ISSN (e): 2250 – 3005 || Vol, 04 || Issue, 11 || November – 2014 ||
International Journal of Computational Engineering Research (IJCER)

Quality of service Routing Using Stable Nodes in Mobile Ad hoc Networks

[1,]G.Madhukar Rao, [2,]T.santhosh
1Assistant Professor, Dept.of Computer Engineering, Sanjivani College of Engineering
2 Assistant Professor, Dept. of Computer Science Engineering, Dehradun Institute of Technology

ABSTRACT *:*
An efficient and secured routing protocol design is the vital concern for mobile ad hoc networks in view of major problems raising on security issues and loss of the network resources is due to changes within the connections of the network like Node failures, link breakages in the network. Our proposed scheme enhances the secured and reliable transmission of data, which also improves the network constancy, efficient packet delivery ratio and network life time by integrating through the AODV Routing protocol. It unites the authentication, stable routes and signal strength of the nodes to attain the secure and reliable transmission of data through nodes.

KEY WORDS: *Ad hoc network, Routing protocols, AODV, power, signal strength, Quality of Service, authentication.*

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is compilation of mobile nodes with no existing pre established infrastructure, forming a temporary network. Each mobile node in the network act as a router. Such networks are characterized by: Dynamic topologies, existence of bandwidth constrained and variable capacity links, energy constrained operations and are highly prone to security threats. Due to all these features routing is a major concern in ad hoc networks. MANET is viewed as suitable systems which can support some specific applications as virtual classrooms, military communications, emergency search and rescue operations, data acquisition in hostile environments, communications set up in Exhibitions, conferences and meetings, in battle field among soldiers to coordinate defense or attack, at airport terminals for workers to share files etc. Due to the frequent changes in network topology and the lack of the network resources both in the wireless medium and in the mobile nodes, mobile ad hoc networking becomes a challenging task. Routing in Ad hoc networks experiences more link failures than in other networks. Hence, a routing protocol that supports QoS for ad hoc networks requires considering the reasons for link failure to improve its performance. Link failure stem from node mobility, secured transmission and lack of the network resources. In such a case, it is Important that the network intelligently adapts the session to its new and changed conditions.

Secured and Quality of service means providing a set of secure and service requirements to the flows while routing them through the network. A new scheme has been suggested which combines four basic features to Achieve security in terms of modification, impersonation, and fabrication exploits against ad hoc routing protocols and QoS; these are authentication ,stable routing, concept of battery power and signal strength. The scheme uses Certificate Authorities (CAs), backbone nodes for stable routes and uses power factor and signal strength to determine active nodes to participate in routing. The rest of the paper is organized as follows: Section 2 takes a look at the Routing protocols classificatio Section 3 analyzes new proposed scheme and Section 4 summarizes the study and the status of the work.

II. ROUTING PROTOCOL CLASSIFICATIONS

A routing protocol has to find a route for packet delivery and make the packet delivered to the correct destination. Many protocols [2] have been suggested keeping applications and type of network in view. Routing Protocols in Ad Hoc Networks can be classified into two types:

A. Table Driven or Proactive Protocols : Table driven routing protocols maintain consistent, upto-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information. These routing protocols respond to changes in network topology by propagating updates information throughout network. This type of routing is called as source routing. The areas in which they differ are the number of necessary routing tables and changes in network structure are broadcast. Some of the table driven or proactive protocols are: GSR, WRP, ZRP, STAR etc.

B. On Demand or Reactive Protocols : A different approach from table-driven routing is source-initiated on-demand routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or until the route is no longer desired. Some famous on demand routing protocols are: DSR, RDMAR, AODV etc. Authenticated Routing for Ad hoc Networks (ARAN), [17] detects and protects against malicious actions by third parties and peers in one particular ad hoc environment. ARAN [17] introduces authentication, message integrity, and non-repudiation to an ad hoc environment as a part of a minimal security policy. The study has been concentrated on reactive routing protocols because of proposed scheme is suitable for this protocols.

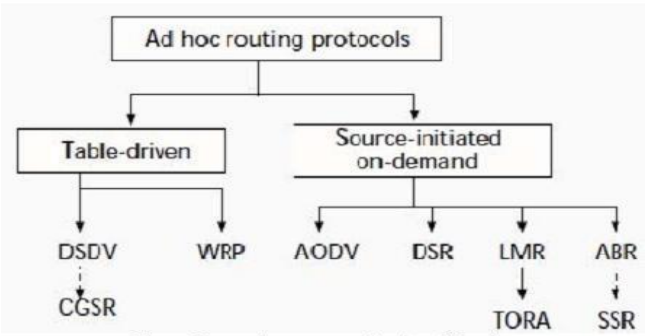


Figure1: routing protocols classification

III. PROPOSED SCHEME: AARRP

The proposed scheme"Authenticated Reliable Routing Protocol for Mobile Ad hoc Networks" takes care of on demand routing along with a new concept of Authenticated backbone nodes with optimal power factor and signal strength. This scheme concerns about the secure, reliable routes and better packet delivery ratio. The emphasis is on concept of authentication, battery power and signal strength or energy requirement for routing process. In this paper four different concepts have been joined together to make an efficient protocol. The backbone nodes help in reconstruction phase i.e., they assist in fast selection of new routes. Selection of backbone nodes is made upon availability of nodes, battery status and signal strength. Each route table has an entry for number of backbone nodes attached to it and their CAs(Certificate authorities), battery status and signal strength. The protocol is divided into three phases. Route Request (RREQ), Route Repair (RREP) and Error Phase (ERR). The proposed scheme is explained with the help of an example shown in Figure 2. The light colored nodes depict the node with less power factor. The Route selection from S (source) to D (destination) is made via 1-2-3-4-5 using shortest path routing

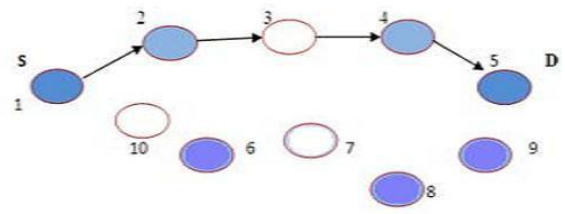


Figure 2: Example of routing

In case any of the participating nodes get damaged or move out of the range, the backbone nodes (6,8 and 9) can be takes care of the process. These nodes are nearer to the routing path nodes and have a sufficient power and signal strength so they can join the process any time. This may lead to slight delay but improves overall efficiency of the protocol by sending more packets without link break than the state when some node is unable to process route due to inadequate battery power and signal strength. The process also helps when some intermediate node moves out of the range and link break occurs. In such cases the backbone nodes take care of the process and the route is established again without much overhead. The nodes which are having battery power and signal strength can be selected for route reconstruction. Backbone Node will be selected at one hop distance from the affected node.

A. Route Construction(REQ) Phase : In AODV routing protocol [5], route request and route reply operations are the most important, and route discovery with AODV is purely on-demand. When a node wishes to send a packet to a destination node, it checks its route table to determine whether it currently has a route to that node. If so, it forwards the packet to the next appropriate hop toward the destination; otherwise, it has to initiate a route discovery process. The source node broadcasts a flooding RREQ packet, which contains the ce rt i f i c at es of t h e no d e; i p a dd r ess broadcast ID to form a unique identifier for the RREQ. The intermediate nodes can avoid processing the same RREQ using this unique identifier. After broadcasting the RREQ, the source node sets a timer to wait for a reply. The node that successfully received the RREQ should The node that successfully received the RREQ should judge whether it is the destination or it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. In the latter case, the node uncast a route reply (RREP) packet back to the source; otherwise, it rebroadcasts the RREQ. If the intermediate nodes receive the RREQ they have already processed, the RREQ should be discarded directly. When the route reply process is done, a forward route is set up. When a link break in an active route is detected, an ERR message is used to notify that the loss of link has occurred to its one hop neighbor. Here ERR message indicates those destinations which are no longer reachable. Taking advantage of the broadcast nature of wireless communications, a node promiscuously overhears packets that are transmitted by their neighboring nodes. When a node that is not part of the route overhears a REP packet not directed to itself transmit by a neighbor (on the primary route), it records that neighbor as the next hop to the destination in its alternate route table. From these packets, a node obtains alternate path information and makes entries of these backbone nodes (BN) in its route table. If route breaks occurs it just starts route construction phase from that node. The protocol updates list of BNs and their c e r t i f i c a t e s , power status and signal strength periodically in the route table.

B. Route Maintenance : When node detects a link break [1], it performs a one hop data broadcast to its immediate neighbors. The node specifies in the data header that the link is disconnected and thus the packet is candidate for alternate routing. Upon receiving this packet route maintenance phase starts by selecting alternate path and checking power status, signal strength.

C. Local Repair : When a link break in an active route occurs as shown in figure 3, the node upstream of that break may choose to repair the link locally if the destination was no farther and there exists BNs that are active. When a link break occurs the route is disconnected. Backbone nodes are broad casts their certificates, power status and signal strength to the neighbor nodes. The node which are having authenticated certificate, maximum battery power and signal strength can be selected as route[7].

.The received signal strength can be calculated as

$Pr = cert(n) + Pt/4*pi*di^2$+power status

Here Pr is the total received signal strength, Pt is the transmission power of the node and di is the distance of the node and cert(n) is the certificate of the node.

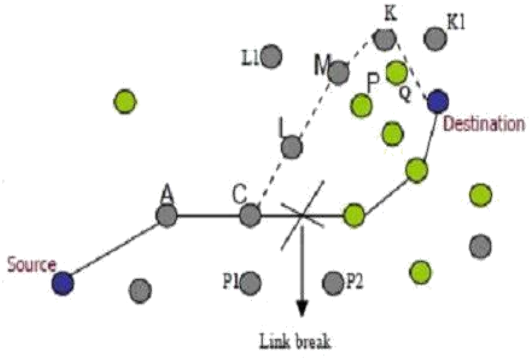
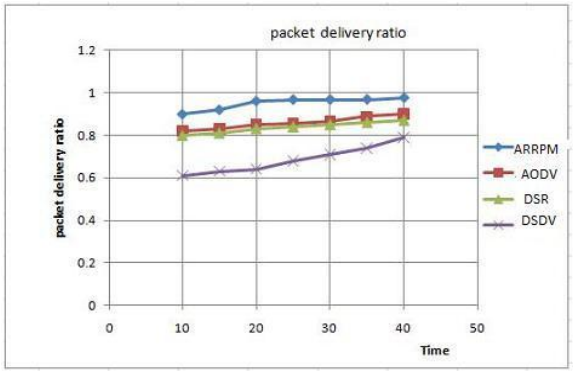


Figure 3: Local repair

When link breaks at node C, route repair starts, node C starts searching for new paths, buffering packets from S-A in its buffer. The nodes L, M, K, K1, L1, P1, P2 are broadcasts their certificates, power status and signal strength to its neighbor nodes. Now backbone nodes are selected and proper selection of nodes is done based on authenticated nodes, power factor and signal strength. Path selected becomes [C - L – M – K – Destination], instead of [C – L– P –Destination], since the node P is not in active state. Even though the route may become longer, the selected route path is far more stable and delivery of packets is reliable. Stability and reliability of route depends upon four major aspects as: Authentication, Life time, Power status and signal strength.

IV. SIMULATION AND RESULTS

Simulation study has been carried out to study the Performance study of existing different protocols Simulation Environment used is NS-2 (network simulator) version NS2.29 to carry out the process. Simulation results have been compared with AODV, DSR and TORA. Simulation study has been performed for packet delivery ratio.



REFERENCES

[1] Vinay Rishiwal, Ashwani Kush, Shekhar Verma "Stable and Energy Efficient Routing for Mobile Adhoc Networks" Fifth International Conference on Information Technology: New Generations 2008, 1028-1033.
[2] E.M. Royer and C.K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks". IEEE Personal Communications, pages 46–55, April 1999.
[3] J.J. Garcia, M. Spohn and D. Bayer, "Source Tree Adaptive Routing protocol", IETF draft, October 1999.
[4] D.B. Johnson, D.A. Maltz, "Dynamic Source Routing in Ad Hoc Networks", Mobile Computing, T. Imielinski and H. Korth, Eds., Kulwer, 1996, pp. 152-81 protocol for mobile ad hoc networks (RDMAR)", CCSR ,UK.
[5] C.E. Perkins, E.M. Royer, "Ad-Hoc On Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Application New Orleans, LA, February 1999, pp. 90-100.
[6] Josh Broch, David A.Maltz and Jorjeta Jetcheva, "A performance Comparison of Multi hop Wireless Adhoc Network Routing Protocols", Mobicomm'98, Texas, Oct 1998.
[7] WU Da-peng , WU Mu-qing, ZHEN Yan, "Reliable routing mechanism based on neighbor stability for MANET" www.buptjournal.cn/xben June 2009, 16(3): 33–39.
[8] C. K. Toh, "Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks", IEEE Comm. Mag., June 2001, pp. 138-147.
[9] Z.J. Hass, M.R. Pearlman, "Zone routing protocol (ZRP)", Internet draft. June 1999, at www.ietf.org

[10] E. Crawley, R. Nair, B. Rajagopalan, and H.Sandick, "A framework for QoS based routing in the internet," RFC 2386, Aug. 1998.
[11] M. Ettus. System Capacity, Latency, and Power Consumption in Multihop-routed SS-CDMA Wireless Networks. In Radio and Wireless Conference (RAWCON '98), pages 55–58, Aug.1998.
[12] X. Lin and I. Stojmenovic. Power-Aware Routing in Ad Hoc Wireless Networks. In SITE, University of Ottawa, TR-98- 11, Dec. 1998.
[13] A. Chockalingam and M. Zorzi, "Energy Consumption Performance of a Class of Access Protocols for Mobile Data Networks," Proc. IEEE VTC, May 1998, pp. 820–24.
[14] A. Michail and A. Ephremides, "Energy Efficient Routing for Connection Oriented Traffic in Ad-hoc Wireless Networks," Proc. IEEE PIMRC, Sept. 2000, pp. 762–66.
[15] G. Zussman and A. Segall. Energy efficient routing in ad hoc disaster recovery networks. Proceedings of IEEE INFOCOM, April, 2003.
[16] C. Schurgers and M. B. Srivastava. Energy efficient routing in wireless sensor networks. Proceedings of IEEE MILCOM, pages 28–31, October 2001.
[17] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, E. M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," 10th IEEE International Conference on Network Protocols (ICNP'02) November 12-15, pages 78-89, 2002.