A study on Advanced Load-Balanced Ad hoc Routing Protocol

Joo-Yeon Lee*, Cheong-Jae Lee*,
Yong-Woo Kim*, Joo-Seok Song*
*Dept of Computer Science, Yon-sei University
e-mail : justair@emerald.yonsei.ac.kr

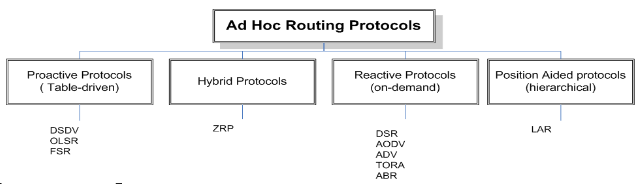
Abstract

The ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure of centralized administration. Load-Balanced Ad hoc Routing(LBAR) protocol is an on-demand routing protocol intended for delay-sensitive applications where users are most concern with packet transmission delay. Although LBAR mechanism is a novel load balancing routing protocol for ad hoc network, it has own limitation in route path maintenance phase. Therefore, in this paper, we propose Advanced Load-Balanced Ad hoc Routing(A-LBAR) that is delay-sensitive and has an efficient path maintenance scheme. The robust path maintenance scheme is maintained by considering about nodal loads all over network and misbehavior of overloaded or selfish nodes. The proposed scheme provides good performance over DSR and AODV in terms of packet delay and packet loss rate when some misbehaving nodes exist in the network.

1. Introduction

In recent years, an increasing interest has been given to an mobile ad hoc network(MANET) due to the proliferation of inexpensive, widely available wireless devices. The ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure of centralized administration. The numerous protocols have been developed for ad hoc mobile networks. As shown in [Figure 1.1], these routing protocols only dealing with unicast routing techniques may generally be categorized as proactive protocols, reactive protocols, hybrid protocols, position aided protocols. Characteristic of each protocol is introduced in [1] in detail. All of the ad hoc routing protocols must deal with the typical limitations of these networks, which include high power consumption, low bandwidth, and high error rates. Also there are a lot of misbehaves by overloaded, selfish, broken and so on. In fact, a major drawback of all existing ad hoc routing protocols is that they do not have provisions for conveying the load and/or quality of a path during route setup. Hence they cannot balance the load on the different routes efficiently. Hassanein et al.[2] introduced Load-Balanced Ad hoc Routing(LBAR) protocol that is an on-demand routing protocol intended for delay-sensitive applications where users are most concern with packet transmission delay. However, it has own limitation in route path maintenance phase.

In this paper, we propose Advanced Load-Balanced Ad hoc Routing(A-LBAR) that is delay-sensitive and has an efficient path maintenance scheme. The robust path maintenance scheme is maintained by considering about nodal loads all over network and misbehavior of overloaded or selfish nodes. The proposed scheme provides good performance over DSR and AODV [1] in terms of packet delay and packet loss rate when some misbehaving nodes exist in the network.



[Figure 1.1] Categorization of Ad Hoc Routing Protocols

The paper is organized as the follows. In

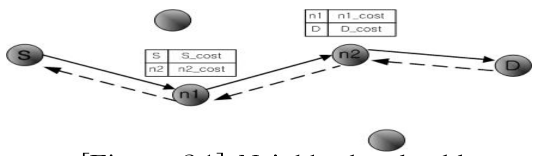
Section 2, the overview and its own limitation of LBAR scheme are described. The details of the proposed A-LBAR scheme are described in Section 3. Finally, Section 4 presents conclusion and future work.

2. Load Balanced Ad hoc Routing Protocol

In this Section 2, the overview and its own limitation of LBAR scheme are presented. After introducing route discovery and path maintenance phase of LBAR briefly, we present its own problems in path maintenance phase.

2.1 Route discovery

The process is divided into two stages: forward and backward. The forward stage starts at the source node by broadcasting setup messages to its neighbors. [Figure 2.1] presents Neighborhood table containing ID and activity of its own and neighbor. Nodes learn about their neighbors in one of two ways: whenever a node receives a broadcast from a neighbor, it updates its local connectivity information in its Neighborhood table. And in the event that a node has not sent data packets to any of its active neighbors within a predefined timeout, hello_interval, it broadcasts a hello message to its neighbors, containing its ID and activity.



[Figure 2.1] Neighborhood table

A setup message carries the cost seen from the source to the current node. The destination node collects arriving setup messages within a route-select waiting period, which is a predefined timer for selecting the best-cost path. The backward stage begins with an ACK message forwarded backward towards the source node along the selected path, which we call the active path. When the source node receives an ACK message, it knows that a path has been established to the destination and then starts transmission.

2.2 Path maintenance

When either the destination or some intermediate node moves outside the active path, it will be initiated to correct the broken path. Once the next hop becomes unreachable, the node upstream of the broken hop propagates an error message to the destination node. Upon receiving notification of a broken link, the destination node picks up an alternative best-cost partial route passing through the node propagating the error message and then sends an ACK message to the initiator of the error message. If the destination has no alternative path passing through the node sending the error message, the destination picks up another route and sends an ACK message to the source. By then, a new active path is defined.

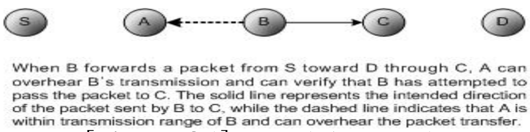
2.3 Limitation of LBAR Mechanism

LBAR has its own limitation such as those stated in the following. First, it only routes data packets circumventing congested paths in the network, not considering about the traffic sent to a misbehaving node that agrees to participate in forwarding packets (it appends its address into setup packets) but then indiscriminately drops all data packets that are routed through it. Finally, the throughput is not improved when some selfish nodes exist in the network. Second, load balancing is not accomplished all over network because it just considers about nodal loads in route discovery. After deciding the path, it does not consider nodal loads in data forwarding. Then as a result, some packet losses by overloaded nodes happen. Third, some time after data forwarding, the alternative paths which are stored at destination could be useless since it does not reflect current network topology accurately. In such a case, unnecessary spaces and ACK control generate overhead for alternative paths. Therefore, we propose Advance Load-Balanced Ad hoc Routing(A-LBAR) protocol that has robust path maintenance method.

3. Advanced Load-Balanced Ad hoc Routing Protocol

The proposed A-LBAR provides robust path maintenance mechanism over LBAR. Hence, A-LBAR focuses on how to manage path maintenance efficiently.

Marti et al.[3] introduced the watchdog tool for detecting and mitigating routing misbehavior assuming the network interface that has the promiscuous mode and Dynamic Source Routing protocol as the routing protocol. [Figure 3.1] illustrates how the watchdog works. In this paper, we apply watchdog for detecting misbehaving node assuming the network interface that has the promiscuous mode and our A-LBAR protocol as the routing protocol.



[Figure 3.1] Watchdog works

Through watchdog, in data forwarding we can detect and circumvent misbehaving node, then we can prevent decrease of throughput by such a selfish node. In addition, we assume wireless interfaces that support promiscuous mode operation. Promiscuous mode means that if a node A is within range of a node B, it can overhear communications to and from B even if those communications do not directly involve A. Lucent Technologies' WaveLAN interfaces have this capability. While promiscuous mode is not appropriate for all mobile ad hoc network scenarios(particularly some military scenarios) it is useful in other scenarios for improving routing protocol performance[4]. As using promiscuous mode in our scheme, the extra overhead in overhearing communication of neighbor is not caused. Although ALARM packet for notifying source node of selfish node is caused, we can prevent decrease of throughput caused by selfish nodes efficiently through it.

Also, for robust path maintenance we define new ALARM packet in our scheme. ALARM packet is expended error packet of DSR [5]. The ALARM packet happens in three case; broken link, selfish node or overloaded node is detected. It carries each information of them, so the source node can know three case of route recovery and recover each of them.

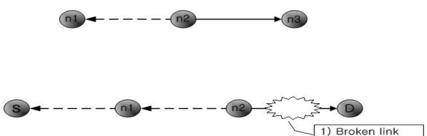
3.1 Route discovery

When route discovery phase, if destination gets many route request messages, destination choose two of them in order of best-cost paths. Then, the destination propagates a route reply message backward towards the source node along the best-cost path, which we call the active path. Up to this time, we also carry the remainder of paths into the route reply message together, which we call this as the alternative path for storing in source node. We delete an alternative path if the waiting period which is a predefined timer for verifying the validity of an alternative path is expired. If a link on the selected path breaks, the route reply message is discarded and the source node could not receive route reply message within a route-discovery waiting period, which is a predefined timer for getting the active path. Then, the source node restart route discovery. When the source node receives route reply message, it knows that a best-cost path has been established to the destination and then starts transmission.

3.2 Advanced path maintenance

The proposed scheme provides advanced path maintenance scheme by using watchdog and new ALARM packet. Following paragraphs, we will describe our advanced route recovery scheme in detail. Route recovery happens in three cases and [Figure 3.2] illustrates these cases.

First, ALARM packet is triggered when a broken link occurs or a selfish node is detected by a watchdog denoted by case 1) or 2) in [Figure 3.2]. We describe the case of 1) in detail. Because the case of 2) is same, so if a selfish node is detected, the recovery scheme of broken link can be built alike. When there is a broken link caused by a nodal mobility in data forwarding, the upstream node of broken link sends ALARM packet to the source node. If the source node which receives ALARM packet happens to have a detour path which can bypass the broken link, then the source node chooses this alternative path and transmits data through the chosen path. Otherwise, the source node starts route discovery. If the selected alternative path does not forward data accurately, it implies that the alternative path does not reflect current network topology. Therefore the source node starts route discovery and finds new path at this time. Of course when there is a damage in the alternative path, the unnecessary data forwarding and control can generate overhead. However, such case does not happen frequently in our scheme. Since in our scheme, we delete alternative path if the waiting period which is a predefined timer for verifying the validity of an alternative path is expired. By putting this bound time in data forwarding, we can decide the validity of an alternative path to a certain degree. This assumption is believable since right after starting data forwarding the possibility of an alternative path reflecting current network topology is sufficiently high. Therefore, we can convince that the alternative path is correct and the case of damage in the alternative is rare.



[Figure 3.2] Recovery cases

Next, ALARM packet happens when an overloaded node occurs as shown in case 3) in [Figure 3.2]. After deciding path, more nodal loads are increased when more source traffics are generated while forwarding data. In such a case, many nodes participate in active path and some nodes drop data packets immediately because of its buffer overflow. In our scheme, in such a case, the upstream node which does not receive ACK message from an overloaded node sends ALARM packet to the source node to indicate this type of situation. The source node which receives ALARM packet retransmits dropped packets at a later time.

4. Conclusion

In this paper, we proposed Advanced Load-Balanced Ad hoc Routing(A-LBAR) that is delay-sensitive and has an efficient path maintenance scheme. The robust path maintenance scheme is maintained by considering about nodal loads all over network and misbehavior of overloaded or selfish nodes. The route recovery in our scheme will be initiated and helpful when the nodal load is overloaded or a selfish node exists in the network, including the situation when the broken link occurs. Therefore, A-LBAR provides good performance over DSR and AODV in terms of packet delay and packet loss rate when some misbehaving nodes exist in the network. A comprehensive simulation study will be conducted to evaluate the performance of A-LBAR in the future.

Reference

[1] Roberto Beraldi and Roberto Baldoni, "7.3 Unicast Routing Techniques for Mobile Ad Hoc Networks," The handbook of Ad Hoc Wireless Networks, CRC PRESS

[2] A. Zhou and H. Hassanein, "Load Balancing Wireless Ad hoc Networks," IEEE Electric and Computer Engineering 2001, vol.2, pp1157-1161, May 2001.

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *Proc. ACM MOBICOM '00*, Boston, Massachusetts, Aug. 2000, pp. 255-265.

[4] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks," *Ad Hoc Networking*, edited by C. E. Perkins, Addison-Wesley, 2001.

[5] David B.Johnson, David A.Maltz, Yih-Chun Hu," http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt," internet draft, 15 April 2003