Performance Analysis of DSR, AODV and DYMO Protocols, Quality of Service Issues and Security in MANET

ArunKumar B. R.
Professor & HOD, MCA Dept.
BMS Institute of Technology
Doddaballapura Main Road
Bangalore, Karnataka, India

Gautam Sharma
Student, Department of MCA
Sir MV Institute of Technology
Bangalore, Karnataka, India

ABSTRACT

Applications of mobile ad hoc networks (MANET) are expected in wide varieties of area in spite of several constraints and challenges. MANET characteristics such as dynamic infrastructure arrangement, high level of heterogeneity, mobile nodes and hence dynamic topology, energy constraints, unreliable communication and security have posed a lot of challenges. The quality of service routing is a crucial factor in such an MANET environment. To optimize the routing algorithms, it is most important to evaluate the performance of the routing protocols, identify the research issues in connection to quality of service (QoS) with proper justification and to explore the security requirements in MANET. This work evaluates the performance analysis of on-demand routing protocols and certain QoS issues pertaining to routing protocols and the security.

Keywords: *MANET, Quality of Service (QoS), Throughput, End-end Delay, Dynamic Source Routing (DSR), Dynamic MANET on-demand, Ad-hoc on demand distance vector (AODV), Security attacks,*

1. *INTRODUCTION*

A mobile ad-hoc network (MANET) is composed of mobile platforms without predetermined infrastructure, nodes are free to move arbitrarily and self-organize to form a network over radio links. The key majority of applications of MANETs are focused on the areas where wire-line networks are not appropriate and rapid deployment and dynamic configuration are crucial. Such applications include military battlefields, emergency search and rescue sites, audio-video conferencing and sharing text/images dynamically using their mobile devices, etc.

These applications involve group-oriented multicast computing without restrictions on number and mobility of members. The majority of the routing protocols proposed in the literature are striving towards the optimization of routing performance and extremely vulnerable to malicious nodes present and the types of attacks that happens on MANET.

The multicasting in ad-hoc networks is a promising research area that requires considerable further study. In the literature survey, there are several quality of service multicast protocols proposed for MANET such as work in [24]. The analysis of the protocols on standard simulation tool such as QualNet is required which facilitates to design an adoptable mechanisms for the routing protocols. Thus, the work focuses on performances characteristics of the on-demand protocols namely AODV, DSR and DYMO which are considered necessary to be evaluated and analyzed in proper context so that the usefulness and the enhancement can be recognized.

This paper is organized as follows: Section 2 presents relevant literature survey on certain routing issues. Brief note of the on demand protocols is discussed in Section 3. The simulation experiment set up and performance comparison of the protocols are detailed in Section 4. The Section 5 explores the security in MANET and finally, Section 6 passes the concluding remarks.

2. *QoS ROUTING ISSUES*

The quality of service of the routing protocols inherently contributes to the performance of the MANET with the real time traffic such as conversational voice, videoconferencing and real time multimedia. It makes sense to get into the technological perspective of both application and network to control the jitter, to optimize the bandwidth utilization , ensure connectivity, monitor network partition, alert on the congestion and notification, admission control [1][2][3] and [4].

Further, the type of the traffic of the network media such as best effort traffic, bursty traffic or bulky traffic generated by the application type can affect the QoS the network offers. Bursty nature of the network media traffic leads to dynamic resource allocation and utilization which calls for additional resources demand and increase in the cost of time. It should be noted that burst traffic of data leads to challenges in resource management which is scarce in MANET and effects the quality of service [5][6][7]. Therefore traffic management mechanism are highly essential for streaming in MANET.

Transfer of media under stringent delay constraint is the characteristic of the streaming media[11]. Hence internet protocol (IP) with “Best Effort service Model” cannot be directly extended to MANET.

TCP which is a dominant and prominent protocol in the internet adopts congestion control mechanisms only after the congestion starts signaling in the network. In addition to this, It is to be noted that TCP fairly shares link bandwidth between multiple connections [11]. This may leads to MANET to collapse if the same basic TCP mechanism is adopted. TCP queuing mechanisms such as First-In First Out (FIFO) or Drop Tail method is not suitable for the scaling up in internet, wireless networks and for heterogeneous type of networks environment.

Packet Loss Analysis (PLA) is an important research issue in case of digitized audio transmission over a network in a series of packets where the receiver has to produce the original audio signal. Since all the packets have to be received with preserved timing relationships among them which is challenging in case of MANET because of node mobility, dynamic topology and connectivity, etc. PLA gains importance as the research issue in MANET.

This literature analysis summarizes and up holds that network traffic type, traffic models such as best effort service model of IP, Congestion control mechanisms and PLA are the key research issues in MANET routing apart from the issues identified in [22]. The issues of the layers other than the network layer have to be adopted by the MANET routing protocol by employing cross layer paradigm to offer the QoS routing.

3. *ON DEMAND ROUTING PROTOCOLS*

In this paper, the brief note of the on demand protocols studied are presented along with the many references to other related works.

3.1 Ad-Hoc on-Demand Routing (AODV)

The Ad hoc On-Demand Distance Vector (AODV) routing protocol belongs to the class of distance vector routing protocol (DVR) which is intentional for use by mobile nodes on demand basis in an ad hoc network. AODV is capable of both unicast and multicast routing. AODV multicast tree connects group members and tree is maintained as long as it is required by the source. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network [8]. It uses destination sequence numbers to ensure loop freedom at all times(even in the face of anomalous delivery of routing control messages),avoiding problems (such as "counting to infinity") associated with classical distance vector protocols. The security is very crucial in mobile communication. The basic AODV has no definition of security mechanisms.

3.2 Dynamic Source Routing (DSR)

The Dynamic Source Routing protocol (DSR) is a simple yet efficient on demand protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. The DSR protocol offers guaranteed loop-free routing, takes care of operation in networks containing unidirectional links, scalable up to two hundred nodes and works efficiently even with high rates of mobility [9].

3.3 Dynamic MANET On-demand Protocol (DYMO)

DYMO is the extension of Ad-Hoc on-demand Distance Vector routing protocol. It is reactive protocol with basic operations namely route discovery and management. It ensures loop free routing using sequence numbers. It’s mechanisms can swiftly get adaptation to dynamic conditions, low processing and memory overhead, low network utilization, and determines unicast routes between nodes within the network [10].

4. CONFIGURATION OF PARAMETERS FOR SIMULATION EXPERIMENT

A simulation is a powerful tool to test the implementation of the research ideas, scale the network easily, consumes less time to incorporate the changes, and it is cost effective. However the accuracy of the results of the real world experiments are not necessarily be correlated and it is clearly independent of the implementation accuracy of the models in the simulator.Many research papers have presented the simulation studies of AODV using an event-driven, packet level simulator, called PARSEC. including Charles. C. Perkins et al of Sun Microsystems Laboratories [6][24].

QualNet is a network simulation tool that simulates wireless and wired packet mode communication networks. QualNet developer is a discrete event simulator used in the simulation of MANET, WiMAX networks, satellite and sensor networks. QualNet is a commercial tool derived from GloMoSim that was first released in 2000 by Scalable Network Technologies.

To carry out the performance evaluation of AODV, DSR and DYMO Protocols on QualNet simulator, the parameters are set which are shown in the Table 1 and Table 2 below. The simulations experiments are carried out for the same set of parameters configuration to evaluate the performance of AODV, DSR and DYMO. A scenario where nodes random and distributed in 1500 X 1500 unit area is shown in Figure 1 where the entire area is further divided into 100 square shaped cells and 1kb of constant bit rate (CBR) data was transmitted in the simulation as shown in the Figure 2. The packet reception model was set to IEEE 802.11b using the parameter in QualNet as,'PHY802.11bReceptionModel' as shown in the Figure 3. Figure 4 shows configuring to enable IP forwarding. The property, routing IPV4 has set to the value AODV, DSR and DYMO while evaluating them, an example set up is shown in Figure 5. The Figure 5 also shows other properties set to carry out the simulation experiment. The simulation scenario set for DSR and DYMO with mobility are shown in the Figure 6 and 7 respectively.

The physical Layer : The basic hardware transmission technologies of the network are consisting in the physical Layer. Because of different variants in hardware technologies and their characteristics, the physical layer is very complex one [15]. Each router has *a priori* knowledge only of networks attached to it directly. A routing protocol shares the topological information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network [16].

Fading Model: In wireless systems, fading may either be due to multipath propagation, referred to as multipath induced fading, or due to shadowing from obstacles affecting the wave propagation, sometimes referred to as shadow fading [17]. The fading may vary with time, geographical position or radio frequency, and is often modeled as a random process.

The performance of the protocols is evaluated based on throughput. Throughput is the average rate of successful data packets received at destination. It is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second. Evaluation of the performance of the simulated protocols in terms of throughput is as follows: Throughput (bits/sec) of the DYMO, AODV and DSR protocols are 564, 375 and 232 respectively. It should be noted that DYMO protocol has performed high compared to AODV and DSR. DSR performance is low compared to DYMO and AODV.

5. **SECURITY IN MANET ROUTING**

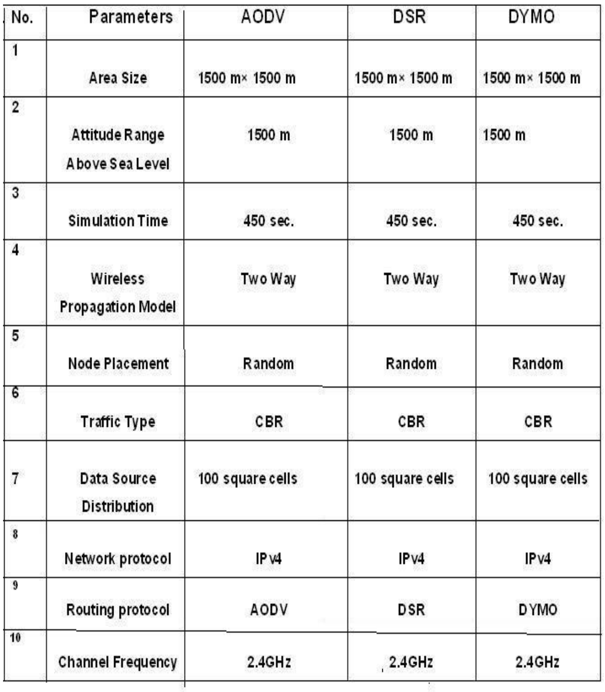
In MANET addition to traditional attacks, network specific attacks have offered a lot challenges to researchers. Security-sensitive applications need to be safeguarded in terms of the attributes such as availability, confidentiality, integrity, authentication, and non-repudiation [20]. The routing protocols without security mechanisms may degrade the network performance. The nature of MANET expects efficient security mechanisms as wireless channel is accessible to both legitimate network users and malicious attackers. The security solutions should take care of the network in it's entirety and each node. The mechanism proposed should work on each device proportional to the resources available within the device such as energy, memory, connectivity and computing capability [18]. To secure the MANET, solution should prevent, detect and react with the network in order to safeguard the system from collapse. Misbehaving nodes degrades the network performance. It is required to be alert always to monitor the malicious nodes and initiate the necessary proper actions if any anomaly is detected. Hence an intrusion detection system (IDS) is essential in MANET. There are protocols that address active attacks such as worm whole attacks [12][13]. For achieving confidential group communication using a symmetric key which is shared by all the nodes for data encryption, Sencun Zhu et al proposed an efficient approach in [14]. A malicious neighbor node may prevent other neighbor nodes from getting fair share of the transmission channel [18]. The distributed zone based secure routing protocol for MANET is proposed in [25] which introduces local and global authority servers.

The security is a major issue as recommended by ITU-T [23] in ad hoc networks. Majority of the routing protocols have used standard digital signatures to authenticate routing update messages. it is worth reiterating that generation and verification of digital signatures is relatively inefficient [19]. All the security attacks leads to either low performance or network collapse. Therefore, security issue has to be considered as an integral characteristic of the routing protocol especially in group communication where they involve more nodes [21].

6. CONCLUSION

In this research endeavor, the work highlights that the issues at other layers which are not considered traditionally with the routing protocols such as network traffic, congestion control etc. are recommended to be adopted in the design of the routing protocol following the cross layer paradigm. The performance analysis of the simulated protocols on QualNet developer recognizes the DYMO as a high performance protocol compared with AODV and DSR for the identical scenarios. It is worth noting that a large no. of research papers have evaluated the protocols in absence of security attacks including the performance comparison of DSR, AODV and DYMO protocols. Security is an essential requirements for both unicast and multicast routing. In the context of multicasting secure concerns increases.

Table 1. Simulation Parameters



No.	Parameters	AODV	DSR	DYMO
1	Area Size	1500 m× 1500 m	1500 m× 1500 m	1500 m× 1500 m
2	Attitude Range Above Sea Level	1500 m	1500 m	1500 m
3	Simulation Time	450 sec.	450 sec.	450 sec.
4	Wireless Propagation Model	Two Way	Two Way	Two Way
5	Node Placement	Random	Random	Random
6	Traffic Type	CBR	CBR	CBR
7	Data Source Distribution	100 square cells	100 square cells	100 square cells
8	Network protocol	IPv4	IPv4	IPv4
9	Routing protocol	AODV	DSR	DYMO
10	Channel Frequency	2.4GHz	2.4GHz	2.4GHz

Table 2. Configured Parameters

Configured Parameters	Values
Physical Layer Protocol	802.11
Routing protocol	AODV,DSR, DYMO
Fading Model	Rayleigh
Shadowing Model	Constant
Energy Model	Mica Motas
Battery power	Simple Linear
Area	1500X1500
Mobility	Random way point
Mobility Speed	0-30mps
Data Link Layer	802.11.DCF
Application Layer	CBR Traffic
Channel Frequency	2.4 GHz
Total Power	1200ma
Antenna Model	Omni Directional Antenna
Enable IP Forwarding	Yes

The simulation experiment is carried out with the network density of 10 nodes, packet size of 512 Bytes, Radio Range of 100m, link capacity of 2Mbps, Pause Time of 2 seconds, Max. No. of packets buffered= 100 for the simulation time of 450 seconds.

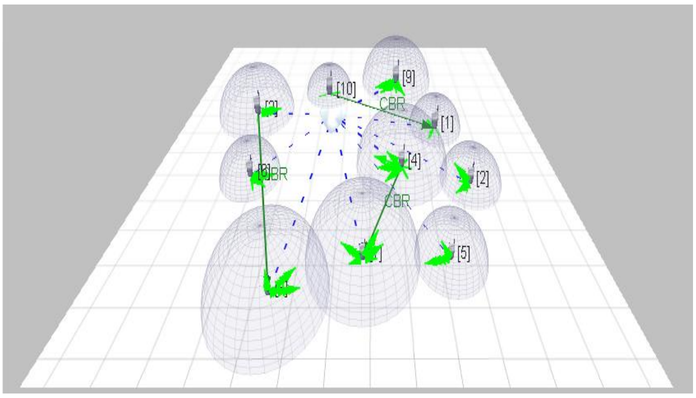


Figure 1.Setting of 10 MANET nodes for simulation on QualNet developer.

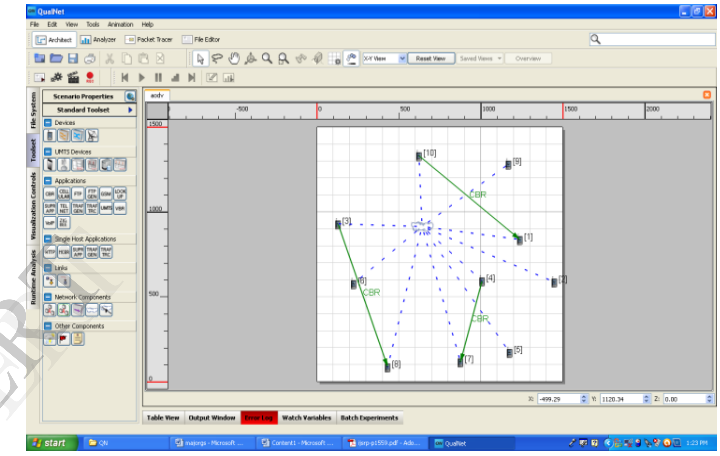
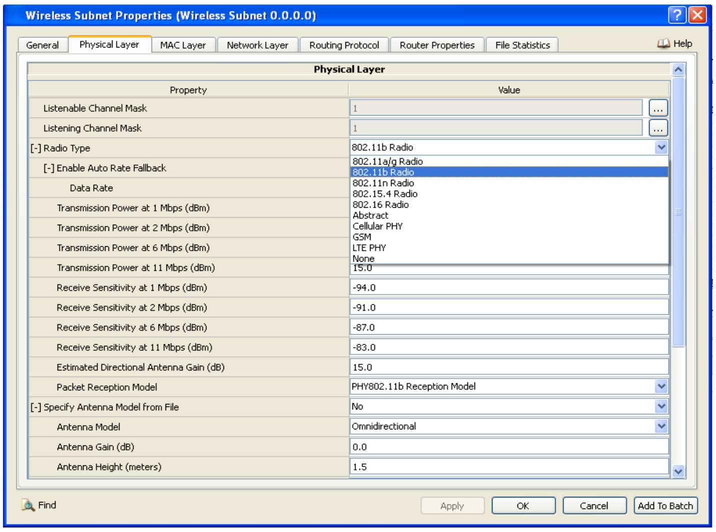


Figure 2 . MANET nodes with CBR of one Kb data.



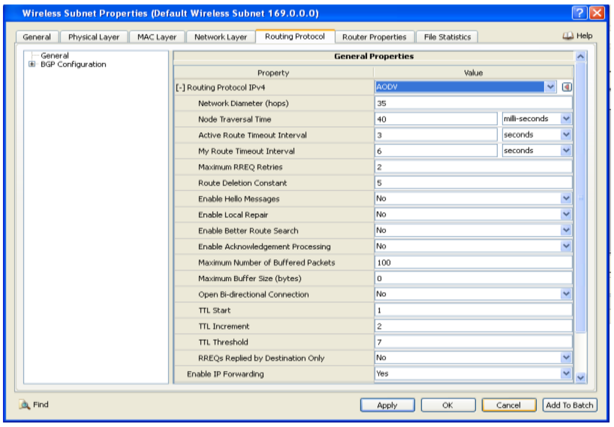
Wireless Subnet Properties (Wireless Subnet 0.0.0.0)

General | Physical Layer | MAC Layer | Network Layer | Routing Protocol | Router Properties | File Statistics | Help

Physical Layer

Property	Value
Listenable Channel Mask	1
Listening Channel Mask	1
[-] Radio Type	802.11b Radio
[-] Enable Auto Rate Fallback	
Data Rate	
Transmission Power at 1 Mbps (dBm)	
Transmission Power at 2 Mbps (dBm)	
Transmission Power at 6 Mbps (dBm)	
Transmission Power at 11 Mbps (dBm)	15.0
Receive Sensitivity at 1 Mbps (dBm)	-94.0
Receive Sensitivity at 2 Mbps (dBm)	-91.0
Receive Sensitivity at 6 Mbps (dBm)	-87.0
Receive Sensitivity at 11 Mbps (dBm)	-83.0
Estimated Directional Antenna Gain (dB)	15.0
Packet Reception Model	PHY802.11b Reception Model
[-] Specify Antenna Model from File	No
Antenna Model	Omnidirectional
Antenna Gain (dB)	0.0
Antenna Height (meters)	1.5

Figure 3. Configuring the Packet Reception Model on the Physical Layer

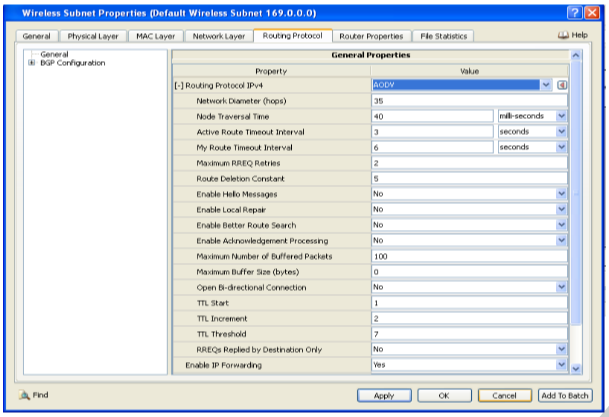


Wireless Subnet Properties (Default Wireless Subnet 169.0.0.0)

General Properties

Property	Value
[-] Routing Protocol IPv4	AODV
Network Diameter (hops)	35
Node Traversal Time	40 milli-seconds
Active Route Timeout Interval	3 seconds
My Route Timeout Interval	6 seconds
Maximum RREQ Retries	2
Route Deletion Constant	5
Enable Hello Messages	No
Enable Local Repair	No
Enable Better Route Search	No
Enable Acknowledgement Processing	No
Maximum Number of Buffered Packets	100
Maximum Buffer Size (bytes)	0
Open Bi-directional Connection	No
TTL Start	1
TTL Increment	2
TTL Threshold	7
RREQs Replied by Destination Only	No
Enable IP Forwarding	Yes

Figure 4. Enabling IP Forwarding in AODV



Wireless Subnet Properties (Default Wireless Subnet 169.0.0.0)

General Properties

Property	Value
[-] Routing Protocol IPv4	AODV
Network Diameter (hops)	35
Node Traversal Time	40 milli-seconds
Active Route Timeout Interval	3 seconds
My Route Timeout Interval	6 seconds
Maximum RREQ Retries	2
Route Deletion Constant	5
Enable Hello Messages	No
Enable Local Repair	No
Enable Better Route Search	No
Enable Acknowledgement Processing	No
Maximum Number of Buffered Packets	100
Maximum Buffer Size (bytes)	0
Open Bi-directional Connection	No
TTL Start	1
TTL Increment	2
TTL Threshold	7
RREQs Replied by Destination Only	No
Enable IP Forwarding	Yes

Figure 5. Setting IPV4 for AODV

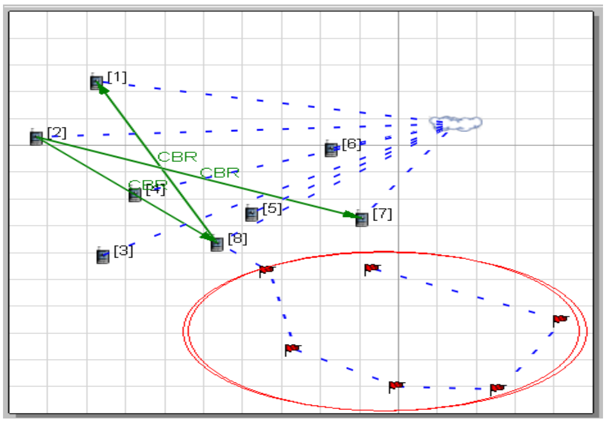


Figure 6. DSR Nodes with Mobility

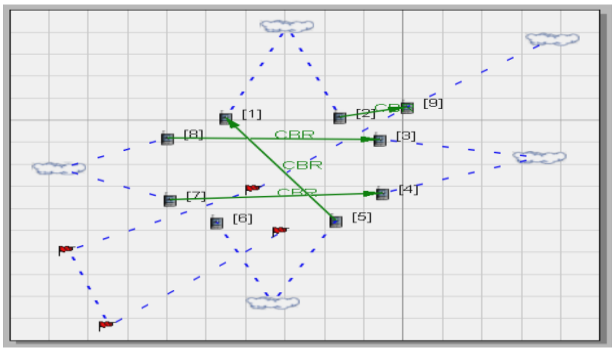


Figure 7. Simulation scenario set for DYMO with Mobility and CBR

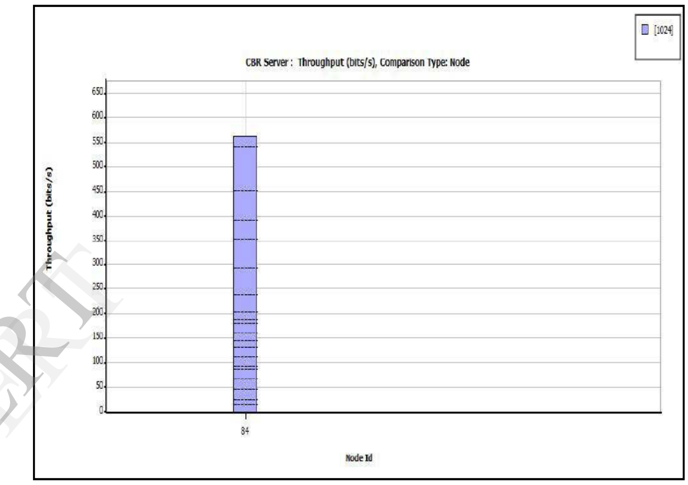


Figure 8. Throughput of DYMO at CBR server

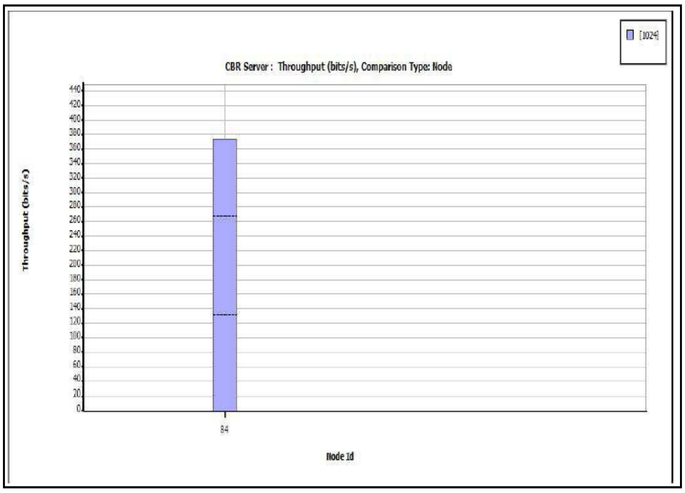


Figure 9. Throughput of AODV at CBR server

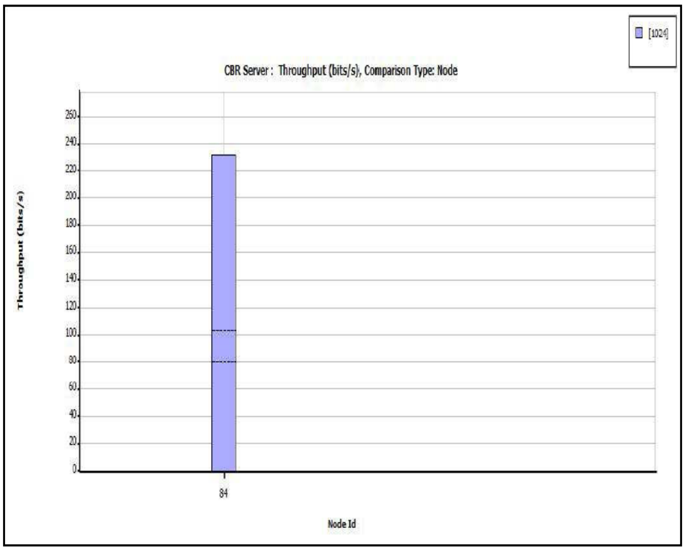


Figure 10 . Throughput of DSR at CBR server

7. ACKNOWLEDGMENTS

Dr. ARUNKUMAR B.R., MCA, M.Phil(CS), M.Tech(CS&E), PGDIPR (National Law School of India University, Banglore) and Ph.D (CS) serving as a Professor and Head of the department, Master of Computer Applications, BMS Institute of Technology, Bangalore, Karnataka, India has published nearly 20 research papers in National/International Journals and 11 papers in National/International Conferences including IEEE international conferences, wishes to place on record his sincere thanks to all those who helped in bringing out this paper.

8. REFERENCES

[1] Michel Borela, "Measurement and Interpretation of packet Loss" IEEE/ACM networking, Vol.4,pp.28-36,1998.

[2] Slater J.H. ,"End-to-end Arguments in System Design",ACM Transaction in Computer Science,pp.277-288,1984.

[3] Yaling Yang and Robin Kravets, " Contention-Aware Admission control protocol for Mobile Ad hoc Networks", IEEE Transaction on Mobile Computing, Vol. 4, pp.363-376 ,2005.

[4] Arunkumar B.R., "Cross layer Design for Quality of Service Multicasting in Mobile Ad Hoc networks", Ph.D Thesis, Chapter 4-9, pp.47-159.

[5] Claffy k. and Miller G. , " The Nature of the Beast: Recent Traffic Measurements from an Internet backbone", Proc INET' 98, Geneva, Switzereland,PP.49-57,1998.

[6] Daniel Minoli, "Traffic Engineering Basics", DataPro. Report 5410MVN, PP. 36-66,1995.

[7] Guerin R. and Peris V. ," Quality of Service in Packet Networks: Basic Mechanisms and Directions", IEEE Netwoking, pp. 120-127, 2000.

[8] Perkins C.E. " Ad Hoc Networking", Addision-Wesley, Chapter 1-5, pp. 28-46,2002.

[9] Johnson D.B., Maltz D.A. and Hu Y. " The Dynamic Source Routing Protocol for Mobile Ad Hoc networks", <draft-ietf-manet-dsr-09.txt>, pp.5-45, 2003.

[10] Ian D. Chakeres, Elizabeth M.Royer and Charles E. Perkins, "Dynamic MANET on-demand Routing Protocol", IETF internet Draft, draft-ietf-manet-dymo-00.txt, pp.140-152,2005.

[11] Keuwon and Shin K," providing Deterministic Delay Guarantees in ATM Networks", IEEE/ACM transactions on Networking",Vol.6, No.6, pp. 838-850, 1998.

[12] Weichao Wang, Bharat Bhargava, Yi Lu and Xiaoxin Wu," Defending Against Wormhole Attacks in Mobile Ad Hoc Networks", Wireless Communications and Mobile Computing, Vol.6, Issue 4, pp.483-503, 2006.

[13] R.K.Gnanamurthy and K.Sankaranarayanan," Issues Related to Quality of Service and Security in MANET: A survey",Karpagam JCS Vol.2, Issue 6, May-June 2007.

[14] Sencun Zhu et al, "An efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Netwoprks", proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and services, IEEE, pp.17-25, 2004.

[15] http://en.wikipedia.org/wiki/Physical_layer

[16]http://en.wikipedia.org/wiki/Routing_protocol

[17] https://en.wikipedia.org/wiki/Fading

[18] S. Madhavi and I.Ramesh Babu, " Security in Mobile Ad hoc networks: Challenges and Solutions", Karpagam JCS Vol.1, Issue 6, Sept.-Oct. 2007.

[19] Yih-Chun Hu, Adrian Perrig and David B.Johnson, "Efficient Security mechanisms for Routing protocols" MobiCom'02,September 23-26,Atlanta,Georgia,USA, monarch.cs.cmu.edu/monarch-papers/mobicom02.pdf.

[20] Lidong Zhou and Zygmunt J.Haas," Securing Ad Hoc networks",IEEE Network, special issue on network security, Novemebr/December, 1999, the work supported by DARPA/RADC, pp. 1-12.

[21] Prassant Mohapatra, Chao Gui, Jian Li,"Group Communications in Mobile Ad Hoc Networks", published by the IEEE Computer Society, pp.70-77, February 2004.

[22] Arunkumar B.R., Lokanatha.C.Reddy, Prakash.S.Hiremath,"Mobile Ad Hoc Networks: Issues, Research Trends and Experiments", IETECH Journal of Communication Techniques, vol.2, No. 2, pp.057-063, IETECH publications 2008.

[23] Ali-H.Al-Bayatti, Hussein Zedan, Antonio Cau,"Security solution for mobile ad hoc networks", 2009 fifth international confernce on Netorking and Services", published in digital library of IEEE Computer Society, pp.255-262, 2009.

[24] Oddi.G et al," A proactive link-failure resilient routing protocol for MANETs based on reinforcement learning", published in digital library of IEEE Computer Society, pp.1259-1264, E-ISBN :978-1-4673-2529,2012.

[25] Khalil.I, et al," Distributed Secure routing Protocol for Mobile Ad Hoc Networks", Computer science and Information technology (CSIT), 2013 5th international Conference, published in digital library of IEEE Computer Society, pp.106-110,2013