SIMULATION ANALYSIS OF ROUTING PROTOCOLS IN MANET'S USING NS2

Qazi Mohammad Nasir, Hamid Farooq, Sandeep Kumar

Abstract— **Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links where each node operates as an end system and a router for all other nodes in the network. These MANETs don't require any centralized infrastructure to work like we have access point in wireless networks. This is how they find their importance in today's world were independent systems are preferred.**
In this paper we have analyzed the performance of routing protocols in terms of Throughput and Packet Delivery Ratio. No hardware is used to accomplish the project. Though a network simulator, NS2 is used which College provides.

I. INTRODUCTION

Wireless communication between mobile users is becoming more popular than ever before. This is due to recent technological advances in laptop computers and wireless data communication devices, such as wireless nodes and wireless LANs. This has lead to lower prices and higher data rates, which are the two main reasons why mobile computing continues to enjoy rapid growth. There are two distinct approaches for enabling wireless communication between two hosts. The first approach is to let the existing cellular network infrastructure carry data as well as voice. The major problems include the problem of handoff, which tries to handle the situation when a connection should be smoothly handed over from one base station to another base station without noticeable delay or packet loss. Another problem is that networks based on the cellular infrastructure are limited to places where there exists such a cellular network infrastructure. The second approach is to form an ad-hoc network among all users wanting to communicate with each other. This means that all users participating in the ad-hoc network must be willing to forward data packets to make sure that the packets are delivered from source to destination. This form of networking is limited in range by the individual nodes transmission ranges and is typically smaller compared to the range of cellular systems. This does not mean that the cellular approach is better than the ad-hoc approach.

Ad-hoc networks do not rely on any pre-established infrastructure and can therefore be deployed in places with no infrastructure. This is useful in disaster recovery situations and places with non-existing or damaged communication infrastructure where rapid deployment of a communication network is needed. Ad-hoc networks can also be useful on conferences where people participating in the conference can form a temporary network without engaging the services of any pre-existing network. Because nodes are forwarding packets for each other, some sort of routing protocol is necessary to make the routing decisions.

There are currently two variations of mobile wireless networks infrastructured and Infrastructureless networks. The infrastructured networks, also known as Cellular network, have fixed and wired gateways.

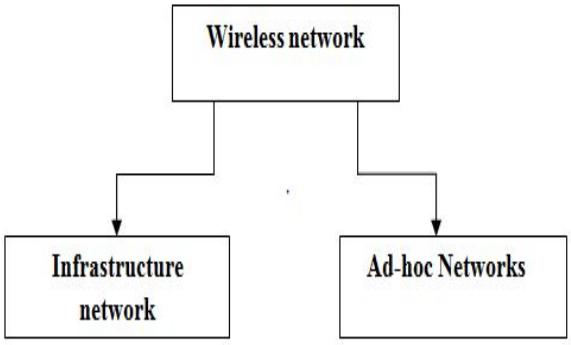


Fig.1.1Wireless network category

They have fixed base stations that are connected to other base stations through wires. The transmission range of a base station constitutes a cell. All the mobile nodes lying within this cell connects to and communicates with the nearest bridge (base station). A hand off occurs as mobile host travels out of range of one Base Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example of this type includes office wireless local area networks (WLANs).

Manuscript received July 19, 2014

Qazi Mohammad Nasir, M. Tech. Computer Science Department, GITM, Bilaspur, Haryana, India
Hamid Farooq, M. Tech. Computer Science Department, GITM, Bilaspur, Haryana, India
Sandeep Kumar, Assistant Professor, Computer Science Department, GITM, Bilaspur, Haryana, India

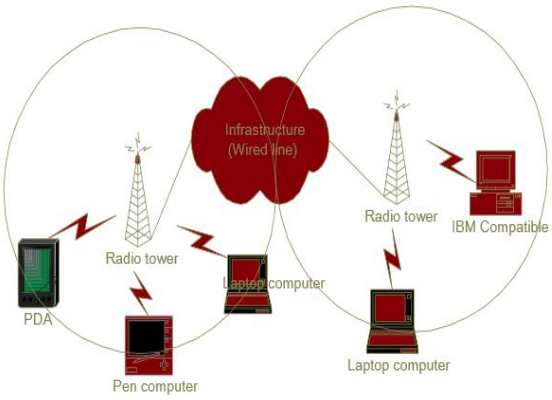


Fig.1.2 Infrastructured Network

The other type of network, Infrastructureless network, is known as Mobile Ad NETwork (MANET). These networks have no fixed routers. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move at will relative to each other. In this type of network, some pairs of terminals may not be able to communicate directly to with each other and relaying of some messages is required so that they are delivered to their destinations. The nodes of these networks also function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices.

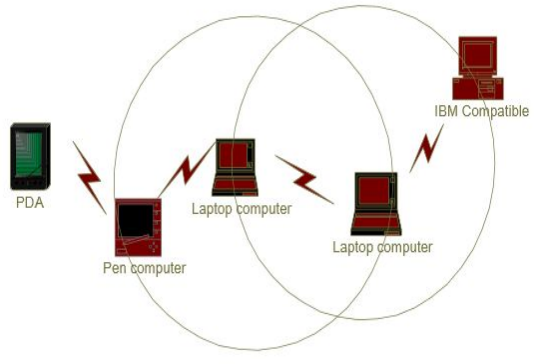


Fig. 1.3 Infrastructureless Network

The chief difference between ad hoc networks is the apparent lack of a centralized entity within an ad-hoc network. There are no base stations or mobile switching centers in an ad hoc network. The interest in wireless ad hoc networks stems from of their well-known advantages for certain types of applications. Since, there is no fixed infrastructure,a wireless ad hoc network can be deployed quickly. Thus, such networks can be used in situations where either there is no other wireless communication infrastructure present or where such infrastructure cannot be used because of security, cost, or safety reasons.

II. Ad-Hoc ROUTING PROTOCOLS

An ad hoc routing protocol is a standard for controlling node decisions when routing packets traverse a MANET between devices. A node in the network, or one trying to join, does not know about the topology of the network. It discovers the topology by announcing its presence and listening to broadcasts from other nodes (neighbours) in the network. The process of route discovery is performed differently depending on the routing protocol implemented in a network.

A number of routing protocols have been suggested for ad-hoc networks. These protocols can be classified into three categories:

- Table driven routing protocols
- Source initiated on demand routing protocols
- Hybrid routing protocol

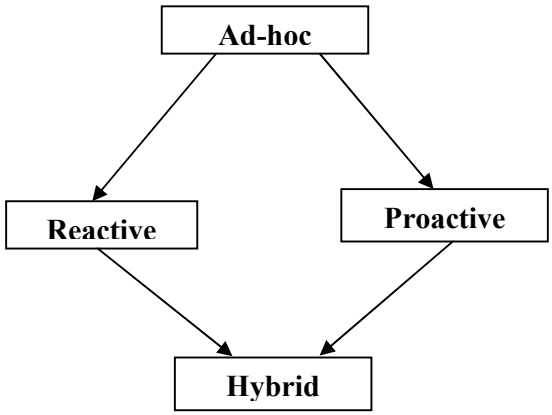
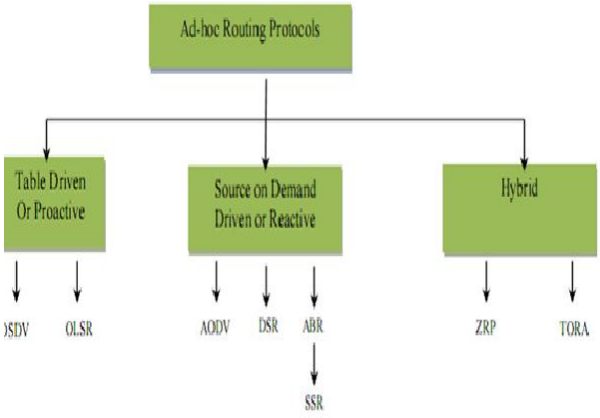


Figure 2(a). Types of routing protocols

The objectives of manet routing protocols are to maximize network throughput, to maximize network lifetime and to minimize delay

Routing protocols can be classified as shown below:



III. Related Study

We have identified several pieces of key literature in the field of MANET routing protocols which highlight existing protocols as well as the current thinking within the field and the directions researchers are moving in the future. Reference [3] proposes that an effective MANET routing protocol must be equipped to deal with the dynamic and unpredictable topology changes associated with mobile nodes, whilst also being aware of the limited wireless bandwidth and device power considerations which may lead to reductions in transmission range or throughput. This is expanded upon by [1] who propose that in addition to these core requirements; MANET routing protocols should also be decentralized, self-healing and self-organising and able to exploit multi-hopping and load balancing, these requirements ensure MANET routing protocols ability to operate autonomously.

Wireless ad hoc networks impose additional challenges in front of the designers, due to the lack of infrastructure and the dynamic and ephemeral character of the relationship between the network nodes. They require more sophisticated, efficient and well designed security mechanisms to achieve security goals [9]. Increasing number of ad-hoc networking applications (including sensor networks, ubiquitous computing and peer-to-peer applications) emphasize a need for strong privacy protection and security mechanisms. Security in ad hoc networking is a huge topic . It defines security goals and possible threats and attacks, explains major security mechanisms and schemes and presents several security architectures and existing projects. There are still many challenges ahead. Ad hoc networks rely on cooperation of involved nodes which can be threatened by node selfishness and result in denial of service, network break down and depriving all users of cooperation. So, demands for efficient resolvement of secure grouping, membership management and trust management are still under investigation. Accountability is another open issue. Concerning trust metrics and repudiation mechanisms, these are partially solved with multi-agent design. Cooperation approach, similar to game theory, may be used in designing ad hoc communication systems. Compromise between anonymity and accountability is applied through micropayment enforcements. Micro-payments are enforcing security and enhancing QoS provisioning at the same time. Secure service provisioning [8,9] incorporates security mechanisms into service discovery procedures. Security features intend to be embedded in ad hoc devices providing secure link layer functionalities. Efficient use of computation resources and guarding against parasitic computation is another challenge. The research in the area of authentication and key management concentrates on designing cryptographic algorithms that should be efficient in sense of computational and message overhead. Variety of broadcast and multicast scenarios are still waiting to be resolved. Designing self-enforcing privacy policies and enhancing privacy mechanisms are challenging issues for ubiquitous computing environments. A number of routing protocols for MANET, which are broadly categorized as proactive and reactive. Proactive routing protocols tend to provide lower latency than that o f the on-demand protocols, because they try to maintain routes to all the nodes in the network all the time. But the drawback for such protocols is the excessive routing overhead transmitted, which is periodic in nature without much consideration for the network mobility or load. On the other hand, though reactive protocols discover routes only when they are needed, they may still generate a huge amount of traffic when the network changes frequently. Depending on the amount of network traffic and number of flows, the routing protocols could be chosen. When there is congestion in the network due to heavy traffic, in general case, a reactive protocol is preferable. Sometimes the size of the network might be a major considerable point. For example, AODV, DSR are some of the protocols suitable for relatively smaller networks. Network mobility is another factor that can degrade the performance of certain protocols. When the network is relatively static, proactive routing protocols can be used, as storing the topology information in such case is more efficient. On the other hand, as the mobility of nodes in the network increases, reactive protocols perform better. Overall, the answer to the debating point might be that the mobility and traffic pattern of the network must play the key role for choosing an appropriate routing strategy for a particular network. It is quite natural that one particular solution cannot be applied for all sorts of situations and, even if applied, might not be optimal in all cases. Often it is more appropriate to apply a hybrid protocol rather than a strictly proactive or reactive protocol as hybrid protocols often possess the advantages of both types of protocols

IV. RESULTS

Here we calculate number of packets received in our simulation. A high number of packet received means higher performance.

AODV with 50 nodes

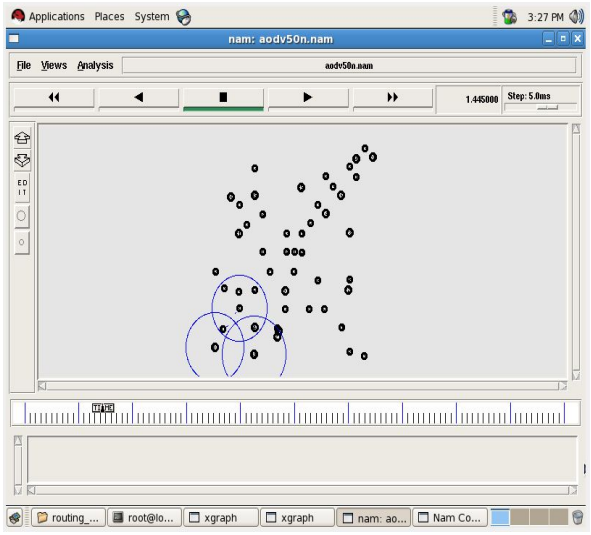


Fig 5.1: Simulation of AODV with 50 nodes.

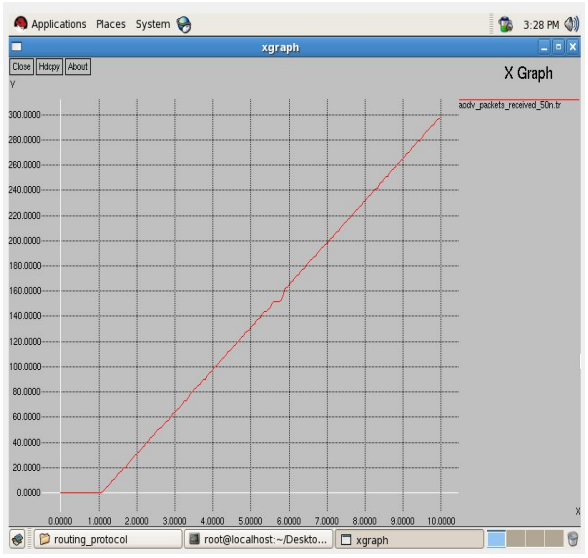


Fig 5.2: X-graph representing packet received in simulation for AODV.

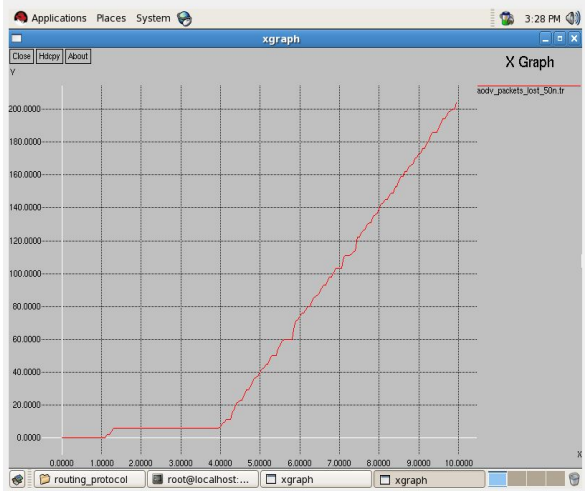


Fig 5.3: X-graph representing packet lost in simulation for AODV.

DSR with 50 nodes

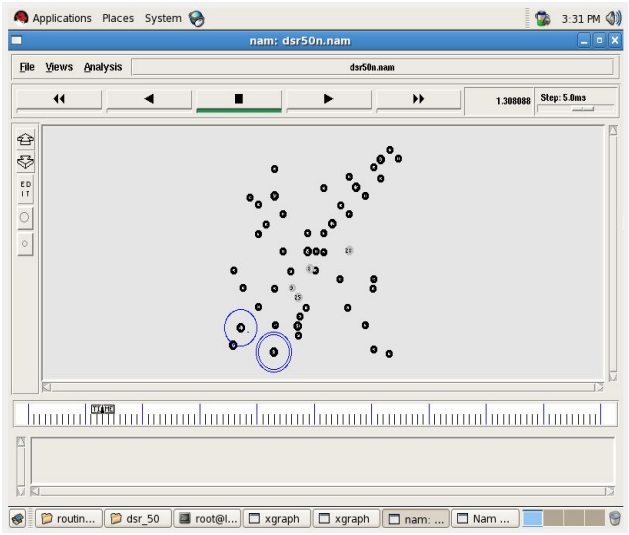


Fig 5.4: Simulation of DSR with 50 nodes.

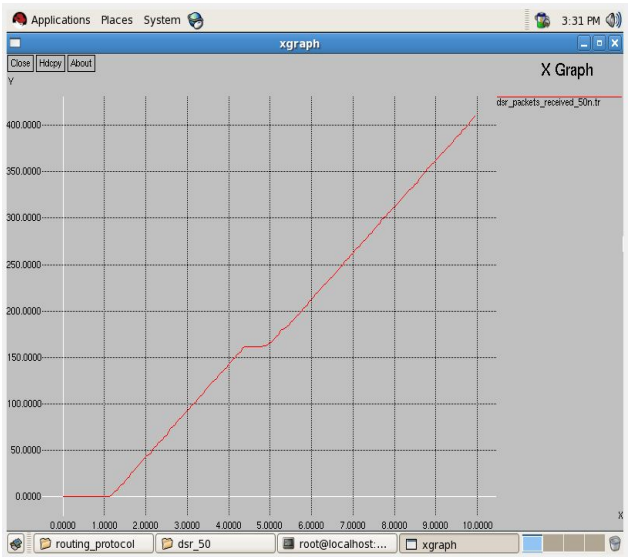


Fig 5.5: X-graph representing packet received in simulation for DSR.

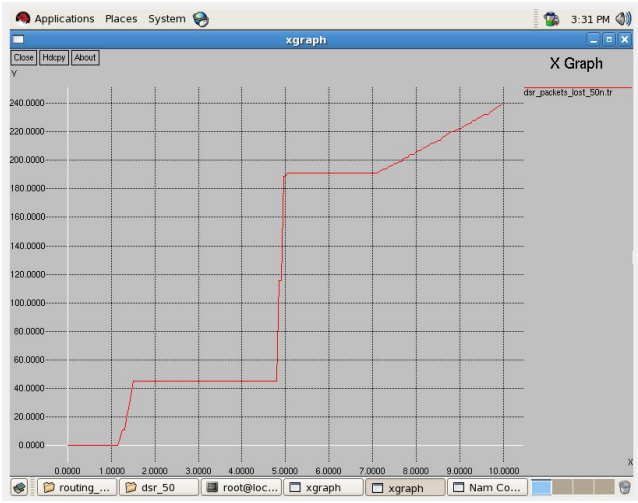


Fig 5.6: X-graph representing packet lost in simulation for DSR.

ZRP with 50 nodes.

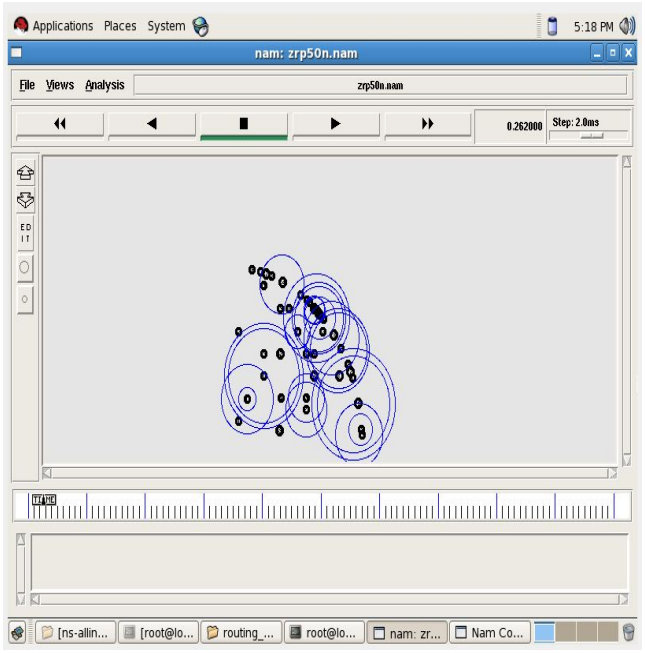


Fig 5.7: Simulation of ZRP with 50 nodes

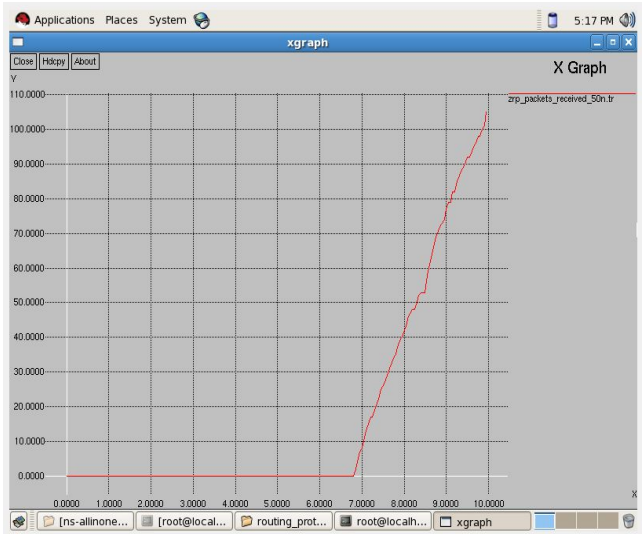


Fig 5.8: X-graph representing packet received in simulation for ZRP.

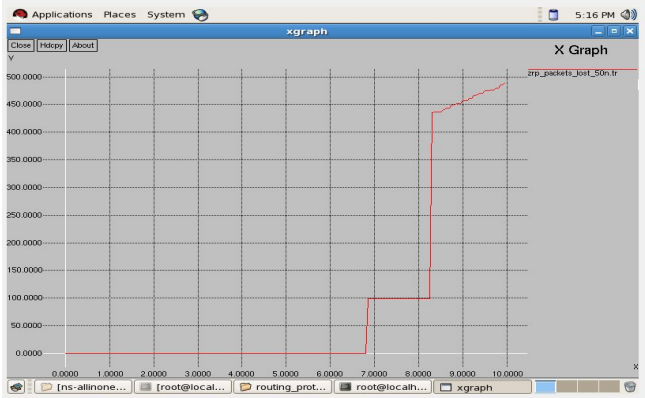


Fig 5.9: X-graph representing packet lost in simulation for ZRP.

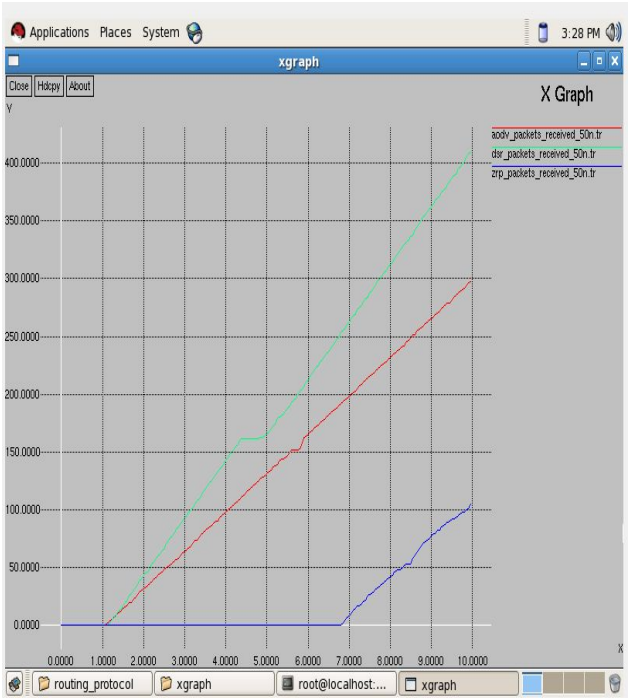


Fig 5.10: X-graph representing comparison of packet received in simulation for AODV, DSR and ZRP.

In fig 5.10 number of packets recieved in DSR is much higher than other routing protocols. ZRP performs worst in this case.

Fig 5.11: X-graph representing comparison of packet lost in simulation for AODV, DSR and ZRP.

In fig 5.11, the number of packets lost in ZRP is much higher than other routing protocols. Packets lost is minimum in case of AODV.

CONCLUSION

The performance of the three MANET Routing protocols such as AODV, DSR and ZRP was analyzed using NS-2 Simulator. When comparing the number of packets received and number of packets lost by each of the protocols, DSR has the high number of packets received. It measures of effectiveness of a routing protocol. The packet received and packets lost of AODV, DSR and ZRP Protocols for 50 Nodes .Based on the simulation results, the packets received value of DSR slowly increases initially and maintains its value when the time increases. ZRP performs worst in this case because of high number of packet lost.

FUTURE WORK

A comparison or routing protocols AODV, DSR and ZRP has been carried out. It is proposed to compare all other routing protocols considering the same simulation parameters so that an exhaustive comparison of various routing protocols can be made.

Also, it would be interesting to observe the behaviour of these protocols by varying other network parameters like Simulation time, Simulation areas, Traffic type etc. More performance metrics can also be considered. These protocols can also be compared with their existence & the work presented here can be used as a reference for future.

REFERENCES

1. R. Misra and C.R. Mandal, "Performance comparison of AODV/DSR on-demand routing Proto-cols for ad hoc networks in constrained situation" ICPWC International Conference, IEEE, 2005, pp. 86 – 89
2. C. E. Perkins and E. M. Royer, "Ad-hoc on demand distance vector routing," in Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99),vol. 3, New Orleans, LA, USA, February 1999, pp. 90–100.
3. C. Perkins, E. Belding-Royer, and S. Das, "RFC 3561: Ad hoc on-demand distance vector (AODV) routing," July 2003, category: experimental. [Online]. Available:ftp://ftp.isi.edu/in-notes/rfc3561.tx
4. D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in Mobile Computing, T. Imielinski and H. Korth, Eds. Kluwer Academic Publishers, 1996,vol. 353, , pp. 153–181
5. Uyen Trang Nguyen and Xing Xiong, "Rate-adaptive Multicast in Mobile Ad hoc Networks," IEEE International Conference on Ad hoc and Mobile Computing, Networking and Communications, WiMob,Montreal, Canada, 2005
6. E. Alotaibi andB.Mukherjee,"A survey on routing algorithms for wireless Ad-Hoc and mesh networks,"Computer Networks: The International Journal of Computer and Telecommunications Networking,vol.56,no.2, pp. 940–965, October 2011.
7. R.O. Schmidt and M.A.S.Trentin,"MANETs Routing Protocols Evaluation in a Scenario with High Mobility: MANET Routing Protocols Performance and Behaviour,"Network Operations and Management Symposium, 2008. NOMS 2008. IEEE,Salvador, Bahia, pp.883-886, 2008
8. Handorean, R. and Roman, G. -C., "Secure Service Provision in Ad Hoc Networks,"Technical Report WUCSE-03-47, Washington University, Department of Computer Science, St. Louis, Missouri, USA, 2003.
9. Eronen, P., Gehrmann, C., and Nikander, P., "Securing Ad Hoc Jini Services,"NordSec2000, Reykjavik, Island, October 2000.
10. Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, vol. 24, no. 2, Feb. 2006.
11. S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," 6th MobiCom, Boston, MA, Aug. 2000.
12. P. Yi et al., "A New Routing Attack in Mobile Ad Hoc Networks," Int'l. J. Info. Tech., vol. 11, no. 2, 2005.
13. T.Ravi Nayak, Sake Pothalaiah and K Ashok Babu, " Implemntation of Adaptive Zone Routing Protocol For Wireless Networks", IJEST, vol.2 (12), 2012.
14. Haas, Zygmunt J., Pearlman, Marc R.: The Performance of Query Control Schemes for the Zone Routing Protocol, August 2001, IEEE/ACM Transactions on Networking, Vol. 9, No. 4
15. Z.J. Haas, M. R. Pearlman, and P. Samer, "Intrazone Routing Protocol (IARP)," Internet Draft, 2001, available at:http://tools.ietf.org/id/draft-ietf-MANETs-iarp-01.txt.
16. Z.J. Haas, M. R. Pearlman, and P. Samer, "Interzone Routing Protocol (IERP),"Internet Draft, 2001, available at:http://tools.ietf.org/id/draft-ietf-MANETs-ierp-01.txt.
17. Z.J. Haas, M. R. Pearlman, and P. Samer, "The Bordercast Resolution Protocol (BRP)," Internet Draft, 2001, available at:http://tools.ietf.org/id/draft-ietf-MANETsbrp-01.txt.
18. Zhan Haawei, Zhou Yun; "Comparison and analysis AODV and OLSR Routing Protocols in Ad Hoc Network", 2008, IEEE.
19. JIRI HOSEK, KAROL MOLNAR; "Investigation on OLSR Routing Protocol Efficiency", Recent Advances in Computers, Communications, Applied Social Science and Mathematics, ISBN: 978-1-61804-030-5, PP: 147 – 153.