ISSN: 0976-3104
SPECIAL ISSUE: Emerging Technologies in Networking and Security (ETNS)
Indhumathi and Deepa

THE IIOAB JOURNAL

ARTICLE OPEN ACCESS

AODV- QRS: A MULTIPATH QUALITY ROUTE SELECTION AODV FOR HIGH MOBILITY NETWORK

Indhumathi and Baby Deepa
Computer Science, Bharathiyar University, Coimbatore, INDIA
Government Arts College- Autonomous, Karur, INDIA

ABSTRACT

Mobile Ad-hoc Network (MANET), a collection of self-configurated mobile nodal networks which can function without the need for any significant infrastructure. Routes have a tendency of switching very frequently and swiftly, especially because of the dynamic nature of network topology and due to this factor issues in route protocols have an important role and they are efficiently handled. Ad hoc On demand Distance Vector (AODV) routing systems are a popularly adopted MANET routing protocol system which is known for its adaptive capacities, especially to highly dynamic topologies even though it has issues in delay and scalability. The proposal of an On-demand Node-Disjointed Multipath Routing is suggested to overcome the shortcomings of on-demand AODV routing protocol. The proposed method is based on two concepts: multiple discoverable routes from the source to its destination and the mobility of node mobility (which is measured using RSSI signals) and there are significant changes in the route patterns and the number of packets dropped (if they increase over a set limit). Under the proposed technique, there have been significant improvements in QoS parameters, especially when comparing AODV and DSR simulations.

Published on: 28th– August-2016

KEY WORDS

Mobile Ad-hoc Network (MANET), Routing, Ad hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Received Signal Strength Indicator (RSSI).

***Corresponding author: Email:** eindhumathi79@gmail.com

INTRODUCTION

A collection of self-configured nodular mobile networks, MANET systems perform well without any significant infrastructures. Nodes are connected to radio interfaces via wireless links in which every instrument within the MANET system is independent and free to randomly change its links frequently to other devices. A dynamic network topology, route networks shift quickly and frequently and this requires the efficient routing systems to handle important protocol roles. As a multihop process, limited transmission ranges constrain multiple mobile nodes, with each network topology actiong as a router for itself. MANET networks have the ability to ensure the safe delivery of packages and handlng any malfunctions within nodal systems, through reconfiguring the network [1].

Typical applications of MANET consist of:

- Application in military battlefields: Military bases have the advantage of maintaining proper network connections between soldiers, military information headquarters and vehicles through the use of Ad Hoc networking systems.
- Collaborative work applications: The need to created collaborated computational data for any form of business space, outside the office environment where it is difficult forpeople to have meettings and have proper exchanges of project information.
- Local level: The automatic linking of Ad-Hoc networks to temporary media can create instant connections using computer notebooks to share and spontaneously spread information among participants in a classroom or a conference. Home networks are an alternative locally used application system where devices and home networkds directly communicate and exchange information.
- Personal area network and Bluetooth: A short ranged personal area network , where nodes are localized and commonly linked with a given individual. MANET based short range devices such as Bluettooth enables machines can help make inter-communication channels between portable devices like mobile phones and

THE IIOAB JOURNAL ISSN: 0976-3104

laptops.

- Applications built for the Commercial Sector: In the case of an emergency rescue operation Ad hoc networks are popularly used for engaging in disaster relief efforts, for instance: in the case of an earthquake, flood or fire. It is essential for using uninterrupted communication systems for engaging in emergency rescue operations and especially for rapidly deploying networks wherever needed [2].

Ths, it is a big challenge to design routing patterns for MANET systems, espcially the task of creating a dynamic topological network. Important reason for this change has been the multiple changes in the topology due to the higher degress of noludar mobility. Numerous protocols were developed in order to achieve this task and especially through selective path routing processes within a network, data packets were shifted from one node to another to transfer data in networks. A conventional MANET routing protocol is a standardized control of data flow in the network and also decide that which path should be followed by the packets to the reach the particular destination [3].

Routing protocols in MANET are categorized based on implementing strategies in routing . The different kinds of Routing Protocols are as follows: (1) Table driven- Proactive Protocols, (2) On demand or Reactive Protocols and lastly, (3) Hybrid Protocols. Table driven Protocols are determined by conjoining nodes which connect a lcation to its destination and these are periodically maintained by updates in the routes. Whereas among o-demand routing protocols pathways are discovered when required and after a certain period of time expire. The last category, namely Hybrid routing protocols have the combined features of both reactive and proactive routing systems to scale network size and calculate the density of nodes in a network.

The AODV routing protocol algorithms are structured to cater to ad hoc modular networks. It has the capacity to both multicast and unicast routing systems and as an on-demand equation, it has created routes between nodes as a desired source route. A reactive protocol creates routes among nodes as required by sourced nodes. This protocol also maintains the above paths as per the requirement of the sources. But, apart from these, AODV systems help in creating new trees which help conjoin members together. These systems utilize systematic and sequenced numbers to promise freshness among routers. It s also free of loops, scalable at large numbers and self-startng mobile nodes[4].

Route REQuests messages are commonly used in AODV protocols to discover new paths needed by source nodes among flooded networks. Intermediate nodes which are present in this setting receive replies from RREQ and use it to route its correspodence with destination points when the sequence number is creater than or equal to what is contained into the RREQ. Most cases, the RREP sources its units back to its origin ortherwise it will be rebroadcasted in the RREQ [5].

RREQ sources are tracked by nodes through IP address and ID of the source. Sources are already processed if they already possess an RREQ ID and do not forward it. RREP propagtes source nodes back to its origin, or forward pointers to its destination and once source nodes receive RREP, it soon starts to forward pointers and data to the appropriate destination. Any RREP is containing a greater amount of sequenced numbers or the same amount with smaller hop counts, it updates routing information for destinations through better routes. The route will continue to be maintaind as long as it is active.

Routes are active as long as there are periodic travels of data packets from the source to the path destination. Links are eventually deleted after the source stios sending data packets from intermediate node tables. If a link break occurs while the route is active, the node upstream of the break propagates a Route ERRor (RERR) message to the source node to inform it of the now unreachable destination(s).

AODV protocols benefits favor least congested routes and not short routes, where it supports multicast and unicasted packet transmissions for constant movements in the nodes. The quick response to any form of topological changes affects the functioning of active routes. And AODV systems do not add any additional overhead changes to data packets which are not a part of source routings [6].

AODV protocols have certain limitations in terms of requiring broadcasting medium nodes to help detect any signals from other broadcasts. It is possible for validated routes to expire and not be able to predict a reasonable expiry time because sending time widely differs from various nodes and can change dynamically. Additionally,

THE IIOAB JOURNAL
ISSN: 0976-3104

as the performan metrics begin to decrease, the size of a network increases. Due to this, AODV networks rvulnerable to multiple forms of attaks as it is based on the assumption that every node cooperates with one another and the failure of this can lead to the breaking of nodes.

A pure example of an On-Demand routed protocol is the DSR system which is based on the theory of source routings. Designed to handled multihop ad hoc networks mobile nodes. It provides complete self-organization, self-configuration and does not require existent network administration or infrastructure [7]. DSR uses no periodic routing messages like AODV, thereby reduces network bandwidth overhead, conserves battery power and avoids large routing updates. Instead DSR needs support from the Medium Access Control (MAC) layer to identify link failure

DSR is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the network. A prominent benefit of DSR based protocols is the lack of requirement for to keep track of routes through routing table systems, to ensure the enitre packet is contained within the packet header. A unique feature of DSR exists in its source routing abilitiesm and since packet routes itself in loops of wither short or long lived patterns, they cannot be formed immediately as they will be eliminated on detection. The above property is a useful optimization protocol to open up features. But noth DSR systems or AODV can ensure a smalll path, as even if the route maybe the shortest, the destination always responds to route requests in which the source request is always the initiator. This study proposes a multipath quality route selection in AODV for high mobility network. Section 2 reviews related work in literature. Section 3 describes methods used and section 4 discusses experiments results. Section 5 concludes the paper.

RELATED WORK

A multipath routing protocol was suggested by Ahn et al., [8] in MANET systems which are composed of highly mobilized nodal networks. New multi-path routing establishes mechanisms for the main route AODV based systems, and then the process data transmission immediately begins. Backup search route processes taking place when data is transmitted by a lower than minimum transmission delay. Unconnected node routes are selected among main node route by avoiding other main body nodes. When main or back up routes break, the data transmitted continuously with another route and the broken route recovered through route maintenance processes. The result of simulation based problems on Qualnet simulator shows how the proposed routing protocol has the backup route 62.5% of the time when the main route was broken, improves the packet transmission rate by 2~3% and reduces the end-to-end delay by 10% compared with AODV and AODV-Local Repair.

Venkataraman, et al., [9] proposed a generalised trust-model over routing protocols in MANETs. The novelty of the approach, that the notion of trust can be easily incorporated into any routing protocol in MANETs. The vector auto regression based trust model was introduced to identify malicious nodes that launch multiple attacks in the network. The proposed trust model was incorporated over AODV routing protocol and Optimised Link State Routing (OLSR) protocol in MANETs. The performance evaluations showed that by carefully setting the trust parameters, a substantial benefit in terms of throughput can be obtained with minimal overheads.

Kuppusamy et al., [10] described the characteristics of ad hoc routing protocols OLSR, AODV and TORA based on the performance metrics like Packet Delivery Ratio (PDR), end-to-end delay, routing overload by increasing a number of nodes in the network. This comparative study proves that AODV, TORA performs well in dense networks than OLSR in terms of PDR.

Bagwari et al., [11] analyzed the performance of reactive routing protocol via increasing number of nodes and observing its effect on Quality of Service (QoS) of MANET. The routing protocols make an important role in improving QoS in MANET. The QoS depends on upon several parameters like end-end delay, throughput, date drop and network load. The reactive routing protocol which was considered AODV for this scenario with Multiple Cluster Head Gateway (MCHG). The author observing the performance of Routing Protocol via enhancing the network size on the basis of following parameters: delay, throughput, traffic sent, traffic received, data dropped and network load. Network simulation tool used in the simulation was OPNET Modeler (Ver. 14.0). Finally, the author has conducted simulation experiments in the conditions can be improved QoS of MANET Network performance.

Sarma & Nandi [12] proposed a Route Stability based QoS Routing (RSQR) protocol in MANET through which QoS routed extensions are controlled with constraints in delay and throughputs . This can ensure that the path was chosen for data transfer is validated and can survive for longer periods. Due to its complex nature, MANET systems suffer this critical issue and the authors suggested a simple method to address link and route stability based on the strength of signals received. By including some extra fields in route request/reply packets, the route stability information can be utilized to be selected higher stability routes within all possible routes among situated route pairs to the given destination of the source. Moreever inclusing the strength of signals on the basis of control at the time of admission can enhance performance factors in routing processes. Results of the experiments show performance improvements in terms of PDR, control overhead and average end-to-end delay in comparison with a QoS routing protocol.

THE IIOAB JOURNAL
ISSN: 0976-3104

Moussaoui et al., [13] proposed a new mechanism to be established stable and sustainable paths between all pairs of nodes in a MANET. In this mechanism, the author used a stability function as the main path selection criterion based on the calculation of the mobility degree of a node relative to its neighbor. The author applied this mechanism on the OLSR protocol to be elected stable and sustainable Multi-Point relays (MPR) nodes and topology. This mechanism can be significantly minimized the recalculation of MPR and the routing tables recalculation process. Moreover, it guarantees other QoS metrics such as the packet loss and the response time. The simulation results show the effectiveness of the mechanism and encouraged further investigations to be extended it in order to be guaranteed other QoS requirements.

Chatterjee & Das [14] proposed an enhanced version of the well-known Dynamic Source Routing (DSR) scheme based on the Ant Colony Optimization (ACO) algorithm, which can be produced a high data PDR in the low end to end delay with low routing overhead and low energy consumption. In this proposal, in the situation where a node needs to transfer the packages from one node to a different one, similar to DSR systems, the node needs to initially evaluate existing route caches. If there is a lack of availablity of known nodes, the sender can find the route by locally broadcast Route Request control packages (also known as Req. Ant packets) to find out the routes. This was similar to the biological ants initially spreading out in all directions from their colony in search of food. The author also proposed a novel pheromone decay technique for route maintenance. The simulation results show that the ACO based Enhanced DSR (E-Ant-DSR) outperforms the original DSR and other ACO based routing algorithms.

Mohanapriya & Krishnamurthi [15] presented a Modified Dynamic Source Routing Protocol (MDSR) to be detected and prevented selective black hole attack. Selective black hole attack was a special kind of black hole attack where malicious nodes drop the data packets selectively. The author proposed an Intrusion Detection System (IDS) where the IDS nodes are set in promiscuous mode only when required, to be detected the abnormal difference in the number of data packets being forwarded by a node. When any anomaly was detected, the nearby IDS node broadcast the block message, informing all nodes on the network to be cooperatively isolated the malicious node from the network. The proposed technique employs Glomosim to be validated the effectiveness of proposed IDS.

Zhao et al., [16] proposed a novel Opportunistic routing (OR) protocol - Context-aware Adaptive Opportunistic Routing (CAOR) for MANETs. CAOR abandons the idea of candidate list and it allows all qualified nodes to be needed in packet transmitted participation. CAOR can transfer simultaneous packets by using multi-cross layered knowledge, like the progress in geography, energy, mobility and quality of linkages quality, geographic progress. Through the assistance of the Analytic Hierarchy Process theory, CAOR adjusts the weights of context information based on their instantaneous values to be adapted the protocol behavior at run-time. Moreover, CAOR uses an active suppression mechanism to be reduced packet duplication. Simulation results show that CAOR can be provided efficient routing in highly mobile environments. The adaptivity feature of CAOR was also validated.

Moussaoui & Boukeream [17] presented a survey of recent routing solutions. The author started by giving general definitions related to the mobility and the link stability. Then, the author proposed a classification for the routing protocols based on the link stability. For each proposed class, the author will list examples of routing protocols. Finally, a conclusion and future research directions are discussed.

Yadav et al., [18] theorized an alternate method for calculating the availability of signal strength predictions in AODV based routing systems. Estimate link breakages in nodes and the time is taken to precaution other nodes about breakages in the pathways and on the basis of this available information, local repair links or newly discovered paths are used in advance to breakages in the route path. This can reduce the impact of daily losses in data usage packages. By the above proposed method and knowledge gained locally route repair or new route discovery, are compared with AODV systems without the need for link prediction. The results show that there was a significant reduction in packet drops and average end-to-end delay. There was also an improvement in data PDR for AODV with link prediction. Proposed approach results in improvement in the QoS.

Amara Korba et al., [19] presented a comprehensive survey of security threats in MANET. In particular, the author examined all routing threats that can target the operation of routing protocol, whether they belong to selfish behaviors or malicious attacks, as well as countermeasures against such attacks. In order to be analyzed the existent countermeasures in a structured manner it has been classified them into three classes; solutions based on cryptography; IDSs; and trust management and reputation-based solutions.

Su [20] focused on the wormhole attack, and proposed a secure routing protocol based on the AODV routing protocol, which was named Wormhole-Avoidance Routing Protocol (WARP). WARP systems use multipathed disjointed links especially at the time of multiple path discoveries, and can significantly give a greater choice in paths and which routes to be avoided due to the presence of malicious nodes, but eventually uses only one path to be transmitted information. It is based on the feature wherein wormhole nodes can access routes with ease, from source nodes to its appropriate destination nodes. Especially via the WARP neighbors are enabled to be discovered inside wormhole nodes which have abnormal attraction paths. After which point wormhole nodes consequently become alone and isolated from neighboring nodes, anf after this point they will be seperated from the entire network.

Yerneni & Sarje [21] proposed modifications to the AODV protocol and justified through the implementation of appropriate simulations via the NS-2.34, the solutions of the given problems The proposed protocol makes use of the number of RREQ and RREPs forwarded by the nodes to be detected the attack. The analysis shows that modified protocol improves PDR even in the presence of attack.

Bhalaji & Shanmugam [22] proposed and analysed a new routing protocol based on the trust model. Here each node has been calculated trust value and association status for all its neighboring nodes through monitoring its behavior in the network. Then this trust model was integrated into the DSR protocol which was the most common on demand routing protocol used in

ISSN: 0976-3104

MANET. The above idea theorizes that selected routes are not allocated based on the premise of initial RREP arrivals and it waits till this factor receives data from neighboring nodes and critically decides a pathway to be chosen based on the relation between each other . Therefore, Greyhole nodes are identified based on the above factors and they are not given any selected preferences based on route decisions wherein the existent rules within routes are examined on the basis of comparing simulation results of it with the standard DSR in the presence of Greyhole nodes. Simulated results can demonstrate how proposed routing protocols can be effectively detected Greyhole Nodes and isolated them from routing.

METHODOLOGY

RSSI portrays relations amongst transmitted and received powers by the following equation (1):

$$p_r = p_t \times \left(\frac{1}{d}\right)^n \quad [1]$$

Wherein pr refers to the amount of power received and, pt is the amount of power transmitted. Distance d is the space which exists among the sending and receiving nodes, whereas n is the amount of factors which is inputed into transmissions where the value depends on environments which are propagated. [23].

Now it needs to show the relation between RSSI and distance, for calculating the received power based on this model, it first calculates the received power at a reference distance using the Friis formula (given in equation (1)). Then, it incorporate the effect of path loss exponent and shadowing parameters.

$$RSSI = -(10 \times \log_{10}(d_{i,j}) - A) \quad [2]$$

Estimated hypothetical space amongs nodes is represented by the following equation given below:

$$d_{ij} = 10^{\frac{RSSI - A}{-10*n}} \quad [3]$$

In which the symbols represent the following factors:
dij as the representative of the estimated distance between node I to node j.
RSSI as the abbreviationo of Receiving Signal Strength Indicator.
“A” symbolizes the amount of power received from reference distance = 1 meter
n: is the transmission factor whose value depends on the propagation environment.
Every node is aware of the distance from their neighbors and able to decide the choice of noce as the nest hop route. This is also visible in the given equation (3)

Power consumption is an important issue for transmitting data via Wi-Fi nodes and this is controlled by the mode of operation and data consumed; by which it can derive the amount of power consumed for transmitting an amount of data during a period of time (t) is presented as follows:

$$E(t) = \sum_j E_j(t_j) + \sum_j \sum_k E_{j,k} \times C_{j,k}(t) \quad (4)$$

Where E (t) is the total energy consumed by the hardware component over the duration t, t =Pjtj, tj is the duration spent in power state j and Ej(tj) is the energy spent during tj. Assuming that Pj , the rate of energy consumption in power state j, is constant during tj, Ej(tj) can be calculated as the product of tj and Pj, Ej,k is the overhead caused by the transition from power state j to k, while Cj,k(t) shows how many times this transition has occurred during t.

The remaining power of each node after transmission of desired data and costs are calculated through the following equation given below. Also, the leftover power is known as Remaining Battery Power (RBP):

$$RBP = \frac{AVLBP - E(t)}{MPB} \quad (5)$$

Where:
RBP : Remaining Battery Power.
AVLBP : Available Battery Power.
E (t) : the total energy consumed by the hardware component over the duration t.
MPB : Maximum Battery Power.

The optimal node should be chosen as an intermediate routing node will be the one with higher RBP after calculating the amount of power will be consumed as described in equation (4).

The RSSI value [24] is calculated with the help of two ray ground model in equation (6):

THE IIOAB JOURNAL
ISSN: 0976-3104

$$P_r(d) = \frac{P_t * G_{t*} G_r * h_t^2 * h_r^2}{d^4 L} \quad (6)$$

P_r : Power received at distance d

P_t : Transmitted signal power

G_t : Transmitter gain (1.0 for all antennas)

G_r : Receiver gain (1.0 for all antennas)

D : Distance from the transmitter

L : Path loss (1.0 for all antennas)

h_t : Transmitter antenna height (1.5 m for all antennas)

h_r : Height of the receiver antenna (All antennas are estimated to be 1.5 m)

NS2 systems adopt RSSI standarized meaurements where the strengths of signals are easured at one node at a time. Assuming that at the point of the simulation, two wireless nodes are at different coordinates. Transmissions are started by one of the nodes, especially Transmission Control Protocols (TCP) and User Datagram Protocol (UDP) packages transferred through a wireless interface, with the provided tramsmitted powers and gains by the antennas. It is propagated through Random way and the threshold for receiver and carier sensitive models. The given thresholds help to define the probable success of receiving packages.

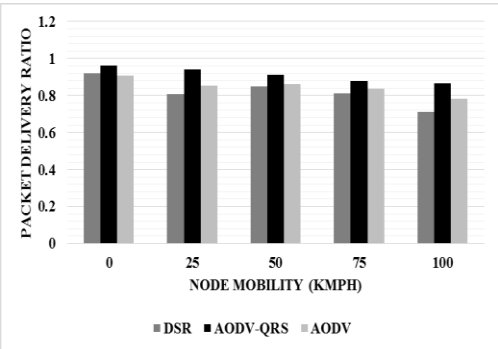
Request Signal Strength (NSS) nodes gain their value from the latest updates and the different between previous and new RSS values differ greatly. Each hop matches new RSS values at fixed intervals with the difference calculated from the Threshold Value (THRS) few link is usually established by this value. After calculations, if any of the parameters is found below the threshold value then the link is considered to be having a breakdown. At this point Possible Route Maintenance Algorithms (PRMA) is considered a solution to fix links between nodes in the midst of a breakdown.

RESULTS

In this section, 80 nodes in 4 sq km. Each node has 250 m range are used. The DSR, AODV-QRS and AODV are evaluated. The Packet Delivery Ratio (PDR), end to end delay in second and number of hops to the destination as shown in **[Table -1], [Table -2], [Table -3]** and **[Figure -1], [Figure -2], [Figure -3]**.

Table: 1. Packet delivery ratio

Node mobility kmph	DSR	AODV-QRS	AODV
0	0.9183	0.9628	0.9074
25	0.8058	0.9422	0.8543
50	0.8486	0.9127	0.8634
75	0.813	0.8783	0.8363
100	0.7127	0.8662	0.7823



THE IIOAB JOURNAL
ISSN: 0976-3104

Fig:1. Packet Delivery Ratio

[Figure- 1] shows how AODV-QRS has higher PDR by 4.73% & 5.92% for 0 node mobility, by 15.6% & 9.7% for 25 node mobility, 7.27% & 5.55% for 50 node mobility, by 7.72% & 4.89% for 75 node mobility and by 19.44% & 10.17% for 100 node mobility when compared with DSR and AODV.

Table: 2. End to end delay in second

Node mobility kmph	DSR	AODV-QRS	AODV
0	0.0015	0.001	0.0015
25	0.002	0.0012	0.0018
50	0.0043	0.0036	0.0039
75	0.0061	0.0045	0.0052
100	0.0189	0.0089	0.0175

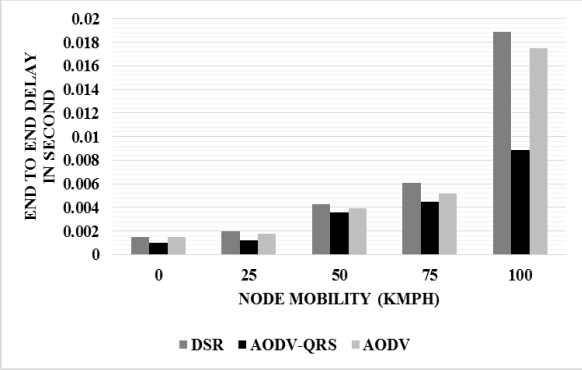


Fig:1. End to End delay in Second

[Figure -1] suggests that AODV-QRS has lower end to end delay in second by 40% & 40% for 0 node mobility, by 50% & 40% for 25 node mobility, 17.72% & 8% for 50 node mobility, by 30.18% & 14.43% for 75 node mobility and by 71.94% & 65.15% for 100 node mobility when compared with DSR and AODV.

Table: 3. Number of Hops to destination

Node mobility kmph	DSR	AODV-QRS	AODV
0	5.2	4.7	4.9
25	6.9	6.6	7.2
50	8.2	6.9	7.8
75	8.4	7.7	8.3
100	9.5	8.7	9.3

THE IIOAB JOURNAL
ISSN: 0976-3104

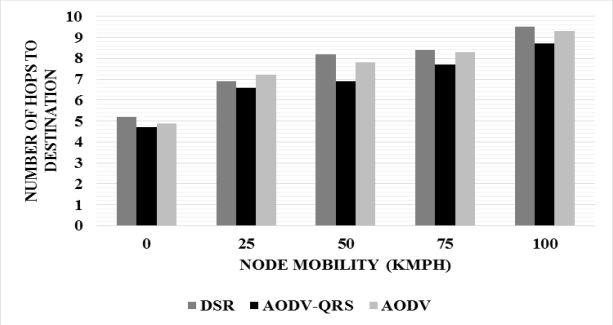


Fig: 2. Number of Hops to Destination

It is obseved from the above **[Figure -3]** that the AODV-QRS has lower number of hops to destination by 10.1% & 4.16% for 0 node mobility, by 4.44% & 8.69% for 25 node mobility, 17.21% & 12.24% for 50 node mobility, by 8.69% & 7.5% for 75 node mobility and by 8.79% & 6.66% for 100 node mobility when compared with DSR and AODV.

CONCLUSION

A MANET contains self-configuring, self-organizing and self-operating nodes, each of them communicates with other nodes directly, without any help of centralized administration or fixed infrastructure, within transmission range of nodes. Due to the quick installation behavior, dynamic configuration, various advantages and different application areas, the field of MANETs is rapidly growing and changing. Although there are still many challenges and issues that need to be faced by the MANET. In order to secure and effective communication within a MANET, an efficient routing protocol is required to discover routes between mobile nodes. The common objective of routing protocol is to provide better efficient energy aware and secure routing schemes to MANET. In this paper, proposed AODV routing protocol and measurement of node mobility using RSSI signal. Experimental results show that the AODV-QRS has higher PDR by 4.73% & 5.92% for 0 node mobility, by 15.6% & 9.7% for 25 node mobility, 7.27% & 5.55% for 50 node mobility, by 7.72% & 4.89% for 75 node mobility and by 19.44% & 10.17% for 100 node mobility when compared with DSR and AODV.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

ACKNOWLEDGEMENT

None

FINANCIAL DISCLOSURE

The authors report no financial interests or potential conflicts of interest.

REFERENCES

[1] Nand P, Sharma DS. Performance Study of Broadcast Based Mobile Adhoc Routing Protocols AODV, DSR and DYMO, *International journal of security and its Applications*, 5(1):53-64.

[2] Aarti DS. [2013] Tyagi, Study of MANET: Characteristics, Challenges, Application and Security Attacks. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(5):252-257.

[3] Bhosle AA, Thosar TP, Mehatre S. [2012] Black-Hole And Wormhole Attack in Routing Protocol AODV in MANET". *International Journal of Computer Science Engineering and Applications*, 2(1):45.

[4] Ade SA, Tijare PA.[2010] Performance Comparison of AODV, DSDV, OLSR And DSR Routing Protocols in Mobile Ad Hoc Networks. *International Journal of Information Technology and Knowledge Management*, 2(2):545-548.

[5] Manikandan SP, Manimegalai R. [2012] Survey on Mobile Ad Hoc Network Attacks and Mitigation Using Routing Protocols. *American Journal of Applied Sciences*, 9(11):1796.

[6] Taneja S, Kush A. [2010] A Survey of Routing Protocols in Mobile Ad Hoc Networks. *International Journal of Innovation, Management and Technology*, 1(3):279.

THE IIOAB JOURNAL ISSN: 0976-3104

[7] Gupta AK, Sadawarti H, Verma AK. [2010] Performance Analysis of AODV, DSR & TORA Routing Protocols. *International Journal of Engineering and Technology*, 2(2):226.

[8] Ahn CW, Chung SH, Kim TH, Kang SY. [2010,]. A Node-Disjoint Multipath Routing Protocol Based on AODV In Mobile Ad Hoc Networks. In Information Technology: New Generations (ITNG), 2010 *Seventh International Conference on IEEE* pp. 828-833.

[9] Venkataraman R, Pushpalatha M, Rama Rao T. [2012] Regression-Based Trust Model for Mobile Ad Hoc Networks. *Information Security*, IET, 6(3):131-140.

[10] Kuppusamy P, Thirunavukkarasu K, Kalaavathi B. [2011] A Study and Comparison of OLSR, AODV And TORA Routing Protocols in Ad Hoc Networks. In Electronics Computer Technology (ICECT), 2011 *3rd International Conference on IEEE* 5:143-147.

[11] Bagwari A, Jee R, Joshi P, Bisht S. [2012] Performance of Aodv Routing Protocol with Increasing the MANET Nodes and its Effects on QoS Of Mobile Ad Hoc Networks. In Communication Systems and Network Technologies (CSNT), 2012 *International Conference on IEEE* , 320-324.

[12] Sarma N, Nandi S. [2010] Route Stability Based QoS Routing in Mobile Ad Hoc networks. *Wireless Personal Communications*, 54(1):203-224.

[13] Moussaoui A, Semchedine F, Boukerram A. [2014]A Link-State QoS Routing Protocol Based on Link Stability For Mobile Ad Hoc Networks. *Journal of Network and Computer Applications*, 39:117-125.

[14] Chatterjee S, Das S. [2015] Ant Colony Optimization Based Enhanced Dynamic Source Routing Algorithm for Mobile Ad-Hoc Network. *Information Sciences*, 295:67-90.

[15] Mohanapriya M, Krishnamurthi I. [2014] Modified DSR Protocol for Detection And Removal of Selective Black Hole Attack In MANET. *Computers & Electrical Engineering*, 40(2):530-538.

[16] Zhao Z, Braun T, Rosario D, Cerqueir E. [2014] CAOR: Context-Aware Adaptive Opportunistic Routing in Mobile Ad-Hoc Networks. *In Wireless and Mobile Networking Conference (WMNC), 2014 7th IFIP (pp. 1-8). IEEE*.

[17] Moussaoui A, Boukeream A. [2015] A Survey of Routing Protocols Based on Link-Stability in Mobile Ad Hoc Networks. *Journal of Network and Computer Applications*, 47:1-10.

[18] Yadav A, Singh, YN Singh RR. [2015] Improving Routing Performance in Aodv with Link Prediction in Mobile ADHOC Networks, *Wireless Personal Communications*, 83(1):603-618.

[19] Amara Korba A, Nafaa M, Salim G. [2013] Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks. In Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference on *IEEE* pp. 693-698.

[20] Su MY. [2010] WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks. *computers& security*, 29(2):208-224.

[21] Yerneni R, Sarje AK. [2012]Secure Aodv Protocol to Mitigate Black Hole Attack in Mobile Ad Hoc. In Computing Communication & Networking Technologies (ICCCNT),2012 *Third International Conference on IEEE* pp.1-5.

[22] Bhalaji N, Shanmugam A. [2012] Dynamic Trust Based Method to Mitigate Greyhole Attack in Mobile Adhoc Networks. *Procedia Engineering*, 30:881-888.

[23] Yasin A, Jabareen S, Al Suqi I. [2014] Enhancing the Connectivity of Mobile Ad-Hoc Networks by Considering the Power, Mobility and Activity of Nodes. *International Journal of Computer Science Issues (IJCSI)*, 11(2):140.

[24] Gupta C, Sharma P. [2014] An Approach to Link Failure in MANET. *International Journal of Computer Science and Network Security (IJCSNS)*, 14(11):108.