# Evaluating the Performance of Routing Protocols In Mobile Ad-hoc Networks

**K. Vijayalakshmi**[1]
[1]Research Scholar, Department of Computer Science, NGM College, Pollachi, India.
Email: viji92.km@gmail.com
**Dr. R. Manicka Chezian**[2]
[2] Associate Professor, Department of Computer Science, NGM College, Pollachi, India.
Email: chezian_r@yahoo.co.in

----------**ABSTRACT**---------- **Mobile ad hoc network (MANET) is a special type of mobile wireless network where a collection of mobile devices form a temporary network without any aid of an established infrastructure. During data transmission between these devices there may be malicious threats, attacks, and penetrations which alters the performance of the system and insecure transmission. Multiple routing protocols especially for these conditions have been developed to find optimized routes that free from attacks from a source to some destination. .We have used NS2 simulator from scalable networks to perform the simulations. NS2 is a discrete event driven packet level network simulator. This provides insight into ad hoc routing protocols (DSDV, AOMDV) and their metrics (Throughput, end to end delay, Packet loss) using NS2. The performance differentials are analyzed using varying metrices. These simulations are carried out using the ns-2 network simulator.This paper presents comparison based on simulation of routing protocol of MANET.**

**Keywords—AOMDV,DSDV,MANET,METRICS,NS2.**

---

## 1. INTRODUCTION

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the assistance of any centralized administration or any stand-alone infrastructure.Its consists of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and omni-directional antennae. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their messages, which effectively builds connected networks among the mobile hosts in the deployed area administration.Many security schemes from different aspects of MANET have been proposed in order to protect the routing information or data packets during communications,[1] such as secure routing protocols , we investigate the performance and efficiency of three representative protocols for Mobile Ad hoc Networks, we have chosen the secure protocols that fall under the most significant categories. Our simulation scenarios have been designed as to capture how different categories of MANET protocols cope with typical dynamic conditions and according to different scalability factors.

## 2 .RELETED WORK

### 2.1 Characteristics

In MANET,eachnode actas both host and router.that is it is autonomous in behavior

1.Multi-hop radio relaying When a source node and destination node for a message out of the radio range.the MANETs are capable of multi-hop routing.

2.Distributed nature of operation for security routing and host configuration. A centralized firewall is absent here.

3.The node can join or leave the network anytime,making the network topology dynamic in nature.

4.Mobile nodes are characterized with less memory, power and light weight features. Mobile and spontaneous behavior which demands minimum human intervention to Configure the network.

5.The reliability, efficiency,stability and capacity of wireless links are often inferior when compared with wired links.this shows the fluctuating link bandwidth of wireless links.

### 2.2 Applications

With the increase of portable devices as well as progress in wireless communication, ad-hoc networking is gaining importance with the increasing number of widespread applications. The set of applications for MANET is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources.

2.2.1MilitaryBattlefield: Military equipment now routinely contains some sort of computer equipment. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, military information headquarters.

2.2.2Commercial Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement.

2.2.3Local Level:Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at e.g. conference or classroom. Similarly in other civilian environments like

taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.

2.3 Security in Mobile Ad Hoc Networks:

Wireless mobile ad hoc nature of MANET brings new security challenges to network design. Mobile adhoc networks, due to their unique characteristics, are generally more vulnerable to information and physical security threats than wired networks or infrastructure-based wireless networks. In this chapter, we explore the various security requirements (goals) for wireless ad hoc network and the different types of threats an ad hoc network faces. [2]We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication.

2.3.1 Security Goals:To secure an ad hoc network, a security protocol must satisfy the following attributes: confidentiality, integrity, availability, authenticity and non-repudiation.

2.3.2 Confidentiality:Ensures:That classified information in the network is never disclosed to unauthorized entities. Sensitive information, such as strategic military decisions or location information requires confidentiality. Leakage of such information to enemies could have devastating consequences.

2.3.3Integrity:Guarantees that a message being transferred between nodes is never altered or corrupted. Data can be altered either intentionally by malicious nodes in the network or accidentally because of benign failures, such as radio propagation impairment or through hardware glitches in the network.

2.3.4 Availability:Implies that the requested services (e.g. bandwidth and connectivity) are available in a timely manner even though there is a potential problem in the system. Availability of a network[5] can be tempered for example by dropping off packets and by resource depletion attacks.Authenticity is a network service to determine a user's identity. Without authentication, an attacker can impersonate any node, and in this way, one by one node, it can gain control over the entire network.

2.3.5 Non-repudiation:Ensures that the information originator cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes.

mentioned characteristics causes difficulty in providing security in ad hoc wireless network is given below.

## 3.ROUTING IN MOBILE AD HOC NETWORKS

Most of the routing protocols are designed for wired and structured network. It is often very hard to adopt these protocols for ad hoc network. Routing mechanism is used to forward packet from source to destination using most efficient path. Efficiency of the path is measured by using various metrics traffic load, delay, packet delivery ratio.Three types of topology based routing

1. **Proactive (table-driven) routing protocols**
2. **Reactive (on-demand) routing protocols**
3. **Hybrid routing protocols**

There is three types of topology based routing the categorization of these routing protocols shown in Fig1

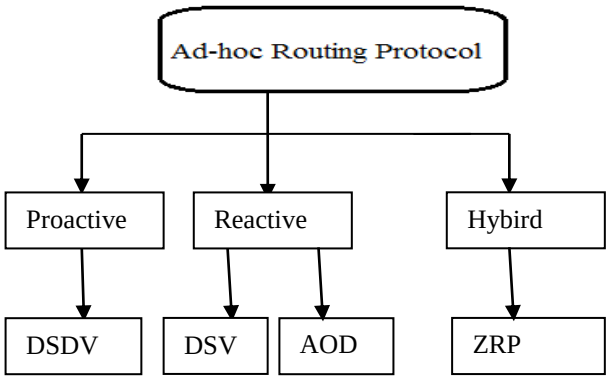


**Fig 1: Categorization Of Ad-hoc Routing Protocols**

3.1 PROACTIVE ROUTING PROTOCOLS

In table-driven or proactive protocols, the nodes maintain an active list of routes to every other node in the network in a routing table. The tables are periodically updated by broadcasting information to other nodes in the network such as the Destination Sequenced Distance Vector routing protocol(DSDV).

3.2 REACTIVE ROUTING PROTOCOLS

In contrast to table driven routing protocols, on- demand routing protocols find route to a destination only when it is required. The on-demand protocols have two phases in common – route discovery and route maintenance. In the route discovery procedure, a node wishing to communicate with another node initiates a discovery mechanism if it doesn't have the route already in its cache. [3] The destination node replies with a valid route. The route maintenance phase involves checking for broken links in the network and updating the routing tables. One of the most popular reactive protocol is Ad hoc On-demand Distance Vector routing protocol (AODV).

3.3 HYBRID ROUTING PROTOCOLS

Hybrid routing protocols inherit the characteristics of both on-demand and table-driven routing protocols. Such protocols are designed to minimize the control overhead of both proactive and reactive routing protocols. The best example of hybrid routing protocols is the Zone Routing Protocol (ZRP).

3.3.1AOMDV: means Ad-hoc on-demand multipath distance vector routing.AOMDV is the extension of AODV protocol to discover the multiple paths between source and destination. Multiple paths in the AOMDV are loop-free and disjoint. AOMDV has three benefits when compared to other on demand protocols. • It does not have high inter-nodal coordination. • It ensures disarticulation of alternate routes via distributed computation without the use of source routing. • It computes alternate paths with minimal additional overhead it does this by exploitingalready available alternate path. In AOMDV when a source wants to communicate with the destination firstiinitiates a route discovery process by sending a RREQ packet. The RREQ packet transmission from the source to destination establishes a multiple reverse paths. The RREQ first sets up a reverse path to the source using the previous hop values of the RREQ. It is the next hop to the[4] node in the reverse path. If the route is valid then the intermediate node generates a route reply packet otherwise RREQ is rebroadcast. Each entry in the routing table consists of,

• All available destinations
• Next hop towards each destination
• No of hops required to reach destination
• A destination sequence number
Routing table for Node1 represent for Fig2

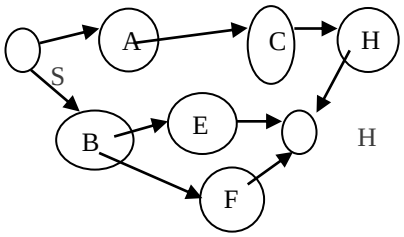


**FIG2: Routing table 1**

**Table1: Routing for node 1**

| AOMDV | | | |
|---|---|---|---|
| NODE'S ROUTING TABLE | | | |
| Destination | Next node | Hops | Sequence number |
| D | A | 4 | 11 |
| D | B | 3 | 11 |

3.3.2DSDV: DSDV is a proactive routing protocol it is extension of bellman-ford routing algorithm .[6] In DSDV each node maintains a routing table consists of entries for all the nodes within the network. The routing table updates periodically when the topology changes are detected.[7] Each node sends the broadcasting message to its neighboring nodes and updates the packets. After receiving packet the neighboring node updates their routing table with incrementing the metric by one and it retransmit the update packet to all its neighbors. The will be repeated until all the nodes in the network receives a copy of the update packet with a corresponding metric. The route selection will be done basing on three steps,

• The update information will be compared to its own routing table.
• Select route with higher destination sequence no.
• Select route with better metric when sequence no's are equal. Routing table for Node2 shown in fig3.

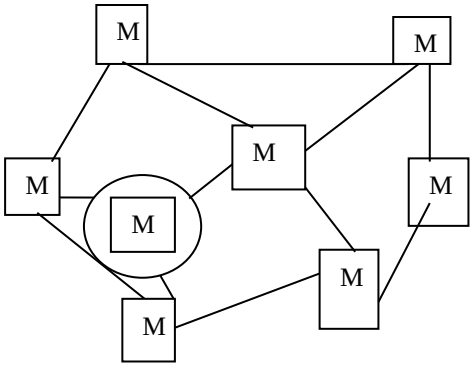


**FIG3: Routing table 2**

**Table2: Routing for node2**

| Destination | Next hop | Metric | Sequence |
|---|---|---|---|
| 1 | 1 | 1 | 123 |
| 2 | 0 | 0 | 516 |
| 3 | 3 | 1 | 212 |
| 4 | 4 | 1 | 168 |
| 5 | 4 | 2 | 372 |
| 8 | 1 | INF | 432 |

**4.NETWORK SIMULATOR**

Simulator is nothing but giving exogenous inputs to the system and it will study the behaviour of the inputs an d generate the results. [9,10]Ns2 is discrete event simulator targeted at networking research. It provides generous support for simulation of TCP, UDP, routing and multicast protocols over wired and wireless networks. It consists package of tools to simulate the behaviour of different networks. Now current version of ns is ns-2. It includes scripting languages, new network protocols, evaluate performances much better. Ns-2 is event driven packet level network simulator. It acts as a simulation tool for Linux journal. It creates network topologies log events that happen under any load and analyse events to understand the network behaviour. Languages used in ns2 are TCL, c, c++. TCL is used as a scripting language where c and c++ as a programming language used for coding purpose. Components used in NS-2 are Network animator (NAM). It is used to observe the behaviour of the network, simulator. Advantages: Find sum bugs in advance Overview over analytic techniques Detail Can simulate system details at arbitrary levels.

| Parameter | Value |
|---|---|
| Simulation | NS-2.35 |
| MAC type | 802.11 |
| Protocols | DSDV,AOMDV |
| No.of.nodes | Omni antenna |
| Simulation area | 1660m*2550m |

**Table 3:Simulation parameter**

4.1 Packet Delivery Ratio (PDR)
The ratio of the data packets delivered to the destination to those generated by CBR sources. This metric illustrates the effectiveness of best effort routing protocols. This performance measure also determines the completeness and correctness of the routing protocol. If P is fraction of successfully delivered packets, N is total number of flows, f is id, R is packets received from f and T is transmitted from f, then F can be determined by,

$$F = 1/N \sum_{f=1}^{c} Rf / Tf$$

It has been found that in all cases perform better than AOMDV and DSDV in packet delivery ratio. Fig. 4 shows the throughput in packet delivery ratio for 100 nodes.
4.2 Throughput
It is the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to

get the last packet. When comparing the routing throughput by each of the protocols, EPRDSR has the high throughput. It measures of effectiveness of a routing protocol. The throughput values of DSR, MTPR and EPRDSR protocols for 50, 75 and 100 nodes at pause time 10,20,30,40 and 50s and they are plotted on the different scales to best show the effects of varying throughput of the above routing protocols as shown fig. 1, 2 & 3. Based on the simulation results, the throughput value of DSR decreases initially and reduces when the time increases.

4.3 End-to-End delay Average end-to-end delay is the delay experienced by the successfully delivered packets in reaching their destinations. This is a good metric for comparing protocols. This denotes how efficient the underlying routing algorithm is, because delay primarily depends on optimality of path chosen

.

$$\textit{Average End to End delay} = 1/S \sum_{i=1}^{s} (ri - si)$$

where S is number of packets received successfully, ri is time at which packet is received and si is time at which it is sent, i is unique packet identifier. Simulations have been conducted for 100 nodes.

**Table 4 : Results of DSDV and AOMDV**

| Protocols | Metrics | 50 nodes | 75 nodes | 100 nodes |
|---|---|---|---|---|
| AOMDV | Through put | 538.80 | 715.26 | 535.52 |
| | End to end deley | 110.334 | 131.794 | 138.193 |
| | Packet loss | 120 | 104 | 128 |
| DSDV | Through put | 880.23 | 765.30 | 870.74 |
| | End to end deley | 120.476 | 103.677 | 136.552 |
| | Packet loss | 76 | 139 | 91 |

Three different simulation network parameters are performed to calculate the performance of these routing protocols. Throughput,,End to End Delay and PacketLoss These are calculated with AOMDV shown in chart.

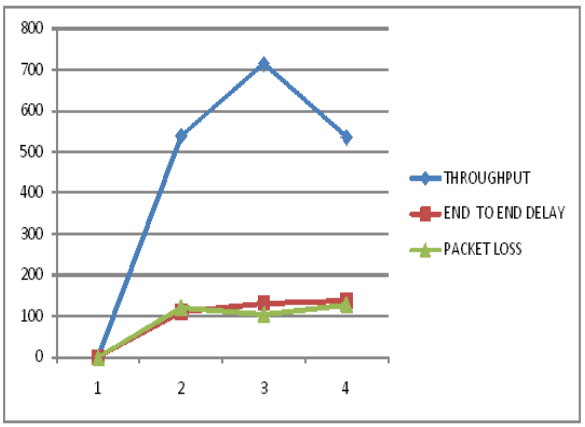


**FIG4:AOMDV (50,75,100 nodes)**

Throughput,,End to End Delay and PacketLossThese are calculated with DSDV shown in chart.

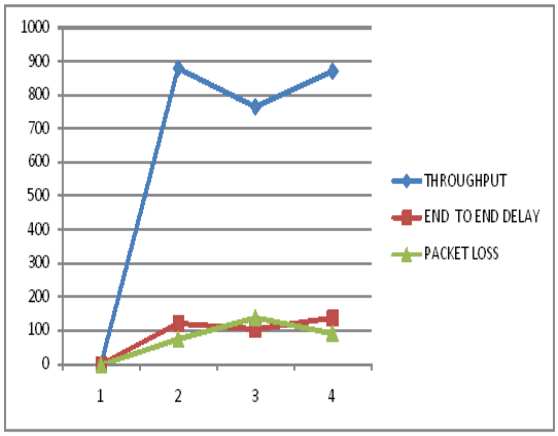


**FIG5:DSDV (50,75,100 nodes)**

## CONCLUSION

The two most important issues in mobile ad hoc networks are the performance and security. Each mobile node in a MANET acts as a router by forwarding the packets in the network. Hence, one of the challenges in the design of routing protocols is that it must be tailored to suit the dynamic nature of the nodes.In this paper we have compared two routing protocols AOMDV, DSDV. The simulation of these protocols has been carried out using NS-2 simulator. [8]Three different simulation network parameters are performed to calculate the performance of these routing protocols. Taking the three metrics for comparison we have concluded that in case of packet loss, End-to-End delay and throughput DSDV showed better results than AOMDV.

## REFERENCES

[1] karthika.M, Dr. R. Manicka Chezian ,Survey On Ad-hoc In Wirelesssensor Networks,International Journal in ComputerEngineering&Technology(IJARCET)Volume1,issue 5,july 2012 pp270-273.

[2]Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad-hoc Networks, in Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000), pp 275–283, August 2000.

[3]Anandhi.R, Dr. R. Manicka Chezian, Local Greedy Distributed Spanning Tree Routing by Reducing Local minima in higher dimensional Space,International Journal Of Innovative Research in Computer and CommunicationEngineering(IJIRCCE)Volume2,Issue8,August2014

[4] K.Vijayalakshmi, Dr. R. Manicka Chezian "A Study On Security Consideration In MANET". National Confrence on Emerging Trends In BigData Analytics, FEB,2015, ISBN 97893 80800417.

[5] "Different Types of Attacks on Integrated MANET-Internet Communication," International Journal of Computer Science and Security (IJCSS) Volume.4, no 5,pp.181-190Dec 1996.

[6] Nishu Garg and R.P.Mahapatra, "MANET Security Issues ," IJCSNS International Journal of Computer Science and Network Security, Volume.9 No.8,August 2009. (MobiCom 2000), ACM Press, 2000, pp. 255–265.

[7] Imad Aad, Jean-Pierre Hubaux and Edward W. Knightly, Denial of Service Resilience in Ad Hoc Networks, in Proceedings of the 10th annual international conference on Mobile computing and networking, pp 202–215, Philadelphia, PA, 2004.

[8] Nitin H. Vaidya,"Mobile Ad Hoc Networks: Routing, MAC and Transport Issues", University of Illinois at Urbana-Champaign,(IEEE International Conference on Computer Communication). INFOCOM 2004, july pp81-94.

[9] Haas Z.J, " A new routing protocol for the reconfigurable wireless network". In Proceedings of the 1997 IEEE 6th International Conference on Universal Personal Communications, ICUPC '97, San Diego, CA, October 1997; pp. 562 -- 566.

[10] Jeroen Hoebeke, Ingrid Merman, Bart Dhoedt and Piet Demeester ―An Overview of Mobile Ad Hoc Networks: Applications and Challenges‖ session4. http://ciemcal.org/manet-and-routing-techniques/

[11] Mahesh K. Marina and Samir R. Das ―On-demand Multipath Distance Vector Routing in Ad Hoc Networks‖ Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/wcm.432

[12] Vivek B. Kute, M. U. Kharat ―Analysis of Quality of Service for the AOMDV Routing Protocol‖ published on ETASR - Engineering, Technology & Applied Science Research Vol. 3, _o. 1, 2013, 359- 362.

[13] P. O. Tariq, F. Greg & W. Murray, "On the Effect of Traffic Model to the Performance Evaluation of Multicast Protocols in MANET", Proceedings of the Canadian Conference on Electrical and Computer Engineering, pp. 404–407, 2005.

[14] The Network Simulator NS-2 tutorial homepage, http://www.isi.edu/nsnam/ns/tutorial/index.html