jun-Beom Lee[a] **Young-Bae Ko**[a] **Sung-Ju Lee**[b]

jblee@dmc.ajou.ac.kr *youngko@ajou.ac.kr* *sjlee@hpl.hp.com*

[a] Graduate School of Information & Communication, Ajou University, Suwon, Korea

[b] Mobile & Media Systems Lab, Hewlett-Packard Labs, Palo Alto, CA, USA

I. Introduction

Although there has been a great amount of research work in ad hoc networks, most of the research assumes the nodes are homogeneous. All the nodes are assumed to have the same or similar radio propagation range, processing capability, battery power, storage, and so forth. In reality however, nodes in ad hoc networks tend to have heterogeneity. In the military scenarios for instance, the troop leader is usually equipped with more powerful networking devices than the soldiers of the troop. Radios installed in the vehicles such as tanks and jeeps have more capabilities than radios the soldiers carry, as vehicles do not have the same size- or power-constraints as the soldiers.

The heterogeneity of the ad hoc network nodes creates challenges to current MAC and routing protocols. Many MAC protocols use the RTS/CTS handshake to resolve channel contention for unicast packets. The assumption here is that when node A can deliver RTS to node B, node A will also be able to receive CTS from node B. Routing protocols in ad hoc networks typically assume bidirectional, symmetric routes, which do not always hold true when node heterogeneity is introduced. The performance of these protocols may degrade in networks with heterogeneous nodes [6].

One of the major challenges in ad hoc networks with heterogeneous nodes is the existence of *unidirectional links*. Medium access control and routing performance suffers from the existence of unidirectional links and routes. Unidirectional links may exist for various reasons in ad hoc networks. Different radios may have different propagation range, and hence unidirectional links may exist between two nodes with different type of equipments. IEEE 802.11b uses different transmission rates for broadcast and unicast packets. That creates gray zones [1] where nodes within that zone receive broadcast packets from a certain source but not unicast packets. The hidden terminal problem can also result in unidirectional links. Moreover, interference, fading, and other wireless channel problems can affect the communication reachability of the nodes. Some recent proposals have nodes adjust the radio transmission range for the purpose of energy-aware routing and topology control. The nodes in these schemes transmit packets with the radio power just strong enough to reach their neighbors. When nodes move out of that range, the link turns into unidirectional, when in fact it could be bidirectional when each node sends packets with the maximum transmission range.

*This work was in part supported by grant No. R05-2003-000-10607-02004 from Korea Science & Engineering Foundation, and University IT Research Center project.

We focus on the routing protocol design in the face of heterogeneity of node transmission power and unidirectional links resulting from it. We propose a routing technique EUDA (Early Unidirectionality Detection and Avoidance) that proactively detects unidirectional links and avoids constructing routes that include such links. We introduce two approaches: (i) a network-layer solution that utilizes node location information and (ii) a cross-layer solution based on a path-loss model.

II. Ad hoc Routing with Early Unidirectionality Detection and Avoidance

In EUDA (Early Unidirectionality Detection and Avoidance), a node detects a unidirectional link *immediately* when it receives a RREQ packet. This early detection is different from existing schemes such as AODV with blacklisting that detect unidirectional links much later when RREP packet is propagated through the reverse route. Our basic idea is that, when node X receives a RREQ from node Y, node X compares its transmission range using the highest power level to an estimated distance between them. If the value of estimated distance from node X to Y is larger than the transmission range of node X, node X considers its link to Y as a unidirectional link, resulting in RREQ packet drop without any further forwarding. Only when a transmission range of node X is equal to or larger than its estimated distance towards node Y, RREQs from Y will be processed. In EUDA, all nodes receiving RREQ packet are required to decide whether to forward it or not. This decision is based on the comparison of transmission range with distance between the nodes.

Let us investigate how existing, popular ad hoc on-demand routing protocols function in the presence of unidirectional links. AODV [5] for example assumes that all links between neighboring nodes are symmetric (i.e., bidirectional links). As an example in Figure 1, a RREQ packet generated by a source node S traverses the path $< S - A - B - C - D >$ until it arrives at a destination node D. Each circle in the figure represents the node transmission range. When node D receives the RREQ, it sends a RREP back to node S via the reverse path. Note that however, the RREP is not able to reach from node C to node B because node B is not located within node C's transmission range. As a result of a RREP delivery failure by node C, the source S cannot receive the corresponding RREP packet and hence it experiences a route discovery failure in its first trial. Such a failure will repeatedly cause

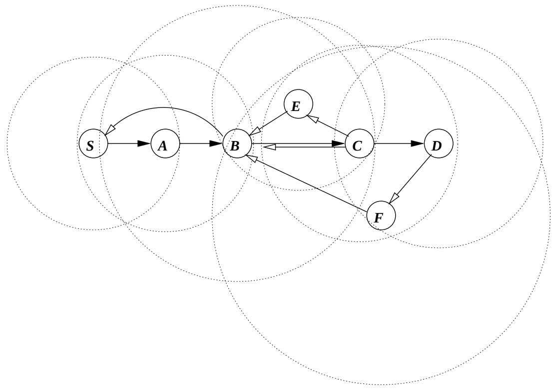

Figure 1: Example topology.

route discovery processes with no benefit. Although there exists a route that does not include any unidirectional link, $< S-A-B-E-C-D >$, this route cannot be found as the shortest hop is one of the main route selection criteria in AODV. We refer to this scheme as the "Basic-AODV."

In the latest AODV specification [4, 2], some mechanisms are newly added to handle the problem of unidirectional links. One way to detect unidirectional links is to have each node periodically exchange *hello* messages that include neighboring information. This scheme however, requires large messaging overhead. Another solution is *blacklisting*. Whenever a node detects a unidirectional link to its neighbor, it blacklists that neighbor from which a link is unidirectional. Later when the node receives a RREQ from one of the nodes in its blacklist set, it discards the RREQ to avoid forming a reverse path with a unidirectional link. Each node maintains a blacklist and the entries in the blacklist are not source-specific. In order to detect a unidirectional link a node sets the "Acknowledgment Required" bit in a RREP when it transmits the RREP to its next hop. On receiving this RREP with the set flag, the next hop neighbor returns an acknowledgment (also known as RREP-ACK) to the sending node to inform that the RREP was received successfully. In the case when RREP-ACK is not returned, the node puts its next hop node on its *blacklist* so that future RREQ packets received from those suspected nodes are discarded. We refer to this version of AODV as the "AODV-BL (Blacklist)" scheme.

Again, let's use Figure 1 to illustrate the AODV-BL scheme. Here, node C cannot be acknowledged by node B when delivering RREP and therefore it will put node B in its blacklist set. Later when node S re-broadcasts a new RREQ packet, node C will ignore this RREQ received from B but forward another copy of the RREQ from node E. Finally, a destination node D will receive the RREQ through a longer route at this time. Node D returns a RREP back to the source S via a reverse path; in this case, the reverse path is $< D-C-E-B-A-S >$, having no unidirectional links.

The AODV-BL scheme may be efficient when there are few unidirectional links. However, as the number of asymmetric links increase, its routing overhead is likely to become larger since a source node will always suffer from a failure in its first trial of route discovery and need to flood RREQ messages more than once to find a route with all bidirectional links. It also results in an increase of route acquisition delay.

Using the same example, let us see how EUDA operates. When node C receives a RREQ from node B, it detects a unidirectional link immediately using the proposed scheme and discards the packet. Later, node C may receive another RREQ from node E. Node C this time will forward this RREQ as it came through a bi-directional link. Finally, the destination D receives the first RREQ via nodes E and C, forming the reverse path $< D-C-E-B-A-S >$ and replying its RREP through this path. Eventually, node S obtains a path having only the bidirectional links. Note that in EUDA, this successful route discovery is achieved from the first attempt by the source, as long as there is at least one bidirectional route from a source to a destination.

The next question is how to calculate an estimated distance between two communicating nodes, so that it can be compared with the radio transmission range to determine whether the link between two nodes are bidirectional or unidirectional. This can be done in two different ways as described below.

(i) *Network Layer Solution with Location Information*: Suppose that the nodes know their geographical position. A transmitter node X includes its own location information in RREQ to be broadcasted. When a node receives a RREQ from X, it calculates the estimated distance (*d*) based on its own physical location. This method can be useful and is easy to implement, but requires information of physical location of the participating nodes.

(ii) *Cross Layer Solution with Path Loss Model*: As an alternative, we can utilize a wireless channel propagation model, i.e., the two-ray ground path loss model that is designed to predict the mean signal strength for an arbitrary transmitter-receiver separation distance. In wireless networks, if we know the transmitted signal power (P_t) at the transmitter and a separation distance (*d*) of the receiver, the received power (P_r) of each packet is given by the following equation:

$$P_r = \frac{P_t * G_t * G_r * (h_t^2 * h_r^2)}{d^4 * L} \tag{1}$$

where G_t is transmitter antenna gain, G_r is receiver antenna gain, h_t is transmitter antenna height, h_r is receiver antenna height, and L is a system loss factor. Now we can derive the following equation from Eq. (1) to compute the distance:

$$d = \sqrt[4]{\frac{P_t * G_t * G_r * (h_t^2 * h_r^2)}{P_r * L}} \tag{2}$$

Eq. (2) states that the distance between two communicating nodes can be estimated at a receiver side, if the transmitted power level P_t of the packet transmitter and the power received at the receiver P_r are known.

To implement this method, the transmitter should make the transmitted power information available to the receiver, by putting the power information on a RREQ packet.

One assumption behind the unidirectionality detection methods presented above is that any node's communication range is constant when it transmits with its maximum power P_{max}. Recall that this theoretically maximum transmission range is compared with the estimated distance between the two nodes to detect unidirectional links. In reality however, there may be some attenuation of the transmitter power over distance. Therefore, one would argue that such an assumption is unrealistic because transmission range of the RREQ receiver (thus, a potential RREP forwarder) can vary due to several negative environmental factors such as obstacles, reflections, fading, etc.

To take this argument into account, we modify the proposed distance estimation based comparison method so that unidirectional link detection is made with more realistic parameters of the channel gain, the receiver sensitivity, and the receiver's signal-to-noise ratio.

Let us assume that there are two nodes *i* and *j*. When node *j* receives a RREQ from node *i*, it measures the received signal power, $P_r(j)$. The channel gain, G_{ij}, is computed as the received power ($P_r(j)$) at node *j* over the transmitted power ($P_t(i)$) at node *i* (see Eq. (3) below):

$$G_{ij} = \frac{P_r(j)}{P_t(i)} \tag{3}$$

We assume that the sender power $P_t(i)$ is advertised in the RREQ packet. We also assume that the channel gain G_{ij} between two nodes *i* and *j* is approximately the same in both directions— note that the same assumption was also made in [3]. Given the transmitter/receiver power information and the channel propagation characteristics, the received power at node *i* must at least be equal to its minimum receiving threshold RX_Thresh_i, in order for node *i* to receive any packet successfully from node *j* with the transmission power $P_t(j)$.

$$P_r(i) = G_{ij} * P_t(j) \geq RX\_Thresh_i \tag{4}$$

This implies that if node *j* transmits at the maximum power $P_t(max)$ (i.e., replacing $P_t(j)$) satisfies Eq. (4), it can successfully deliver packets to node *i*. Observe that the value of RX_Thresh_i is related to the receiving sensitivity at node *i*.

We now define one additional equation such that the observed signal-to-noise ratio SNR_i for the transmission at node *i* must at least be equal to its minimum SNR_Thresh_i (representing the channel status observed at node *i*):

$$SNR_i = \frac{G_{ij} * P_t(j)}{P_n(i)} \geq SNR\_Thresh_i \tag{5}$$

where $P_n(i)$ is the total noise node *i* observes on the channel. Again, this implies that node *j* can successfully transmit to *i* when *j* with its maximum transmission power satisfies Eq. (5).

To summarize, if the above two equations (Eqs. (4) and (5)) are satisfied when one node receives a RREQ from another node, these two nodes are considered to be able to communicate directly with each other and hence have a bidirectional link. Otherwise, it can be concluded that there is a unidirectional link between them. With this modification, we have our scheme work better in more realistic scenarios, with its improved estimation accuracy. Nevertheless, there is a clear tradeoff between accuracy and complexity in estimation. Furthermore, the RREQ packet size needs to be increased to include additional information. The transmitter node *i* of a RREQ packet is now required to include more information (i.e., its transmitted power $P_t(i)$, observed total noise $P_n(i)$, minimum received power threshold RX_Thresh_i, and minimum signal-to-interference ratio SNR_Thresh_i) on the RREQ packet.

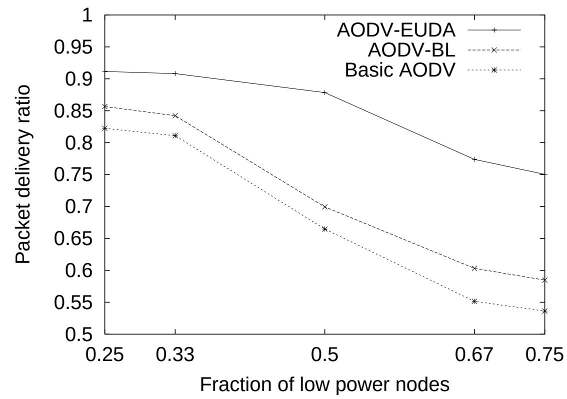

Figure 2: Packet delivery ratio.

III. Performance Evaluation

We have performed ns-2 simulations for performance evaluation. We apply the EUDA framework to AODV to simulate AODV-EUDA and compare it with the Basic-AODV without any unidirectional link detection and AODV with Black Listing (AODV-BL) protocol [2].

Figure 2 presents the *packet delivery ratio* of the three schemes as we vary the fraction of low power nodes (transmisstion range is 125 m for low power nodes and 250 m for high power nodes). There are 10 CBR connections and nodes move following the random waypoint model with zero pause time and 20 m/s maximum speed. As the fraction of low power nodes increases, the packet delivery ratio decreases for all protocols. We can see that the drop in packet delivery ratio is much less drastic and the success delivery rate is consistently higher for AODV-EUDA compared with the other two AODV schemes. This improvement of AODV-EUDA is due to efficient and fast detection of unidirectional links. With AODV-EUDA, a route search failure will not occur even when there is unidirectional path from a source to a destination. The Basic-AODV performs poorly in most cases as it does not take notice of unidirectional links and repeatedly performs route re-discoveries. As for AODV-BL, although it detects unidirectional links, it only does so after a delivery failure and hence requires another route discovery process. AODV-

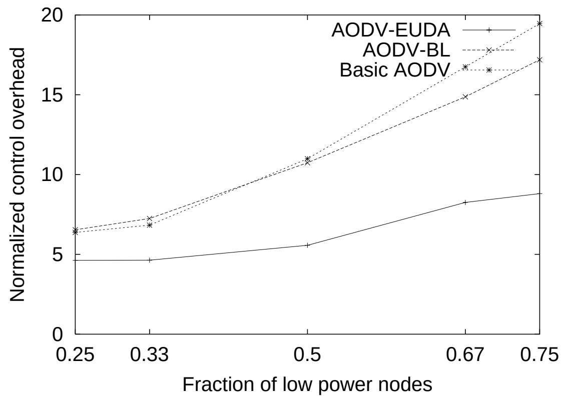

Figure 3: Normalized control overhead.

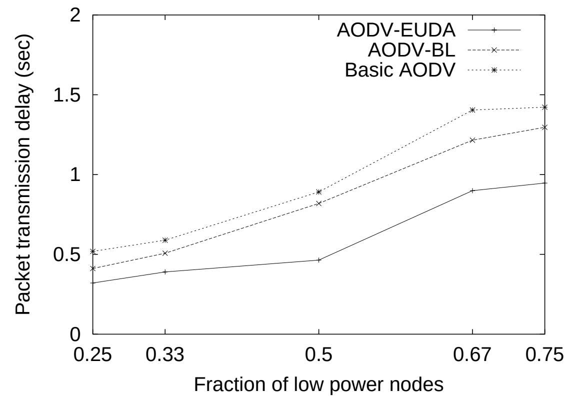

Figure 4: End-to-end delay.

EUDA on the other hand, finds unidirectional links during the RREQ propagation phase and avoids including them in the route in the first route discovery attempt.

Figure 3 shows the *normalized routing overhead* with varying fraction of low power nodes. We define the normalized routing overhead as the ratio between the total number of routing control packets *transmitted* by all nodes and the total number of data packets *received* by the destinations. Overall, AODV-EUDA has the lowest overhead compared with AODV-BL and the Basic-AODV. AODV-BL and the basic AODV perform excessive flooding as they can neither detect unidirectional links or detect them in a timely fashion. Such an excessive flooding clearly contributes to a larger routing overhead. AODV-EUDA shows better efficiency because of its unique ability of early detection and avoidance of unidirectional links.

In Figure 4, we report the *average end-to-end delay* of successfully delivered data packets. The end-to-end delay is measured for the time from when a source generates a data packet to when a destination receives it. Therefore, this value includes all possible delay such as a buffering delay during route discovery, queuing and MAC delay during packet transmission, and propagation delay. The result again shows that AODV-EUDA yields a significantly better performance (i.e., smaller end-to-end latency) than other protocols for both cases of two different maximum node speeds. This shows that AODV-EUDA effectively overcomes unidirectional links. By exploring the early unidirectionality detection and avoidance feature, AODV-EUDA is able to shorten the route discovery latency and hence the overall end-to-end delay. Note that route (re)discovery latency may dominate the total end-to-end delay. For this reason, the Basic-AODV and AODV-BL consistently showed poor delay performance. When any shortest path includes a unidirectional link, the sources running the Basic-AODV experience significant amount of route discovery delay as they cannot receive corresponding RREP packets until such unidirectional links disappear by some network topology change. AODV-BL also shows a poor delay performance compared with AODV-EUDA because it produces more number of RREQ packets to find bidirectional routes.

References

[1] H. Lundgren, E. Nordstrom, and C. Tschudin, "Coping with communication gray zones in ieee 802.11b based ad hoc networks," in *Proc. of ACM WoWMoM*, Atlanta, GA, Sept. 2002, pp. 49–55.

[2] M. K. Marina and S. R. Das, "Routing performance in the presence of unidirectional links in multihop wireless networks)," in *Proc. of ACM MobiHoc*, Lausanne, Switzerland, June 2002, pp. 12–23.

[3] J. Monks, V. Bharghavan, and W.-M. Hwu, "A power controlled multiple access protocol for wireless packet networks," in *Proc. of IEEE INFOCOM*, Anchorage, AK, Mar. 2001.

[4] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," IETF, RFC 3561, July 2003.

[5] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. of IEEE WMCSA*, New Orleans, LA, Feb. 1999, pp. 90–100.

[6] N. Poojary, S. V. Krishnamurthy, and S. Dao, "Medium access control in a network of ad hoc mobile nodes with heterogeneous power capabilities," in *Proc. of IEEE ICC*, Helsinki, Finland, June 2001.