IJCSC International Journal of Computer Science and Communication Vol. 2, No. 2, July-December 2011, pp. 423-426

AN IMPROVEMENT OF AODV PROTOCOL BASED ON THREADED ROUTING IN MOBILE AD HOC NETWORKS

Yogendra Kumar Jain[1] and Nilesh Vani[2]

[1]Head of CSE Department, Samrat Ashok Technological Institute, Vidisha (M.P.), India 464001.
E-mail: ykjain_p@yahoo.co.in
[2]Research Scholar M. Tech., Samrat Ashok Technological Institute,Vidisha(M.P.), India 464001.
E-mail: nileshvani@gmail.com

ABSTRACT

The Mobile Ad hoc NETworks (MANETS) are suitable to be utilized in the context of an extreme emergency conditions such as battle field and disaster recovery because less requirement of infrastructure and dynamic nature. These, along with applications of these networks in military, government and in commercial area, MANETs are being researched by many organizations and institutes. Many protocols have been developed for data link layer and network layer. Many researchers have been conducted numerous simulations for comparing the performance of these protocols under varying conditions and constraints.

The widely-used protocol in Mobile Ad hoc Network (MANET) achieves a dynamic, self-organizing and on-demand multi-hop routing by means of the AODV routing protocol. MANETs are characterized by self-organized, dynamic changes of network topology, limited bandwidth, and instability of link capacity, etc. The reliability of data transmission in the network cannot be guaranteed, in some special application conditions with harsh requirements on Packet Delivery Ratio (PDR) and link quality, higher criteria for routing protocol will have been laid out. This paper presents an AODV with threaded routing (AODV-FLTR) for security purpose. To reduce routing overhead and to increase packet delivery ratio, local route discovery process is used when link breaks during transmission. The performance comparison of AODV-FLTR with DSR and AODV is also carried out.

Keywords: MANET, AODV, DSR, AODV-FLTR, Security.

1. INTRODUCTION

A common name for 802.11 is Wi-Fi. This standard had to work in two modes, in the presence of a base standard and in the absence of a base station. In former case, all communication was to go through the base station, called an access point in 802.11 terminologies. In the latter case, the computers would just send to one another directly. This mode is now sometimes called mobile ad hoc networking (MANET). Each node in the network also acts as a router, forwarding data packets for other nodes. A central challenge in the design of ad hoc Networks is the development of a dynamic routing protocol that can efficiently find routes between two communicating nodes.

Mobile ad hoc network is a collection of mobile nodes that are dynamically communicating without centralized supervision. An efficient routing algorithm that minimizes the access delay and power consumption while maximizing utilization of resources remains a challenge for the ad hoc network design. For these reasons we have considered efficient routing protocols and we have evaluated their performances. This task becomes more complex as the network nodes change randomly their positions.

Recent research in ad hoc networks has focused on security and routing problems. Different protocols have been developed for both layers and some analysis work and performance work has been done. Most of such performance analysis work is based on simulation studies with several design parameters in commercial settings.

DSR [1] and AODV [2] shares an interesting common property-they both initiate routing activities on an on demand basis. This reactive nature of these protocols is a significant departure from more traditional proactive protocols, which find routes between all source-destination pairs regardless of the use or need for such routes. The key motivation behind the design of on-demand protocols is the reduction of the routing load. High routing load usually has a significant performance impact in low-bandwidth wireless links. In particular DSR uses source routing, whereas AODV uses a table-driven routing framework and destination sequence numbers. Destination sequence number is used to prevent from looping problem in AODV. DSR does not rely on any timer based activities, while AODV dose for a certain extent. In AODV least recently used entry is deleted from routing table. one of our goal in this study is to extract the relative merits of these mechanisms and to overcome some security problems.

The rest of this paper is organized as follows. In section II related work on reactive protocol is shown. In section III we present overview of AODV. In section IV proposed scheme is described then in section V results are described. Section VI concludes this paper.

2. RELATED WORK

AODV shares DSR's on-demand characteristics in that it also discovers routes on an as needed basis via a similar route discovery process. However, AODV adopts very different mechanism to maintain routing information. It uses traditional routing table, one entry per destination. In DSR multiple route cache entries for each destination is used.

An improvement of AODV protocol based on backup route (AODV-BR) in mobile ad hoc networks was proposed by S.J. Lee and M. Gerla. AODV-BR establishes the mesh and multi-paths to destination. In AODV-BR the primary route and alternate routes together establish a mesh structure that looks similar to a fish bone [3]. AODV-BR increases PDR but, has longer end-to-end delay. The simulation was performed on ns-2 network simulator.

The author suggested in his work, that the multi hop routing information is required for an intermediate node to determine a substitute node to replace the unreachable node. Hence, extended routing table is given for maintaining reverse multi hop routing information of each entry. The hop of a routing entry *j* in a mobile node *I* is denoted as next hop $^{h}_{j}(i)$.

A safe AODV mechanism is implemented by Jin Taek Kim, Jeong-Ho Kho, Chang-Young Lee, Cheol-Soo Bang and Geuk Lee in 2008. In this work two additional control messages are used to verify the path. These messages are IREQ (route investigation request) and IREP (route investigation reply) [12].

In 2008 Zhao Qiang Zhu Hongbo proposes an optimized AODV(OAODV) [10] which is a link-disjoint multipath routing approach in MANETs it tries to optimize routing overhead of both route discovery process and route maintenance process of multipath extensions to AODV. When detecting a link failure in primary route, ORMAD invokes a local repair procedure between the upstream and downstream nodes of the broken link. For route efficiency and minimization of routing overhead it applies route maintenance process to only efficient route.

An improvement of AODV protocol based on reliable delivery(AODV-RD) [5] in mobile ad hoc networks was proposed by LIU Jain and LI Fang-Min. In AODV-RD a link failure fore-warning mechanism, metric of alternate node in order to better select, and also repairing action after primary route breaks is perform. AODV-RD is an improvement in AODV-BR. In this work link failure prediction mechanism is used for this strength of the packet signal [11] is checked. The strength is in the warning state then alternate route is discovered. If more than one alternate path is present with same hop-count then the route is selected whose communicating power is stronger. AODV-RD significantly increase packet delivery ratio (PDR).

AODV-BRL [4] was proposed by Liu Yujun and Han Lin cheng. AODV-Backup-Routing with Least hop count first broadcast the RREP packet in one hop to avoid waste of resources and security risk by listening to RREP blindly instead of establishing the backup rout by monitoring the RREP packets. At the same time, besides RREP, the extended Hello message is introduced to establish the backup route to increase the adaptability to the network topology diversification. The Least Hop Count First, it is required to determine the optimal node that significantly reduces the distance between the repair node and the destination. A simulated OPNET ad hoc network is comprised of 50 nodes within 600m*600m area.

In 2010 Sethi and Udgata propose an Optimized reliable ad hoc On-Demand distance Vector (ORAODV) [9]. Scheme that offers quick adoption to dynamic link conditions, low processing and low network utilization in ad hoc network. They use a mechanism of retransmission of undelivered data packet with blocking ERS technique to enable optimal path routing and fast route delivery with an improvement of PDR.

3. AODV

AODV is flat, reactive Hop-by-Hop routing protocol. AODV adopts DSR's on-demand characteristics and in contrast to DSR, It uses traditional routing table it is similar to DSDV [6]. AODV uses routing table entries to propagate an RREP back to the source and subsequently, to route data to the destination. AODV relies on sequence number to maintain freshness of routing information and to prevent routing loop [2], sequence number information is carried by all routing packets.

To maintain routing table entries AODV uses timer based states in each node. A set of predecessor node is maintained for each routing table entry, indicating the set of neighboring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next –hop links breaks. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. If more data packets has to be send to the destination, AODV restarts route discovery process to find new path. The route reply in DSR carry the address of every node along the route, whereas in AODV the route reply carry only the destination IP address and the sequence number. The advantage of AODV is that it is more suitable for highly dynamic networks.

4. PROPOSED WORK

To improve packet delivery ratio of AODV and some security purpose, AODV-Flat Threaded Routing uses new mechanism when link breaks. In AODV-FLTR each node stores one thread per destination. Route discovery process is similar to AODV. If link breaks then its previous node will send route request packet to already stored neighbors, it will not broadcast that request. Neighbor node will follows same process to reach the destination. After the ending of this process, if destination is found then packets will be send by this new path otherwise RERR packet will be send back by the node to the source node and by source node route discovery process will be restarted.

4.1 Route Discovery

Route discovery process is same as used in AODV. Source node will search the destination by flooding route request (RREQ) packet to their neighbor; neighbor node will search their routing table. It then broadcast the RREQ packet to its neighbor or will send RREP to source if it has a route to the destination and so on. When first RREQ packet reaches to destination, it replies by RREP packet. This packet will follow the same path which is followed by RREQ packet. If destination node receives more RREQ packet then it will reply by one hello message this hello message will follow the same rout which was followed by RREQ packet. Hello message is discarded at the source node. When a node receives RREP or Hello message from a neighbor, this neighbor node will be recorded as a next hope to the destination.

Hence in FLTR extended routing table is used where next hop and previous node entries are stored. Every node is registered in its predecessor and ancestor node. In contrast to DSR, Only one path will be established for destination in AODV and AODV-FLTR.

4.2 Route Maintenance Process

In AODV-FLTR if link breaks then previous node of that link will perform route discovery for the destination. Previous node will multicast RREQ packet to its all neighbor. After receiving RREQ packet, node will search their routing table. It then sends back a route reply (RREP) if it has a route to the destination. If it has not, then it will multicast RREQ to their neighbor node. When RREQ packet reaches to destination it will send RREP back and data transmission will be restarted. If destination node is not reachable, then route discovery process will be restarted by original source.

Hence in the proposed work route discovery process initializes by intermediate node it increases packet delivery ratio and decreases routing overhead. Already registered node can participate in data transmission which can prevent from malicious node.

5. RESULT & ANALYSIS

5.1 Environment

We have implemented our work in C++ on the Linux environment in which in built compiler Genome has been used. Simulated network is comprised of different number of nodes placed randomly within 1500m*1500m area. Packet size is used 512-byte. The node moves randomly towards a random spot until it reaches that spot, then it pauses for some pause time and moves again. Simulation is performed for different pause time. Node sends and receives range 150m. Each node uses IEEE802.11 [8] as MAC layer and physical layer protocol.

A. Packet Delivery Ratio

Packet delivery ratio for 25 and 80-nodes network is shown in figure 1 and figure 2 respectively in percent of all routing load for DSR, AODV, and AODV-FLTR. AODV-FLTR uses extended and threaded routing table therefore PDR is more in AODV-FLTR than DSR and AODV. In figure PDR is shown for different pause time. It shows that if pause time increases then PDR also increases and if number of node increases then Packet delivery ratio decreases slightly.

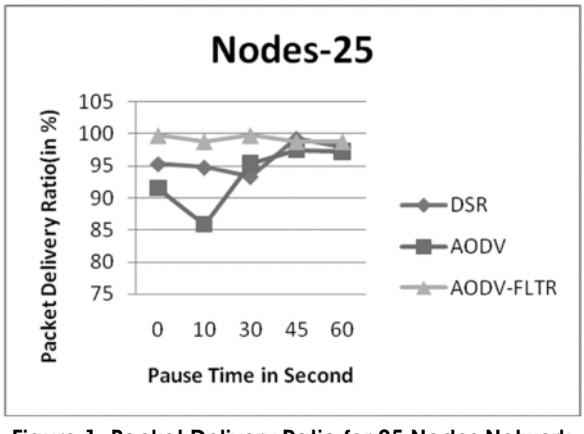

Figure 1: Packet Delivery Ratio for 25 Nodes Network

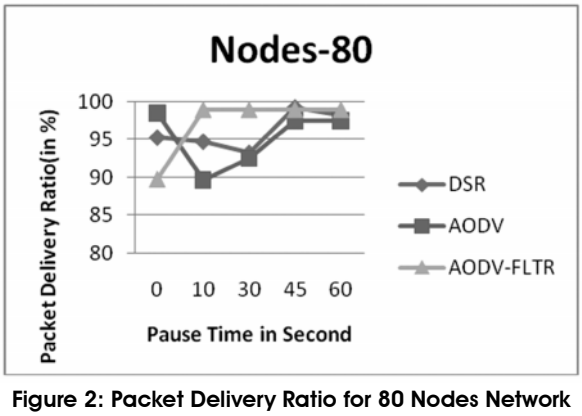

Figure 2: Packet Delivery Ratio for 80 Nodes Network

B. Routing Load

The routing load is calculated by taking the total number

of per-hop control packet transmissions, and dividing this by the number of data packets successfully delivered to their destination. Routing load is for pause time 30s and 60s is presented in figure 3 and figure 4 respectively in percent of all routing load. This routing load is calculated for different size network. In AODV-FLTR routing load is less than DSR and AODV. In AODV-FLTR, if link breaks, route discovery process is initiated by intermediate node. Graph shows that, if network size increases then routing load is also increases.

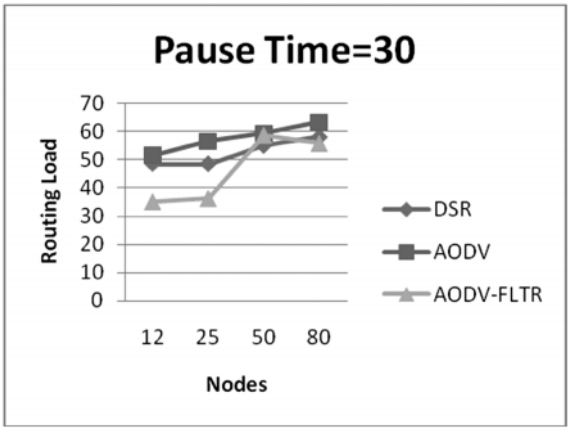

Figure 3: Routing Load for Pause Time 30s

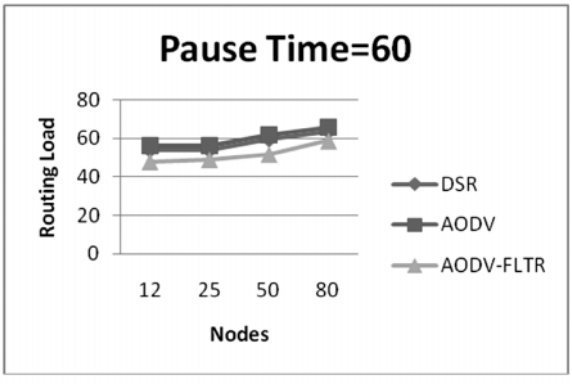

Figure 4: Routing Load for Pause Time 60s

6. CONCLUSION

In this paper we have developed new mechanism to reactive protocol AODV, to improve the packet delivery ratio and extended routing table and threading concept to prevent from malice node. AODV-FLTR's Packet delivery ratio is more than AODV and DSR. Routing load is more in AODV and DSR than AODV-FLTR. If network size increases packet deliver ratio decreases and routing load increases in both protocol. If link breaks then, any malicious node cannot take responsibility to transmit data packets in AODV-FLTR.

REFERENCES

[1] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad hoc Wireless Networks", T. Imielinski and H. Korth, *Eds. Mobile Computing*, Ch. 5, Kluwer, 1996.

[2] C. E. Perkins and E. M. Royer, "Ad Hoc on- Demand Distance Vector Routing", *Proc. 2nd IEEE Wksp. Mobile Comp.Sys. and Apps.*, Feb. 1999, pp.90-100.

[3] S.J. Lee and M. Gerla. "AODV-BR : Backup Routing in Ad hoc Networks", In *Proceedings of the IEEE Wireless Communications and Networking Conference*, page 1311-1316, 2000.

[4] Liu Yujun and Han Lincheng, "The Research on an AODV-BRL to Increase Reliability and Reduce Routing Overhead in MANET", *International Conference on Computer Application and System Modeling*, Age v12-526 to v12-530, 2010.

[5] LIU Jian and LI Fang-min, "An Improvement of AODV Protocol Based on Reliable Delivery in Mobile Ad hoc Networks", *Fifth International Conference on Information Assurance and Security*, page 507-510.

[6] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing for Mobile Computers", *Comp. Com-mun. Rev.*, Oct.1994, page 234-44.

[7] Harisavan Somnuk and Mayuree Lertwatechakul, "Multi-hop AODV-2T", *International Symposium on Intelligent Ubiquitous Computing and Education*, page 214-217,2009.

[8] IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer Speciphications", IEEE std. 802.11-1997,1997.

[9] S. Sethi and S. K. Udgata,"Optimized and Reliable AODV for MANET", *International Journal of Computer Application*, **3**, No. 10, July 2010.

[10] Zhao Qiang Zhu Hongbo, "An Optimized AODV Protocol in Mobile Ad hoc Networks", In *Wireless Comm., Networking and Mobile Computing 2008 (WiCOM'08)*, 4th International Conference on Oct. 12-14, 2008, pp 1-4.

[11] Qing Li, Cong Liu, Han-Hong Jiang, "The Routing Protocol of AODV Based on Link Failure Prediction [C]", *Proceeding of the International Conference on Software Process*, 2008.

[12] Jin Taek Kim, Jeong-Ho Kho, Chang-Young Lee, Cheol-Soo Bang and Geuk Lee, "A Safe AODV (Ad hoc On-Demand Distance Vector) Security Routing Protocols", *Proceeding ICHIT '08 Proceedings of the 2008 International Conference on Convergence and Hybrid Information Technology.*