International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 4, April - 2013

Detecting and Recovering Link-Failure in Ad-hoc Network Using Signal Stability-Oriented Routing Protocol

Ashok. P[1] Satheesh P. S [2] Karthikeyan. J [2]

[1, 2] *PG Scholar (Computer Science and Engineering)*
Karthikeyan. J, PG Scholar (Computer and Communication Engineering)
ashokit009@gmail.com
Sri Sai Ram Engineering College, Chennai.

ABSTRACT

Ad-hoc network is a temporary network connection that can change locations and configure itself on the fly. Packet may loss in network due to frequent link failure in ad hoc network. In this paper, we maintain log at each router to find out where the loss actually occur and a special scheme used is Signal Stability-Based Adaptive routing protocol that uses signal stability to find stable route during link failure. This protocol is *beacon-based,* in which the signal strength of the beacon is measured for determining link stability. The node then select alternate route to forward the packets without any loss. The significant nodes are assumed and implemented by using *beacons* count of previous node. This model finds more stable routes to reduce path breaks and ill effects.

Keywords: Log record, Beacon count, Signal Stability, Stable/unstable link.

1. INTRODUCTION

The wireless ad hoc network does not have any kind of infrastructure to form network, due to this it had relative congestion in network which leading to packet buffering and continuously degrades the performance in network. In this paper, an *operationally viable* approach used to find out where the loss arises. The key idea is that detecting packet loss is to find where the packet lost in the network. Thus, when a broken link is detected, it searches for strongest signal strengths of its neighbor's beacons to provide alternate path to its destination.

2. PROTOCOL

Maintaining logs states the information about each packet that passes through it. If the actual behavior deviates from the predicted behavior, then a failure has occurred.

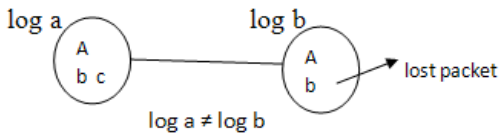

Fig 2.1

Below condition to be satisfied to detect where the packet has lost:
Buffer limit (BL) is maintained at each router. If BL<QP+ps, then the packet P is dropped due to congestion. Every log is evaluated with the previous one before it is forwarded. In our case, if log a ≠ log b, then rb stops forwarding packets further- detect failure.

3. LOG RECORD

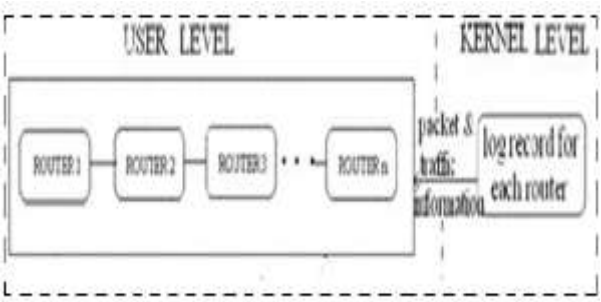

Fig 3.1

Each router in the network maintains a log record containing information about the number of packets sent and received (N), the size of each packet (ps), header of the packet (P), time at which the packet

was received (t). This log record helps in detecting where the loss in packet occurred. Each router maintains a queue (Q) before it gets the particular packets. Buffer limit (BL) is maintained at each router. If BL< (qp+ps), then the packet P is dropped. When a packet arrives at router r and is forwarded to a destination that will traverse a path segment ending at router x, r increments an outbound counter associated with router x. Conversely, when a packet arrives at router r, via a path segment beginning with router x, it increments its inbound counter associated with router x. periodically, router x sends a copy of its outbound counters to the associated routers for validation. Then, a given router r can compare the number of packets that x claims to have sent to r with the number of packets it counts as being received from x, and it can detect the number of packet losses.

4. *SIGNAL STABILITY-BASED ADAPTIVE ROUTING*

Signal Stability-based adaptive routing protocol is an on-demand routing protocol that uses signal stability to find the stable route to its destination. This protocol is beacon-based, in which it is measured for determining link stability. It is classified as stable and unstable link which is based on its signal strength. Every node has signal stability routing table that contains the beacon count and signal strength of each of its neighbor's node. If a node has received strong beacons for the past few beacons, the node classifies as stable link. Otherwise the link is called as unstable link.

5. *IMPLEMENTATION*

5.1 Route Establishment

5.1.1 Route-REQUEST Packet:

When a source node needs to send packet to its destination node, first it broadcasts a *Route Request* for finding the route to its destination node. When the Route Request packet is initiated by the source, it is broadcasts to all neighbor's node. Before processing of broadcasts to other nodes it checks whether the Route Request packet had been received over a stable link. If the Route Request has been received through a stable link and had not been sent already, it is forwarded by the node; otherwise, it is dropped. When source node broadcasts Route Request, it reaches node 2, 5, and 6, it is forwarded only by nodes 2 and 5 as the link between nodes 1 and 6 is weak. Similarly, the Route Request forwarded by node 2 is rejected by nodes 3 and 5, while node 4 forwards it to neighbors, provided it has not already been forwarded. In this manner, request reaches to its destination. In figure 5.1.1, solid lines represent the stable links and dotted lines represent weak link. Consider only one strong link is established from source to destination. A path through 1-5-10-14-15 is rejected by its destination as it receives node 14 on a weak link. The stable path consisting of strong links is 1-2 (or 5)-4-8-13-15. The first Route Request packet that reaches the destination over a stable path is selected by the destination

5.1.2 Route-REPLY Packet:

When a source node does not have route to its destination, floods the networks with Route Request packets. But unlike other routing protocols, nodes that employ the Signal stability Adaptive routing protocol process a Route Request only if it is received over a strong link. A Route Request receives through a weak link is dropped without being processed. The destination selects the first Route Request packet received over strong links. The destination initiates a Route Reply to notify the selected route to the source.

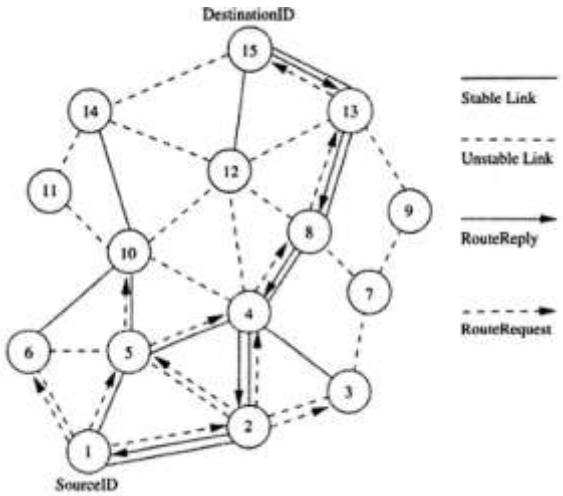

Fig 5.1.1 SSA Route establishment

5.2 Route Maintenance

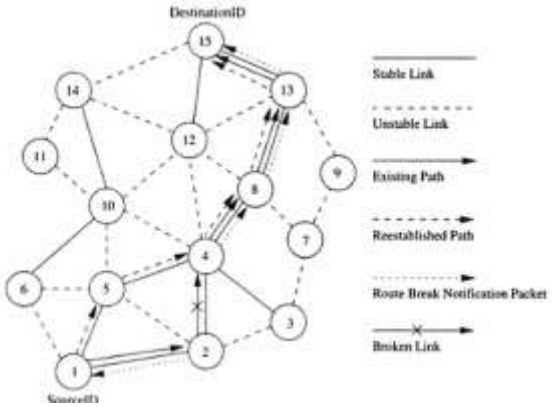

Fig 5.2.1 Route Maintenance in SSA

In the route maintenance, when a link failure occurs the end nodes of the broken link notify the corresponding end nodes of the path. Upon receiving a route break notification, source node rebroadcasts the Route Request to find another stable link path to its destination. In figure 5.2.1, link breaks between the nodes 2 and 4, and then end nodes notify corresponding nodes 1 and 15. If the link breaks between 2 and 4, a new strong path is established through 1-5-8-13-15. If no strong path is available to route packets to its destination, (e.g., 8-13) then new route is established by considering weak links also. This is done when multiple route request attempts fail to get a path using only the stable links.

6. *PERFORMANCE EVALUATION*

It has following steps.

6.1 Throughput

It is the ratio of bits received to the amount of time taken to travel from source to destination.

T=bits received/time taken

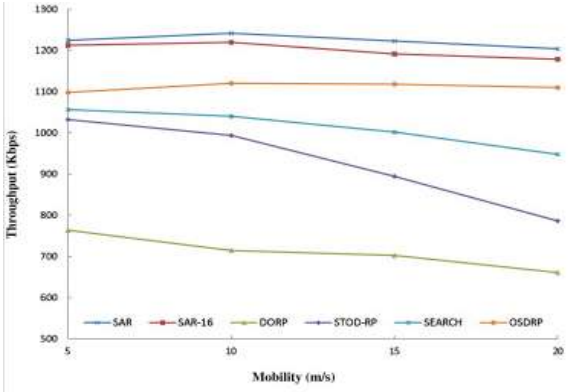

Fig 6.1.1 Comparison of Throughput

6.2 Router Overhead:

It is defined as the average amount of routing protocol control packets in the network.

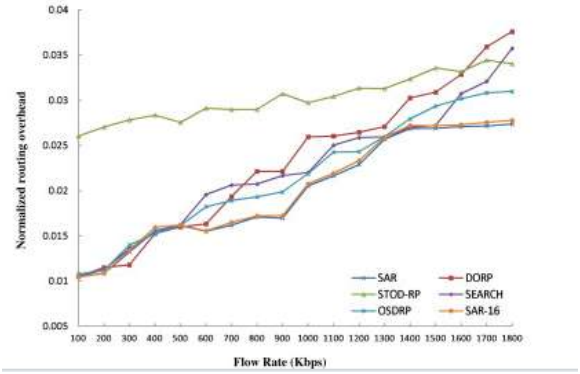

Fig 6.2.1Comparison of Router Overhead

6.3 End-to-end delay:

It is the time taken for a packet to be transmitted across a network from source to destination.

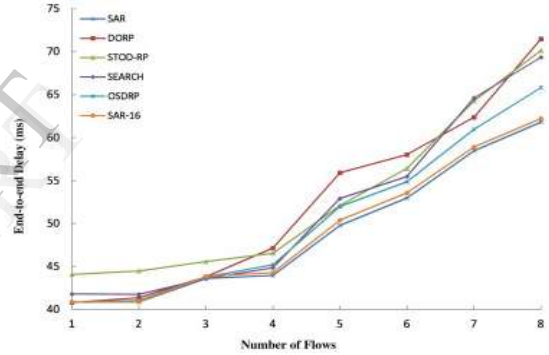

Fig 6.3.1 Comparison of End-to-end delay

7. *CONCLUSION*

If any loss of packet in network, log record helps in detecting where the loss in packet occurred and it can be recovered by Signal Stability-Based Routing, which is simulated by using beacons count. The simulation results show that this protocol provide best stable route to transfer packet to its destination when compare to the shortest path route selection protocol such as DSR and AODV.

8. *REFERENCE*

[1] R. Dube, C. D. Rais, K. Y. Wang, and S. K. Tripathi, "Signal Stability-Based Adaptive Routing for Ad Hoc Mobile Networks," IEEE Personal Communications Magazine, pp. 36-45, February 1997.

[2] Ashok, P.; Purushothaman, N.; Elumalai, K., "Detecting and temporarily recovering lost packets in Ad-hoc network by using Bypass routing," *Radar, Communication and Computing (ICRCC), 2012 International Conference on* , vol., no., pp.264,267, 21-22 Dec. 2012.

[3] E. Royer and C.-K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE Personal Communications*, vol. 6, no. 2, pp. 46–55, Apr. 1999.

[4] Levente Buttyán, Jean-Pierre Hubaux "Simulating Cooperation in Adhoc Wireless Network" "Mobile Networks and Applications" October2003.8thvolume

[5] C.E Perkins and E.M Royer, "Ad Hoc On-Demand Distance Vector Routing," Proceeding of IEEE Workshop on Mobile Communication System and Applications 1999, pp. 90-100 Februaru 1999.

[6] V. Padmanabhan and D. Simon. Secure traceroute to detect faulty or malicious routing. In *Proc. ACM SIGCOMM HotNets Workshop*, Oct. 2002

[7] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields and Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", in proc. of 10th International Conference on Network Protocol,November 2002

[8] M. K. Marina and S. R. Das, "On demand multipath distance vector routing in ad hoc networks," in *IEEE International Conference of Network Protocols (ICNP)*, 2001

[9]http://www.scribd.com/doc/37457740/Detecting-Malicious-Packet-Losses

[10]*www.ecse.rpi.edu/ "router overhead "*

[11] Hari, K.K.K., "On demand temporary route recovery for frequent link failures in adhoc networks," *Trendz in Information Sciences & Computing (TISC), 2010* , vol., no., pp.181,185, 17-19 Dec. 2010 doi: 10.1109/TISC.2010.5714635

[12] *Alper T. Mizrak, Stefan Savage and Keith Marzullo, "Detecting Malicious Packet Losses" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 20, NO. 2, FEBRUARY 2009*