Comparative Analysis of OLSR and AODV under IPv6 Environment

Amritbir Singh
Punjabi University Regional Center For Information Technology And Management Mohali

ABSTRACT

Due to the inherent property of mobile ad hoc network, nodes in this environment move arbitrarily or illogically. Due to the mobility of nodes the topology changes dynamically. As routing of data in such dynamic topology is an important issue in mobile ad hoc network, so the selection of suitable routing protocol is necessary which enables to route data between mobile nodes efficiently by using less bandwidth of the network. Each routing protocol has its own architecture and working. Routing protocols behave differently under different environments. Thus, it is necessary to analyze the behavior of different routing protocols under different environments. Many studies have been done on the performance evaluation of routing protocols of MANET, but most of these studies are based on IPv4. On the other hand, IPv6 gains popularity because it has some additional features over IPv4 as it supports multicasting, multi-homing, efficient routing. IPv6 is more secure as compared to IPv4 and has large address space to support. On account of these features of IPv6, many organizations are moving to use IPv6, and therefore, it is worthwhile to evaluate the performance of routing protocols under IPv6 environment**.** In this research performance of two ad hoc routing protocols OLSR and AODV evaluated under IPv6 environment on the basis of end-to-end delay, throughput, and network load. The objective of this research is to investigate how these routing protocols behave under IPv6 environment and identify which routing protocol performs better. OPNET Modeler 14.5 is used as simulation tool. On the basis of simulations we conclude that OLSR performs well which proves that it is suitable for efficient routing.

General Terms

Mobile Ad Hoc Network, Routing Protocols, Internet Protocol Version 6

Keywords

AODV, MANET, OLSR, OPNET

1. INTRODUCTION

Mobile Ad Hoc Network is a type of wireless network in which collection of mobile nodes form a network without any fixed architecture or prior organization. Mobile ad hoc network gains popularity because it is easy to deploy infrastructure less through their dynamic nature. Mobile ad hoc network is self-creator, self-organizer and self-administrator network. In mobile ad hoc network nodes move arbitrarily so topology in mobile ad hoc network may change frequently. Study of the routing protocols of mobile ad hoc network is an area of research since past two decades. Many routing protocols have been studied and new routing protocols are proposed. Routing of data packets efficiently to mobile nodes in the absence of pre defined infrastructure are major problem in mobile ad hoc networks. There is always a need in mobile ad hoc network to search a good path for the routing of data packets from source to destination. In mobile ad hoc network every mobile node acts as a host and as a router. Due to the limited transmission range of wireless networks, multi-hops are needed to exchange data packets between source to destination in network. Bandwidth, energy, physical security and other resources are limited in mobile ad hoc network. Congestion in network may arise due to the limited bandwidth of mobile ad hoc networks and to avoid this problem efficient routing in mobile nodes is essential.

2. ROUTING PROTOCOLS IN MANET

On the basis of properties mobile ad hoc routing protocols are divided into two types:

- Reactive Routing Protocols
- Pro-active Routing Protocols

A. Reactive Routing Protocols

Reactive routing protocol is a type of routing protocol in which route is established when it is needed by source node to send data packets to the destination node. In reactive routing protocol flooding technique is used for route discovery. Once routes are discovered the routes are stored and maintained in route cache. The main advantage of this type of routing protocols is to save precious bandwidth of ad hoc network.

AODV:AODV is a type of reactive protocol in which route is created when it is needed. In AODV, the routing table stores the information about the next hop to destination and sequence which it gets from destination. This is to avoid problem of loop of messages and to retain the freshness of the information received. In discovery of the destination node information about active nodes is received. If the route breaks, the neighbors can be notified. Four types of control messages are used. The RREQ message is used to make request for route when a source node wants to communicate with destination node. RREP message is sent by destination node to source node in response to RREQ message. This means the destination node is alive and connection is fresh. The RERR message is sent to neighbors when link is broken. RREP-ACK message is sent by destination to source when acknowledgement option is selected.

B. Proactive Routing Protocols

Proactive is a type of routing protocol in which each node maintains routing information of every other node in a network. In proactive routing protocol routing information is kept in routing tables and updated when topology is changed. The main advantage of this type of routing protocols is that nodes get the route information immediately and establish a session.

OLSR: OLSR is a type of table-driven pro-active link state routing protocol developed for mobile ad hoc network. OLSR exchange information with other nodes in the network .In OLSR the concept multi point relay (MPR) is used to reduce control traffic overhead. In OLSR nodes elect MPR among themselves. MPR is transmitting the control messages on the behalf of other nodes in the network. Each node in a network has a list of MPR nodes. The OLSR is suited for large and dense networks. MPR helps in providing the shortest path to destination. Different types of control messages are used in OLSR. Hello messages are used to find link status information and host's neighbors. Topology Control (TC) messages are used for broadcasting information about own advertised neighbors which includes at least the MPR selector list. Multiple Interface Declaration (MID) messages are used to inform other nodes that announcing node may use multiple OLSR interface. Host and Network Association (HNA) messages are used to provide external routing information and giving the possibility of routing to external addresses.

3. INTERNET PROTOCOL

Internet protocol is a primary communication protocol which is used to send data packets from source to destination node in network. Data is transmitted in the form of data gram.

Fragmentation is a technique which is used to send large datagram in network in it large datagram is divided into small data packets that can easily be transmitted in the network, because every network link has limited size for messages transmission in a network which known as maximum transmission unit (MTU). Datagram is used to send large amount of data. Datagram structure is defined by internet protocol and data is which is encapsulated in these datagram is sent from source to destination.

Internet Protocol is connectionless protocol so there is no guarantee of delivery of data. Internet Protocol has two versions, namely, Internet Protocol Version 4 and Internet Protocol Version 6. Internet protocol version 4(IPv4) is a widely used protocol which was deployed by Internet Engineering Task Force(IETF) in early 1990. IPv4 has 32 bits address space and is able to provide 4,294,467,294 addresses[5].Some addresses are reserved for special purposes and are not available for public use. IPv4 is more prone to network attacks because no encryption and authentication is used. IPSec which is responsible for secure routing is optional in IPv4. IPv4 header format is complex and not easy to understand. IPv4 supports Quality of Service(QoS) but it relies on 8 bits type of service(TOS) field and identification of payload.IPv4 type of service(TOS) has limited functionality and payload identification is not possible when the IPv4 packet is encrypted. IPv4 address space is divided into five types of classes A, B, C, D, E, in which addresses of A,B,C are available for public use but address of class D is reserved for multicasting operations and class E address is reserved for future research and experimentation. This may lead to the problem of address exhaustion. Address exhaustion problem of IPv4 provides a base for IPv6's recent growth amongst the internet users, since IPv4 is unable to fulfill the demand of internet users. Due to address depletion problem of IPv4 mobile nodes are unable to obtain IP address from regional address registries to connect to the internet. So the need of new Internet Protocol arose, which could be fulfilled by IETF in year 1999 with the deployment of IPv6 which is also known as Internet Protocol for next generation (IPng). IPv6 has 128 bits address space and is able to provide approximately 3.4×10^{38} addresses.IPv6 and also it is more secure as compared to IPv4 because several encryption and authentication techniques like ESP are used. IPSec is mandatory in IPv6. IPv6 uses flow label mechanism so router easily recognize where to send information. IPv6 header size is 40 bytes and so, it is simple and small in size as compared IPv4. IPv6 supports multicasting and multi- homing, efficient routing which is not supported by IPv4 [2]. On the basis of the above discussion we conclude that internet protocol version 6 is the future internet protocol and the future internet technology depends on IPv6. Therefore, it is necessary to evaluate the performance of these routing protocols under IPv6. This can help us if immediate shifting from IPv4 environment to IPv6 environment is required.

4. RELATED WORK

In[4],the author compares two routing protocols AODV and OLSR on the basis of various parameters like performance and scalability,security,resource usage and has drawn the conclusion about AODV and OLSR, and on the basis of this study and has suggested the appropriate routing protocol which is suitable under different situations. In[14],the author explains the working of OLSR under IPv4 and IPv6 and explains the header information and basics of OLSR in IPv4 and IPv6. In[6], the author explains the implementation of OLSR routing protocol and study various extensions of OLSR routing protocol. In[7], the author explains how mobility is affected by the two mobile ad-hoc routing protocols. In this study, he first compares the two routing protocols under static condition linear fashion, and then under mobility. This helps to know how rapid changes in topology may affect routing protocols.

5. SIMULATION TOOL

Discrete Event Simulation software OPNET Modeler 14.5 is used in this study. OPNET is commercial network simulator used widely to design heterogeneous networks like ad hoc networks. OPNET is a graphical user interface based network and so it is easy to use . OPNET incorporates a number of features to support an increase stability and mobility in the mobile ad-hoc network. A number of routing parameters of MANET are supported by OPNET Modeler and so it is easy to design network in OPNET Modeler and to evaluate the performance of these routing protocols. These parameters are known as performance metrics. Specific application and transport layer protocols demand their own set of performance metrics to evaluate the network efficiency. In this study, the performance of these routing protocols is evaluated on the basis of three parameters network load, end-to-end delay and throughput. Performance of these routing protocols is evaluated for the selection of efficient routing protocol in this communication network. The parameters used in this study are summarized below in Table 1:

Table 1 : Parameters of Simulation

Parameters	Value
Number of Nodes	10,15,20
Maximum Speed	10 m/s
Simulation Time	10 minutes
Pause Time	60 sec
Environment Size	4000X4000
Packet Size	50000 bytes
Traffic Type	FTP
Packet Rate	11Mbps

6. PERFORMANCE METRICS

1.End-To-End Delay: End-To-End Delay is the average time that take by a data packet to reach its destination. This metric is calculated by subtracting time that first packet take to traverse the network from time at which first data packet arrived to destination. This is a time the generate data packet by sender and it received by receiver at destination in application layer and it is measured in seconds. All delays in network is cause by node mobility, packet retransmission and due to weak signal strength between nodes connection tearing and its making is also be included. Applications like voice requires a low average delay in network but other applications like FTP may be lenient to delay at certain level. This metric is more significant in understanding the delay introduced by path discovery.

2.Network Load: Network load represents the bit/sec load submitted by all higher layers in all WLAN nodes of the network to wireless LAN layers. When more traffic is coming on the network it is difficult for network to cope up with this heavy load of traffic it is called network load. The efficient network should cope up with this heady traffic load and provide best network infrastructure and many techniques are used for this. Heavy load on network may affect mobile ad hoc networks the data packets may collide this increases congestion on the network and makes the routing process slow.

3.Throughput: It is ratio of total amount of data transfer from sender to receiver and the time it takes for the receiver to receive last packet of data from sender. In other words we say that it calculates how constantly data is provided by network to receiver. Throughput is the number of data packets arriving at the receiver per milliseconds.

7. SIMULATION AND PERFORMANCE ANALYSIS

Simulation process is divided into different scenarios. We use 10, 15 and 20 randomly deployed nodes under campus network environment of 4000X4000 square meters. The FTP high load traffic is used. The file size is 50,000 bytes. Every node moves with constant speed of 10 m/s with 60 seconds pause time. Mobility between nodes is based on random waypoint mobility model. All nodes are defined as workstations with one WLAN server. WLAN connection speed is 11 Mbps The simulation time is 10 minutes.

In this paper we evaluate the performance of two ad hoc routing protocols OLSR and AODV under IPv6 environment on the basis of three parameters, that is, end- to-end delay, network load and throughput.

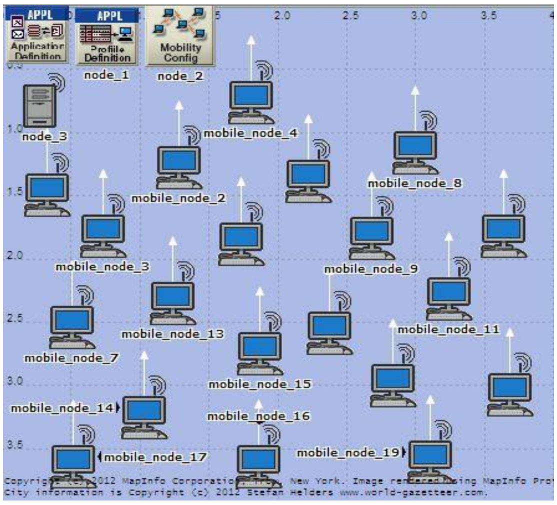

Figure 1:Simulation Scenario Having 20 Nodes

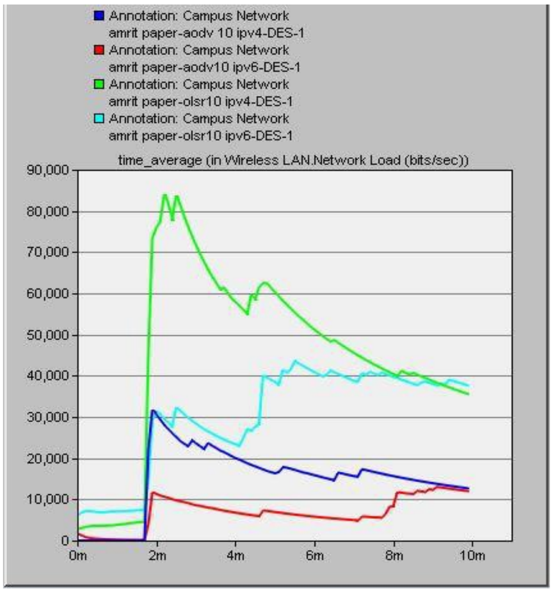

Figure 2: Network Load for 10 Nodes

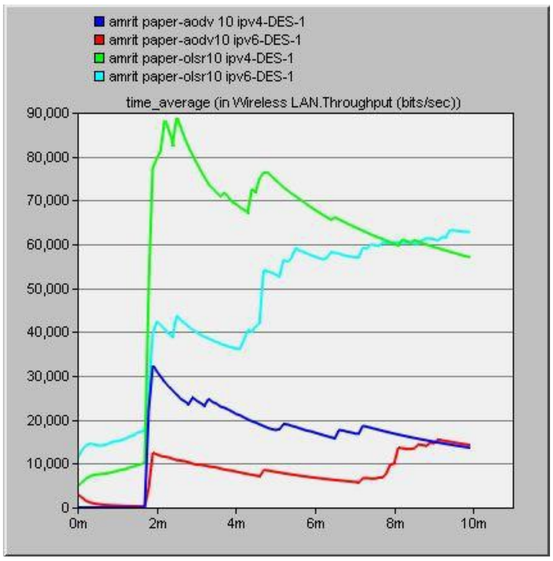

Figure 3: Throughput for 10 Nodes

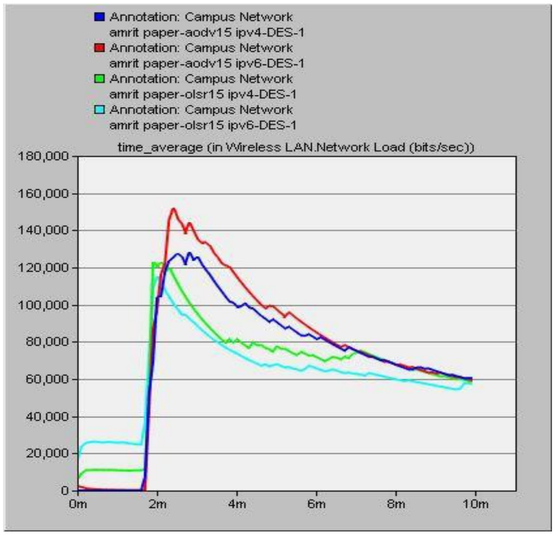

Figure 4: Network Load for 15 Nodes

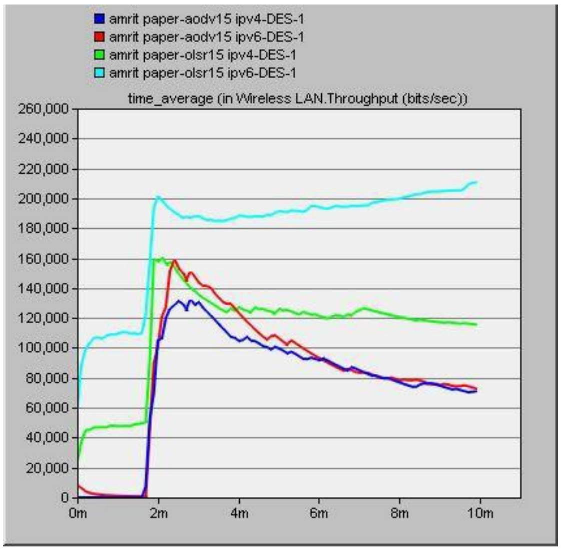

Figure 5: Throughput for 15 Nodes

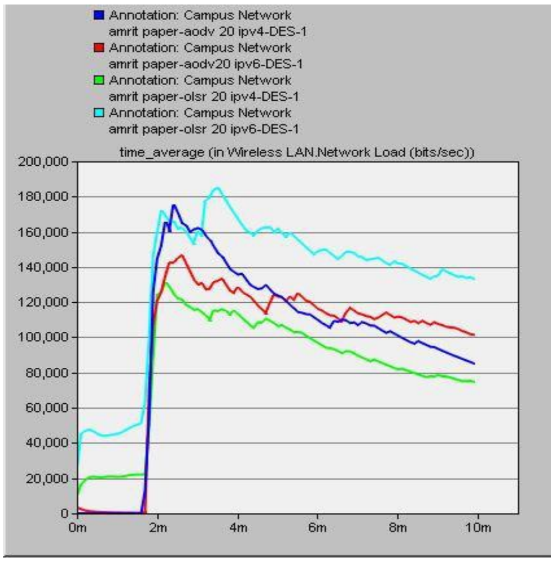

Figure 6: Network Load for 20 Nodes

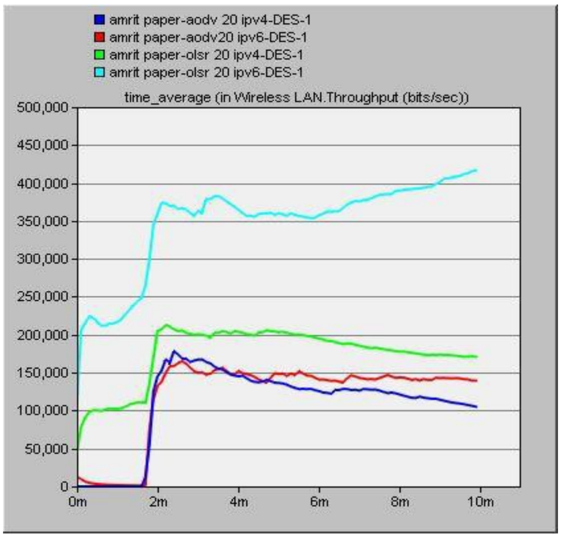

Figure 7: Throughput for 20 Nodes

Table 2 : Resultant Values

Nodes	Protocol	IP Version	Delay(sec)	Network Load(bits/sec)	Throughput (bits/sec)
10	AODV	IPv4	0.005509	420213	421952
10	AODV	IPv6	0.004661	288922	301605
10	OLSR	IPv4	0.008013	784282	774805
10	OLSR	IPv6	0.005984	595728	616709
15	AODV	IPv4	0.004653	860277	863904
15	AODV	IPv6	0.005348	920149	941882
15	OLSR	IPv4	0.005037	1440309	1448826
15	OLSR	IPv6	0.004625	814490	890378
20	AODV	IPv4	0.004089	1476474	1474698
20	AODV	IPv6	0.005541	1324709	1384938
20	OLSR	IPv4	0.003759	834608	903194
20	OLSR	IPv6	0.005593	1029557	1227296

8. CONCLUSION

In this research we tested two routing protocols of mobile ad hoc networks OLSR and AODV under IPv6 environment. On the basis of observation, we say that OLSR performs better in terms of end-to-end delay and throughput, whereas AODV shows good results in terms of network load. Thus we conclude that OLSR performs better as compared to AODV. However, it is not necessary that OLSR always perform better the results may vary by varying networks.

9. REFERENCES

[1] Clausen T, Jacquet P "Optimized Link State Routing Protocol(OLSR)" IETF RFC 3626 October 2003

[2] Deering S,Hinden R "Internet Protocol Version 6" IETF RFC 2460 December 1998

[3] Deering S,Hinden R "Internet Protocol Version 6" IETF RFC 1883 December 1995

[4] Huhtonen A,"Comparing AODV And OLSR Routing Protocols" Helsinki University of Technology Sjökulla, 2004-04-26

[5] Internet Protocol DAPRA IETF RFC 791 September 1981

[6] Jacquet P,Muhlethaler P,Clausen T,Laouiti A,Qayyum A.,Viennot L."Optimized Link State Routing Protocol For Ad Hoc Networks"Proc.5th IEEE Multi Topic Conference INMIC 2001 pp.62-68,2001

[7] Kumar Tanuja," Performance Evaluation Of AODV And OLSR Under Mobility" Rutgers University, 2009

[8] Laouti A,Muhlethaler P,Najid A,Plakoo E,"Simulation Results Of OLSR Routing Protocol For Wireless Network",INRIA,2002

[9] Perkins C.E and Royer E.M "Ad-Hoc On Demand Distance Vector Routing", Mobile Computing Systems and Applications Proc. IEEE Workshop Mobile Computing Systems & Applications(WMCSA 99) pp. 90-100, 1999

[10] Perkins C.E,Royer E.B,Das S "Adhoc On Demand Distance Vector(AODV) Routing" IETF RFC 3561 July 2000

[11] Perkins Charles E ,Royer Elizabeth M,Das Samir R,"Ad Hoc On Demand Distance Vector(AODV) Routing For IP Version 6",IETF DRAFT,10 November 2000

[12] Perkins Charles E ,Royer Elizabeth M,Das Samir R,"Ad Hoc On Demand Distance Vector Routing", IETF DRAFT,22October1999

[13] Tonnesen Andreas "Implementing And Extending Optimized Link State Routing Protocol",Deptt. of Informatics,University of OLSO,2004

[14] Wakikawa Ryuji ,Tuominen A J,"OLSR For IPv6(OLSR6)" OLSR Interop and Workshop 2004, San Diego CA USA, 2004/8