**Performance Comparison of MANET Routing Protocols**

*Daniel Elstob*

*Liverpool Hope University*

*14011862@hope.ac.uk*

**Abstract**

Mobile Ad-Hoc Network (MANET), a network in which nodes are able to communicate with each other without an infrastructure or central management. In Ad-Hoc networks how quickly and efficiently a packet can be exchanged between nodes is a primary goal when choosing a routing protocol. This paper will compare two routing protocols Ad hoc On-Demand Distance Vector (AODV), Destination-Sequenced Distance Vector (DSDV) comparing and presenting their performance based on the performance metrics of packet delivery ratio, average delays and throughput. Finally a conclusion will be discussed and the future work will be presented.

**Key Words –** MANET, AODV, DSDV, NS3

**1. Introduction**

In current society wireless mobile points have progressed to be integrated into most infrastructures however they can still be progressed and implemented into locations that lack such an infrastructure either due to a lack of technology constraints or the location has rapid or unpredictable changes. These types of situations could be emergency situations for instance search and rescue operations [1], military operations or crisis management following a major disaster which require a rapid network of communication.

The research goals of this paper are to implement a MANET using AODV and DSDV using different mobility models and carry out simulations to analyse and compare their performance. The simulation will be representative of how these types of networks can be integrated into certain real world scenarios.

This paper will introduce current and related literature in section 2 as well as some security based research that will be referenced to the future work of this paper. In section 3 the methodology of MANET’s in presented explaining the simulation parameter that will be used to implement the simulation. In section 4 the results will be illustrated and a discussion of what they mean before finally concluding the paper in section 5 with the future work of the paper.

**2. Literature Review**

2.1 Related Literature

There have been many research papers that look at how different networking protocols perform when applied to specific scenario, either real world or simulation, or in comparison of other protocols.

One paper that looked at the performance of MANET’s in realistic scenarios and simulations [2] presented a performance study using protocols including but not limited AODV, DSR and OSLR and gave an evaluation of how they performed under specific simulation scenarios based on metrics such as latency of the data packets and the packet delivery ratio. They concluded that overall the superior protocol was AODV beating the others due to its dynamic adaptability.

Another similar paper that analysed the performance of different reactive and proactive protocols [3] focused on the protocols DSR, DSDV and AODV. Similar to [2], [3] also showed that AODV usually outperformed, or was of equal performance to, the other protocols in average end-to-end delay or packet delivery ration however in packet loss it underperformed.

A comparison and analysis of the on-demand and table-driven protocol was made in [4], comparing the data packet delivery and end-to-end delays and showing that in their results that AODV had a lower average end-to-end delay compared to DSDV but that it’s routing load drastically increased linearly with the number of nodes in the network. It was a similar result routing load and the speed of the nodes whereas DSDV remained almost the same.

In [5] they investigated DSR and DSDV and observed that in the simulation area of 500m by 500m by changing the number of nodes the behavior of the protocols changed. The results showed that for metric such as throughput and packet delivery DSR performed better than DSDV. Further work on this paper would be to factor in different constraints such as Number of packets or node speed.

Study into specific or constrained scenario and how a protocol can respond and perform has been evaluated in [6]. The paper looks at two protocols AODV and DSR and the study began knowing that AODV will outperform DSR in a normal situation however in a constrained situation DSR can outperform AODV with observations that there was a 20% difference in degradation. Their work highlighted that local route repair would be important to AODV and proposed improvements.

A comprehensive comparison paper [7] examines AODV, DSDV, ZRP, OLSR and DSR giving a quantitative analysis of which protocols should be chosen for a specific network and/or goal. They compare these five protocols in three different scenarios and conclude that the reactive protocols, AODV and DSR, outperform the proactive in terms of throughput and packet delivery fraction however the proactive protocols, OLSR and DSDV, were the best at average end-to-end delay and network routing load. Similar to most other papers the overall best protocol was AODV, followed by DSR and OLSR, DSDV performed average and the hybrid protocol ZRP performed the worst. In their experiment they noted that for the on-demand protocol such as DSR perform linearly worse as the node speed increases resulting in a longer routing load and drops of packets however work better in small network but not at larger networks. This is due to the inability to get rid of the stale routes unlike a protocol like AODV.

A study proposes a design for a radio dispatch system using MANET [8]. Unlike other research papers that look at the comparative performance of protocols within a scenario, this paper reviews both the technical and financial feasibilities. This goal of the paper was to produce a commercial MANET for a city taxi scenario which unlike conventional networks and the other research papers, has a central origin of messages but uses ad-hoc for communication purposes.

2.2 Security Literature

As MANET can be vulnerable to attack some research adds in security as a factor when creating a simulation such as detection or prevention towards certain types of attacks. Security within a mobile ad-hoc network can be an important factor for instance if the simulation is of a search and rescue operation or military communication where the correct information is needed, then incorrect information being passes between node or dropped is an issue. However in real world implementations this can be a serious problem that few researchers consider when designing simulations.

In the paper [9] they discuss and analyses protocols that aim toward securing routing in MANETS identifying some of the fallibilities and attempt to make future work recommendation to overcome these problems in such a way to secure without adding to the routing load. Three popular types of attacks are that are being researched are blackhole, jellyfish and wormhole.

In the paper [11] they present both blackhole and jellyfish attacks on a MANET simulation by creating both of these through altering the routing protocols and creating their own headers for the attacks. The describe blackhole as an attack that impacts the traffic of the network by redirecting it into a malicious node which discards the received packets or redirects to a nonexistent whereas jellyfish is an attack that is similar to blackhole but when a jellyfish node acquires the packets it slowly starts to either delay or drop within a certain amount of time before resuming to a normal node and forwarding the packets. It is a type of attack that exploits the MANETS packet loss whilst hiding in the network.

A similar attack called greyhole was researched in [10] which similar to blackhole creating a malicious node to drop the packets. They propose a bait detection algorithm that would locate and isolate the malicious node, testing it on different version of a greyhole.

Wormhole on the other hand is essentially a DOS attack that can cause a lot of damage to a network. In the study [12] they implement a new detection technique for wormholes and make a comparison with the current existing techniques. By implementing this approach on various different routing protocols they can show how effective their own detection techniques is specific to the routing protocol chosen and as an overall to the current techniques.

2.2 Summary

One observation from this literature review is AODV tends to outperform all the other routing protocols in was compared to. Another is that with some experiment varying in their use on simulator, result can differ for example an experiment using network simulator 2 can give different result to network simulator 3.

Given that these most of these papers aimed to compare their chosen protocols in real world simulations an area that the research lacked is not taking into account the real world issues such as security, identification and privacy. There have been other more specific research papers such as [4, 5, and 7] that focus completely on the problems as a MANET problem but do not implement or simulate them as real world problems.

The papers that consider the real world situations [1, 2, 3] or the security type research areas [8, 9, 10, 11, 12] are likely the most realistic as they must consider the real world situations or issue that could happen in order to successful simulate them.

**3. Methodology**

3.1 MANET

A MANET is a type of dynamic topology which forms a temporary network. MANET does not require an existing infrastructure because nodes are not fixed to locations with wires and instead move anywhere in the network, as a result it becomes a viable solution to have a form of communication that lacks central management that in certain situations such as a disaster would not have. Additionally with its rapid deployment and self-configuration it can be applied to areas of military, rescue operations or even more tourism type scenarios such as a museum tour.

3.2 MANET Routing Protocols

3.2.1 Reactive Routing Protocols

Reactive protocols are able to through a flooding query create routes dynamically instead of taking the initiative to find routes. AODV is a dynamic routing protocol used in MANETS that is popular due to its adaptability towards highly dynamic topologies and its ability to reduce control overhead however the disadvantages to this protocol are that it has problems with scaling, it is good for small networks however in large networks could perform bad. It also has a large delay that is caused by the route discovery process which becomes more of an issue and the number of node increase. Regardless of these AODV is still a popular and good example of reactive routing which will be used in this paper.

3.2.2 Proactive Routing Protocols

Proactive routes are setup based on controlled traffic with all routes being maintained continuously. DSDV a table-driven protocol, where each node acts similar to a router with a router table which gives DSDV the advantages that it avoids traffic and reducing the routing table, features that could become important in a network however is does have a high wastage of bandwidth and control overhead. DSDV is a popular proactive protocol that will be used in this paper to compare again AODV.

3.3 Mobility Models

3.3.1 Introduction

Depending on the type of situation that the simulation will represent the mobility may change. In this subsection the two mobility models that will be experimented with are the random waypoint and random direction mobility models.

3.3.2 Random Waypoint

Random waypoint is a mobility model where nodes will choose some random speed and random destination and after arriving at the destination the node will pause for a specific time delay and then starts moving again towards the next random destination

This type of mobility model will be a good representation of student moving around at a campus each node going to its own waypoint i.e. a student going to class.

3.3.3 Random Direction

The random direction is intended to be an improvement to the random waypoint discussed in 3.3.2 as an attempt to overcome the issue of node clustering in a part of the simulation. In random direction the nodes will move at specified speed and random direction, pausing for specific delays before moving again. If the node meets the bounds of the model the node will bounce off and continue in another direction until simulation end.

This type of mobility model will be a good representation of a search operation, for instance if police needed to search an area for any evidence they can select an area of movement, stopping occasionally to examine the surrounding and then move again until they hit the boundaries of their search space or the search is finished.

3.4 Simulation Tool

For this simulation analysis we have used Network Simulator 3 a C++, open source discrete event network simulator targeted primarily for networking research and educational purposes.

Table 1 Simulation Parameters

|  |  |
| --- | --- |
| Simulation Parameters | Values |
| Protocols | AODV, DSDV |
| Simulation Area (m) | 500 by 500 |
| Simulation Time (s) | 30 |
| Mobility Model | RandomWaypoint, RandomDirection2d |
| Node Speed | 20 |
| Packet Size | 1024 |
| Each Node Sends | 100 |
| Number of Nodes | 50, 150, 250 |
| Data Rate (Mbps) | 1, 3, 5 |

3.5 Performance Metrics

To evaluate the performances of routing protocols performance metrics can be used. Here we discuss the following metrics of packet delivery ratio (PDR), average delays and throughput.

3.5.1 Packet Delivery Ratio

PDR is the percentages of packets actually received at their destination compared to how many were sent and can be shown in the equation (1) where PDR is Packet Delivery Ratio, RP is the Received Packet, NP is Number of Packets and NN is Number of Nodes.

(1)

3.5.2 Average Delays

Average end-to-end delays are the amount of time taken for a packet to go from the source to destination and can be calculated using the equation (2) where AD is Average Delay, TD is Total Delay and RP is Received Packets.

(2)

3.5.3 Throughput

This measurement is the performance value of how well data is provided to its destination within the network and can be shown in the equation (3) where T is Throughput and RP is Received Packets and PS is Packets Sent.

(3)

**4. Results**

4.1 Introduction

In this section we present the simulation results for a scenario, the protocol and performance metrics Packet Delivery Ratio (Figures 1, 2, 3), Average Delay (Figures 4, 5, 6), and Throughput (Figures 7, 8, 9).

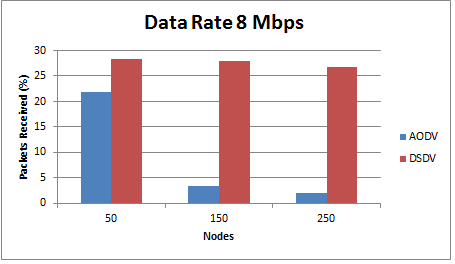


Figure Packets Receive 8 Mbps

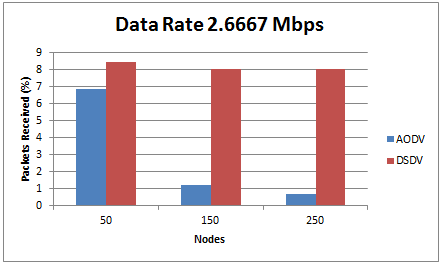


Figure Packets Receive 2.6667 Mbps

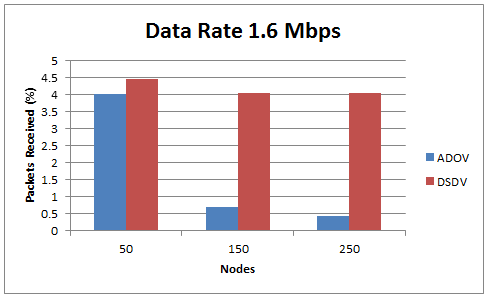


Figure Packets Receive 1.6 Mbps

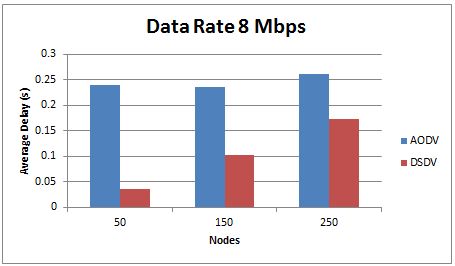


Figure Average Delay 8 Mbps

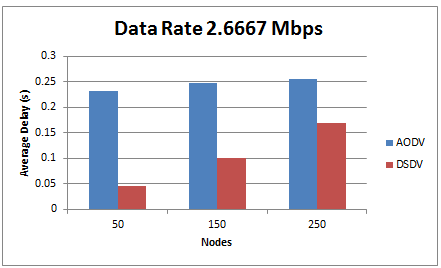


Figure Average Delay 2.6667 Mbps

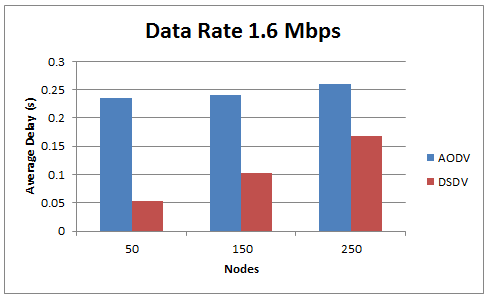


Figure Average Delay 1.6 Mbps

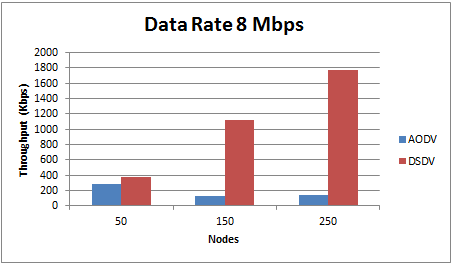


Figure Throughput 8 Mbps

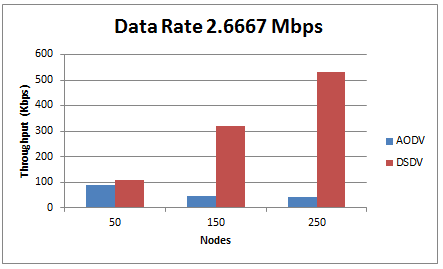


Figure Throughput 2.6667 Mbps

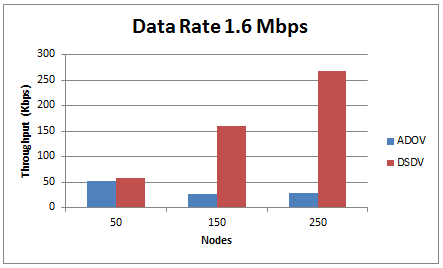


Figure Throughput 1.6 Mbps

4.2 Packet Delivery Ratio (PDR)

In this section we examine the communication reliability for different group sizes. We measure the PDR. The PDR is the percentage from the sent messages that were actually delivered and represents how reliable the communication is. The higher the PDR, the better the communication reliability is. Furthermore the different group sizes determine how heavy the traffic is because it defines how many the senders there are. We use three different group sizes (50,150, 250 nodes) the higher the number of nodes the heavier the traffic is. We will see how the different speed values affect the communication.

From Figures 1, 2 and 3 DSDV performs the best overall. At 50 nodes both AODV and DSDV are fairly equal with DSDV being the better. However once the number of node increases to 150 and 250 AODV drastically worse at 150 and worse again at 250 whereas DSDV slightly decreases at a data rate of 8 Mbps and for 2.6667 and 1.6 Mbps the results are equal.

4.3 Average Delay

In this section we examine the average delay between the two protocols. We measure how long the end-to-end delay between messages is and give and overall average.

From Figures 4, 5 and 6 DSDV is shown to outperform AODV. AODV has a high average delay starting 50 nodes and increased linearly as the node do. DSDV on the other hand performed best at small networks and also increases linearly with network size.

4.4 Throughput

In this section we examine the throughput of the network. Throughput is the amount that can be processing within the time frame. Therefore as the amount of nodes increase so should the threshold for the throughput to ensure that all messages can be sent and shows a good performance of the network.

From Figures 7, 8, and 9 both protocols have fairly equal results at 50 nodes however once the number of node increases DSDV greatly outperforms AODV.

4.4 Conclusion of Results

4.4.1 Mobility Modes

Two mobility models have been implemented, the Random Waypoint and the Random Direction in order to investigate whether the mobility model will have an impact of the result for the two chosen protocols. The results shown in the figures were the same for both mobility models for both of the protocols.

4.4.2 Routing Protocols

The two routing protocols that have been implemented are AODV and DSDV. The result of PDR, average delay and throughput show that in small networks AODV can perform satisfactory however networks that will have a high density or heavy traffic implementing DSDV would be the preferable routing protocols.

Overall this shows that DSDV is the preferable routing protocol to implement in shown in the figures this could be a result of its ability to reduce the amount of space and avoid traffic compared to AODV which has problems with scaling, has shown it is good for small density of networks but performs poorly in larger networks. This is contradictory to most of the literature review which for the majority expressed AODV to be the superior routing protocol. This could be a result of different simulators or simulation parameters however from this study it is concluded that DSDV is the superior protocol within in the performance metrics taken.

**5. Discussion**

5.1 Introduction

In this paper we have presented the MANET protocols AODV and DSDV as possible solutions. In 5.3 the possible future work will be introduced and discussed.

5.3 Future Work

5.3.1 Realism

The scenario script could be expanded to include a more realistic simulation instead of simple making a comparative analysis of how two protocols and two mobility models work under different number of nodes and data rates. This could be expanded to have exact values for a type of situation, for instance if the simulation was to represent a rescue operation where node much find a specific node or a military operation where they nodes must find a malicious node.

5.3.2 Security

If we focus future work on an implementation similar to the military operation and given the security issues stated previously in 2.2 adding in a feature to detect any malicious activity or designing and implementing a malicious node within the MANET could be a possible research project. In order to implement this in ns3 would mean altering the routing protocol file code as these codes are not implemented yet. It would also mean creating a header file for the malicious code. Depending on the choice of attack type would be important depending on the type of situation being simulated.

**6. References**

[1] I.A. Tøndel, M.G. Jaatun, and Å.A. Nyre, “Security requirements for manets used in emergency and rescue operations”. In Security and Communication Networks (IWSCN), 2009 Proceedings of the 1st International Workshop on, 2009.

[2] S. Singla, and S. Jain, 2014, July. “Performance Comparison of routing protocols of MANET in real world scenario using NS3”, In Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on (pp. 543-549). IEEE.

[3] J. Hsu, S. Bhatia, M. Takai, R. Bagrodia, and M.J. Acriche, “Performance of mobile ad hoc networking routing protocols in realistic scenarios”, Proceedings of IEEE conference on military communications, Vol. 2, pp. 1268-1273, 2003.

[4] N.S Yadav, and R.P. Yadav, “Performance comparison and analysis of table-driven and on-demand routing protocols for mobile ad-hoc networks.”, International Journal of Information Technology, 4(2), pp.101-109, 2007.

[5] S.S Tyagi, and R.K. Chauhan, “Performance Analysis of Proactive and Reactive Routing Protocols for Ad hoc Networks”, International Journal of Computer Applications, Vol. 1, No. 14, pp. 27-30, 2010.

[5] R. Singh, D.K. Singh, and L. Kumar, “Performance Evaluation of DSR and DSDV Routing Protocols for Wireless Ad Hoc Networks” International Journal Advanced Networking and Applications, Volume: 02, Issue: 04, pp: 732-737, 2011.

[6] R. Misra and C.R. Manda1, “Performance Comparison of AODV/DSR On-demand Routing Protocols for Ad Hoc Networks in Constrained Situation”, ICPWC, 2005

[7] T. Bhatia, and A.K. Verma, “QoS Comparison of MANET Routing Protocols.”, International Journal of Computer Network and Information Security (IJCNIS), 7(9), p.64, 2015.

[8] E. Huang, W. Hu, J. Crowcroft, and I. Wassell, “Towards commercial mobile ad hoc network applications: A radio dispatch system.”, InProceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (pp. 355-365). ACM, 2005, May.

[9] S. Gupte, and M. Singhal, “Secure routing in mobile wireless ad hoc networks.”, Ad Hoc Networks, 1(1), pp.151-174, 2003.

[10] R.H. Jhaveri, and N.M. Patel, “A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks.”, Wireless Networks, pp.1-18, 2015

[11] N. Purohit, R. Sinha, and K. Maurya, “Simulation study of Black hole and Jellyfish attack on MANET using NS3.”, In Engineering (NUiCONE), 2011 Nirma University International Conference on (pp. 1-5). IEEE, 2011.

[12] G. Mathur, R.K. Singh, and M.V. Raju, “Implementation and Comparison of a New Wormhole Detection Technique with Existing Techniques”, IOSR Journal of Computer Engineering Volume 16, Issue 3, Ver. VI, PP 84-91, 2014.