Research Analysis of Different Routing Protocols of Mobile Ad Hoc Network (MANET)

[1]Gunjan Bahl, [2]Amit Dawar, [3]Mandeep Singh

[1,2,3]Dept. of Computer Science Engineering, HMR Institute of Technology & Management, Delhi, India

Abstract

Mobile Ad-Hoc Network (MANET) is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. Due to the mobility of the nodes in the network, these nodes are self-organizing and self-configuring. Not only they act as hosts, but also they function as routers. They direct data to or from other nodes in the network. Currently, it is one of the most attractive research topics in the wireless communication. These mobile nodes dynamically create temporary network and transferring messages from one mobile node to others in peer-to-peer fashion. A routing protocol runs on every mobile host and therefore subjected to the limitation of resources on every node. Therefore, to guarantee communication an efficient routing technique is desirable to that allow nodes to communicate in a timely manner. The primary goal of any ad-hoc network routing protocol is to meet the challenges of the dynamically changing topology. Therefore, an efficient route between any two nodes with minimum routing overhead and bandwidth consumption should be established. In this paper, the MANET characteristics and attacks are highlighted .In addition, the previously mentioned categories of routing protocols, proactive and reactive are explored. Moreover, a comparison is conducted between different protocols; namely, DSDV, AODV, DSR and AOMDV in terms of both properties and performance.

Keywords

MANET; Proactive Protocols; Reactive Protocols; MANET Characteristics; DSDV; AODV; Routing Protocols

I. Introduction

Recently, wireless networks and mobile devices gained a wide popularity because they are expected to bring the interaction between human, environment and machine to a new level. This led to the significant increase of mobile ad-hoc networks in the last few years as these mobile ad hoc network can be developed by connecting different mobile nodes through a wireless link with no supporting fixed infrastructure. Accordingly, MANETs became one of the most prevalent areas in research. The ability of this type of networks to operate anywhere and anytime made it adaptable in many new applications.MANET stands for Mobile adhoc Network also called as wireless adhoc network / adhoc wireless network that is usually on the top of a Link Layer ad hoc network. They consist of set of dynamic and mobile nodes connected wirelessly in a self configured, self healing network without having a fixed infrastructure and thus , all nodes cooperate with each other to exchange information and forward packets; thus extending the limited transmission range of each node's wireless network interface without using any pre-existing fixed network infrastructure.MANET nodes are mobile and can move independently in any direction and therefore changes its links to other devices frequently. Due to this dynamic nature of the MANETs, routing protocols should be efficient enough to satisfy the network's requirements. They use wireless connections to connect to various networks. Like a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission[1]. But in real-time MANET environment, the mobility and dynamic nature of nodes in MANETs may have a negative impact on the performance of message sending and receiving. So, Each node have to perform the responsibilities to behave as a router[1,15] and run routing protocol to forward traffic to other specified node in the network by participating and maintenance of routes with other nodes in the network.

II. Background

A mobile ad-hoc network (MANET) is an infrastructure-less network of mobile devices connected by wireless communication. They are characterized by the following criteria:

- **MANET forms a completely symmetric environment-** where all nodes have identical features and capabilities.
- **Capable of long distance communication -** Each node act as both host and router. That is it is autonomous in behavior and thus, these nodes
- **Multi-hop radio relaying-** When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
- **Absence of centralized firewall-** Distributed nature of operation for security, routing and host configuration.
- **Dynamic Network topology-** The nodes can join or leave the network anytime
- **Efficient Mobile nodes** – characterized with less memory, power and light-weight features. 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.
- **Efficient User- Mobility**- High user density and large level of user mobility.
- **Limited Security:** Wireless network are more prone to security threats. A centralized firewall is absent due to its distributed nature of operation for security, routing and host configuration.

III. Applications

Ad-hoc networking is gaining importance, with the increase of portable devices as well as progress in wireless communication. Ad-hoc networking can be applied anywhere where there is infrastructure-less communication or the existing infrastructure is expensive or inconvenient to use[18]. 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. Decentralization makes the networks more flexible and more robust. Typical applications include:

A. Military Battlefield

Ad- hoc networking would allow the military to maintain a fast and possibly short term military communications and an information network between the soldiers, vehicles, and military information headquarters.

B. Commercial 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.

C. Local 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.

D. Personal Area Network (PAN)

Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS.

E. MANET-VoVoN

A MANET enabled version of JXTA peer-to-peer, modular, open platform is used to support user location and audio streaming over the JXTA virtual overlay network. user and a call setup until a path is available to reach the user. The application uses a private signaling protocol based on the exchange of XML messages over MANET-JXTA communication channels .

F. Law Enforcement

For secure and fast communication during law enforcement operations.

IV. Attacks

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is the major step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information [16]. De-centralized co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks .There are a number of attacks that affect MANET[14]. These attacks can be classified as in the following table

MANET security Layer	Attacks
Application Layer	Malicious code, Repudiation
Transport Layer	Session hijacking, SYN Flooding
Network Layer	Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing etc.
Data Link Layer	Traffic analysis and monitoring.
Physical Layer	Traffic Jamming, Eavesdropping
Multi-layer Attacks	DoS, impersonation etc

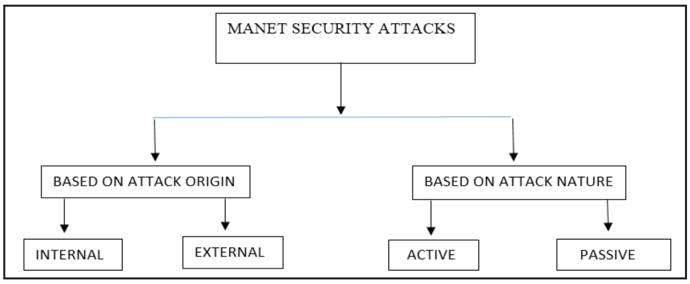


Fig. 1:

A. Attacks on mobile Ad Hoc networks can be classified

1. Based on Attack Origin

(i). External Attack

External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.

(ii). Internal Attack

Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities.

B. Based on Attack Nature

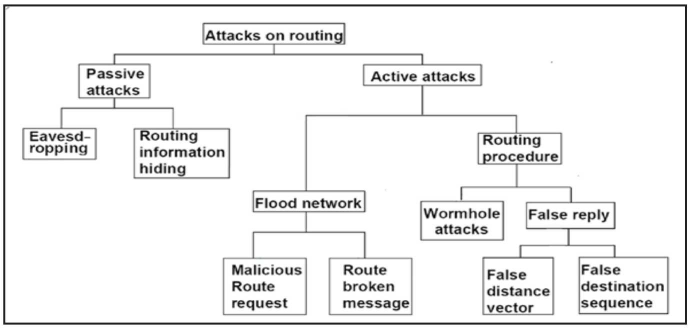


Fig. 2:

1. Passive Attack

In this type of attack, the intruder only monitors certain connections to get information about the traffic or about the nature of communication without injecting any fake information .This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully.

(i). Eavesdropping

The node simply observes the confidential information .This information can be later used by the malicious node.The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

(ii). Traffic Analysis

In MANETs the data packets as well as traffic pattern can be used to access and analyze confidential information about network topology. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered.

(iii). Snooping

Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. Malicious hackers frequently use this technique to monitor key strokes, capture passwords and login information etc.

2. Active Attacks

An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement.

(i). Flooding Attack

In flooding attack, attacker exhausts the network resources and make them unavailable for legal/ authorized user. The attacker generally uses radio signal jamming and the battery exhaustion method. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network.

3. Black Hole Attack

A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one[17]. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

4. Wormhole Attack

In this, when an attacker receives packets, it tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel is known as a wormhole .In DSR, AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Wormholes are dangerous because they can do damage without even knowing the network.

5. Gray-hole Attack

This attack is also known as routing misbehaviour attack .It decreases the performance of the system and thus, leads to dropping of messages[14]. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

V. Routing Protocols

Several MANETs routing protocols[5] may be broadly classified into two types as :

1. Table Driven or Proactive Protocols

In this type of protocols, each node maintains one or more tables containing routing information to every other node in the network[8]. All nodes keep on updating their routing tables to maintain the latest view of the network. DSDV is an example of such protocols.

2. On Demand or Reactive Protocols

In this type of protocols, routes are created only when required. In other words, when a packet is to be transmitted from a source to a destination, it invokes the route discovery procedure. The route remains valid till either the destination is reached or the route is no longer needed. Some of the existing on demand routing protocols are: DSR and AODV[11] .

This paper emphasizes on DSDV and AODV routing protocols since it was proven that these are the best suited for Ad Hoc Networks. The next subsections describe the basic features of these protocols:

A. DSDV

Destination Sequenced Distance Vector (DSDV) is a hop-by-hop vector routing protocol requiring each node to periodically broadcast routing updates. This is a table driven algorithm based on modifications made to the Bellman-Ford routing mechanism.[3] Each node in the network maintains a routing table that has entries for each of the destinations in the network and the number of hops required to reach each of them. Each entry has a sequence number associated with it that helps in identifying stale entries. This mechanism allows the protocol to avoid the formation of routing loops[11]. Each node periodically sends updates tagged throughout the network with a monotonically increasing even sequence number to advertise its location. New route broadcasts contain the address of the destination, the number of hops to reach the destination, the sequence number of the information received regarding the destination, as well as a new sequence number unique to the broadcast. The route labeled with the most recent sequence number is always used. When the neighbors of the transmitting node receive this update, they recognize that they are one hop away from the source node and include this information in their distance vectors. Every node stores the "next routing hop" for every reachable destination in their routing table. The route used is the one with the highest sequence number i.e. the most recent one[19]. When a neighbor B of A finds out that A is no longer reachable, it advertises the route to A with an infinite metric and a sequence number one greater than the latest sequence number for the route forcing any nodes with B on the path to A, to reset their routing tables. Routing table updates in DSDV are distributed by two different types of update packets:

1. Full Dump

This type of update packet contains all the routing information available at a node. As a consequence , it may require several Network Protocol Data Units (NPDUs) to be transferred if the routing table is large[11]. Full dump packets are transmitted infrequently if the node only experiences occasional movement.

2. Incremental

This type of update packet contains only the information that has changed since the latest full dump was sent out by the node. Hence, incremental packets only consume a fraction of the network resources compared to a full dump.

(i). DSDV Advantages

- Guarantees no loop.
- Guarantees the freshness of routing information in the routing table by using the sequence number.
- Avoids extra traffic by using incremental updates
- Maintains the best path only to every destination. Therefore, the space of the routing table is reduced

(ii). DSDV Disadvantages

- The required periodic updates messages impose a big overhead. Therefore, it is not effective in large networks
- Does not support multipath routing.
- Waste of bandwidth due to the needless advertising of routing information even if there is no change in the network topology.

B. AODV

An Ad Hoc On-Demand Distance Vector (AODV) is a routing protocol designed for wireless and mobile ad hoc networks. This protocol establishes routes to destinations on demand and supports both unicast and multicast routing[12]. The AODV protocol builds routes between nodes only if they are requested by source nodes. AODV is therefore considered an on-demand algorithm and does not create any extra traffic for communication along links. The routes are maintained as long as they are required by the sources. They also form trees to connect multicast group members. AODV makes use of sequence numbers to ensure route freshness. They are self-starting and loop-free besides scaling to numerous mobile nodes. In AODV, networks are silent until connections are established. Network nodes that need connections broadcast a request for connection[6]. The remaining AODV nodes forward the message and record the node that requested a connection. Thus, they create a series of temporary routes back to the requesting node[2].A node that receives such messages and holds a route to a desired node sends a backward message through temporary routes to the requesting node. The node that initiated the request uses the route containing the least number of hops through other nodes. The entries that are not used in routing tables are recycled after some time. If a link fails, the routing error is passed back to the transmitting node and the process is repeated.

1. AODV Advantages

- Very effective in highly dynamic networks
- Since the information of stale routes expire after a specific time, AODV requires less space as compared to other reactive routing protocols.
- AODV supports multicasting.

2. AODV Disadvantages

- AODV lacks an efficient route maintenance technique since routing information is always obtained on demand.
- AODV suffers from high route discovery latency

C. DSR

Dynamic Source Routing (DSR) is a self-maintaining routing protocol for wireless networks. The protocol can also function with cellular telephone systems and mobile networks with up to about 200 nodes. A Dynamic Source Routing network can configure and organize itself independently of oversight by human administrators.

In Dynamic Source Routing, each source determines the route to be used in transmitting its packets to selected destinations. There are two main components, called Route Discovery and Route Maintenance. Route Discovery determines the optimum path for a transmission between a given source and destination. Route Maintenance ensures that the transmission path remains optimum and loop-free as network conditions change, even if this requires changing the route during a transmission.

Microsoft has developed a version of Dynamic Source Routing known as Link Quality Source Routing (LQSR) specifically for use with their Mesh Connectivity Layer (MCL) technology. MCL facilitates the interconnection of computers into a wireless mesh network using WiFi or WiMax services.

D. AOMDV

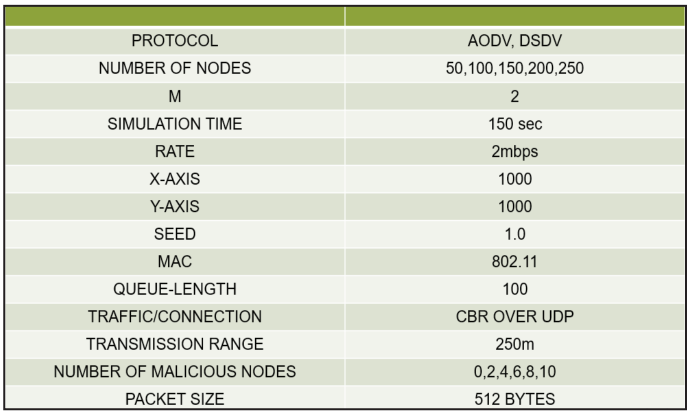
The main idea in AOMDV is to compute multiple paths during route discovery procedure for contending link failure. When AOMDV builds multiple paths, it will select the main path for data transmission which is based on the time of routing establishment. The earliest one will be regarded the best one, and only when the main path is down other paths can be effective. In fact, a large number of studies indicate that the aforementioned scheme is not necessarily the best path. Mobile nodes, which usually due to residual energy are too low or under heavy load and other factors, seriously affect the performance of the network. In order to improve the performance, we propose the novel NS-AOMDV protocol based on existing AOMDV. First, we consider the rate of node residual energy and idle buffer queue as the weight of node. Second, in route discovery process, the routing update rules calculate the node weight of each path and sort the path weight by descending value of path weight in route list, and we choose the path which has the largest path weight to transmit data packets. At the same time, the protocol uses the technology of RREQ delay forwarding and energy threshold to ease network congestion, limit the RREQ broadcast storm, and avoid low energy nodes to participate in establishment of path.

VI. Comparative Study

This section provides a comparative analysis of routing protocols [3]. Comparison is conducted in terms of both characteristics and performance. The metrics used in the performance analysis include the following:

- **Throughput:** Throughput refers to how much data can be transferred from one location to another in a given amount of time.
- **Packet Delivery Ratio:** PDR is defined as the ratio between the received packets by the destination and the generated packets by the source.
- **Normalized Routing Load (NRL):** NRL is the number of routing packets transmitted per data packet sent to the destination.
- **Average Delay:** The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another.

A. Simulation Parameters



PROTOCOL	AODV, DSDV
NUMBER OF NODES	50,100,150,200,250
M	2
SIMULATION TIME	150 sec
RATE	2mbps
X-AXIS	1000
Y-AXIS	1000
SEED	1.0
MAC	802.11
QUEUE-LENGTH	100
TRAFFIC/CONNECTION	CBR OVER UDP
TRANSMISSION RANGE	250m
NUMBER OF MALICIOUS NODES	0,2,4,6,8,10
PACKET SIZE	512 BYTES

Fig. 3:

B. Analysis of Characteristics

the differences between the most important characteristics of the two routing protocols [8].

Table 1: Routing Protocols Characteristics

Characteristic	DSDV	AODV
Loop free	Yes	Yes
Multicasting	No	No
Distributed	Yes	Yes
Periodic broadcast	Yes	Yes
QoS Support	No	No
Routes maintained in	Route Table	Route Table
Route cache/table timer	Yes	Yes
Reactive	No	Yes
Proactive	Yes	No

C. Analysis of Performance

1. Average end-to-end Delay

AODV gives the highest average end-to-end delay of packets delivery as compared to DSDV. Even under the influence of Black Hole Attack, DSDV performs better in this aspect.

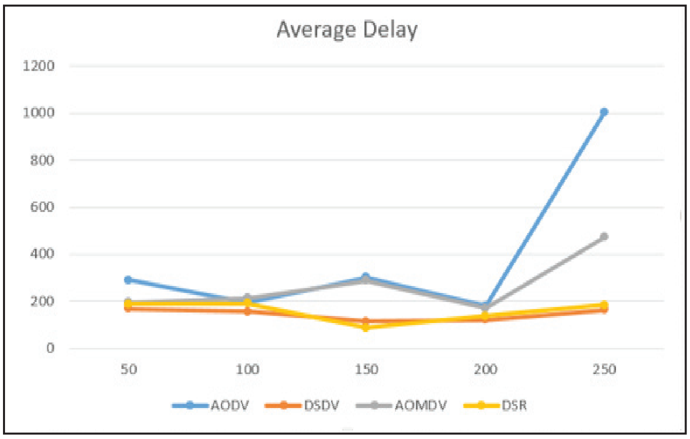


Fig. 4:

2. Packet Delivery Ratio

In case of low mobility, both protocols deliver a large percentage of the packets. This may reach 100% when there is no node motion. Under high mobility simulation, DSDV performs better than AODV.But under the influence of Black Hole attack, AoDV has a better packet delivery ratio than DSDV

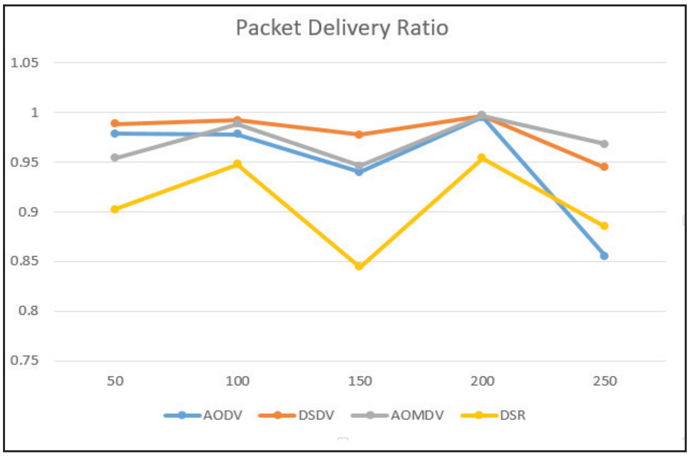


Fig. 5:

3. Normalized Routing Load

This is the ratio of the total number of the routing packets to the number of data packets as calculated at the MAC layer. Both AODV and DSDV have similar Routing Load under normal conditions. On the other hand, DSDV suffers from a lot of routing control packets. Therefore, the routing overhead is higher than the other protocol. DSDV routing overhead is negligible. However, it suffers from less route stability as compared to AODV.

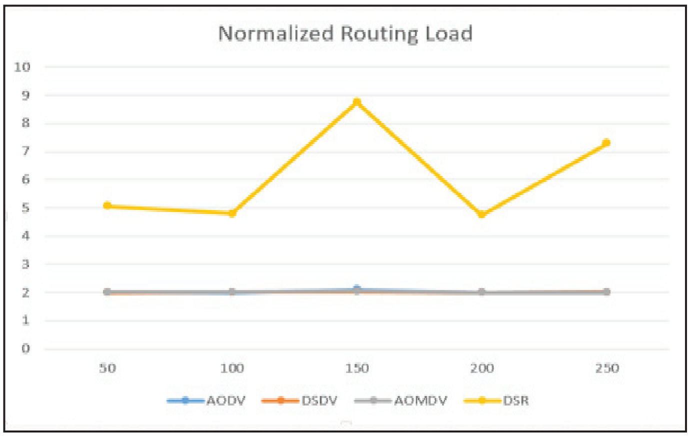


Fig. 6:

4. Throughput

Throughput refers to how much data can be transferred from one location to another in a given amount of time.DSDV provides a better throughput than AODV for corresponding no. of nodes. Even Under the influence of Black hole attack, DSDV has better throughput than DSDV.

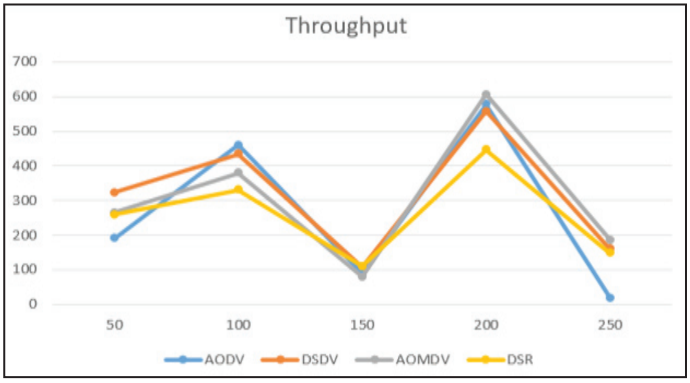


Fig. 7:

VII. Conclusion

In this paper, a comparative study is conducted between AODV, DSDV, DSR and AOMDV routing protocols in terms of both characteristics and performance. The performance metrics used are the packet delivery ratio, the average delay, the routing load, throughput, the nodes mobility and the increasing number of nodes in the network. As a conclusion, DSDV outperforms AODV, AOMDV and DSR in ordinary situations. Also, DSDV is better in more stressful situations. Therefore, practically speaking, it is better to use DSDV as it has the best performance in situation similar to the real life situation.

References

[1] S. Kumar, J. Kumar,"Comparative analysis of proactive and reactive routing protocols in mobile Ad-Hoc networks (MANET)," Journal of Information and Operations Management, 3(1), pp. 92—95, 2012.

[2] R. Bansal, H. Goyal, P. Singh,"Analytical study the performance evaluation of mobile ad hoc networks using AODV protocol," International Journal of Computer Applications, 14(4), pp. 34 – 37, 2011.

[3] K. Lego, P. K. Singh, D. Sutradhar,"Comparative study of Ad-hoc routing protocol AODV, DSR and DSDV in mobile Adhoc NETwork," Indian Journal of Computer Science and Engineering, 1(4), pp. 364 – 371, 2010.

[4] C. Perkins, E. B. Royer, S. Das, "Ad hoc On Demand Distance Vector Routing", Network Working Group, [Online] Available: http://www.ietf.org/rfc/rfc356 1.txt, July 2003.

[5] Broch, D.A. Maltz, D.B. Johnson, Y.c. HU,"A Performance Comparison of Multi-Hop Wireless Ad-hoc Network Routing Protocols", Proceeding of the 4th Annual ACM/IEEE Int. Conference on Mobile Computing and Networking, 1998

[6] S. Tamilarasan,"A comparative study of multi-hop wireless ad-hoc network routing protocols in MANET," International Journal of Computer Science Issues (IJCSI), 8(5), pp. 176—184, 2011.

[7] S. Shah, A. Khandre, M. Shirole, G. Bhole,"Performance evaluation of Ad-hoc routing protocols using NS2 simulation", Mobile and Pervasive Computing (CoMPC), pp. 167–171, 2008.

[8] L. Tony, H. Nicklas,"Routing Protocols in Wireless Networks "A Simulation Study", Lulea University of Technology, Stockholm, 1998.

[9] C. S. Rammurty, B. S. Manoj,"Ad-hoc wireless networks architectures and protocols", Prentice Hall, 2004.

[10] Z. J. Haas, M. R. Pearlman,"The Zone Routing Protocol (ZRP) for Ad-Hoc Networks," IETF MANET working group, Internet draft, June 1999.

[11] C. Mbarushimana, A. Shahrabi,"Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-hoc Networks", 21st International Conference on Advanced Information Networking and Applications Workshop (AINA W'07), IEEE Computer Society, Mar 2007.

[12] C.E. Perkins, E.M. Royer, I.D. Chakeres,"Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol", draft-perkinmanet-aodvbis-OO.txt, Oct. 2003.

[13] Yi-Chun Hu, Adrian Perrig,"A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy, May/June 2004.

[14] Zhou Lidong, J. Haas Zygmunt,"Securing Ad Hoc Networks", IEEE network special issue, November/December 1999.

[15] Deng Hongmei, Wei Li, Dharma P. Agarwal,"Routing Security in Wireless Ad Hoc Networks", University of Cincinnati IEEE Communications magazine, October 2002.

[16] Yang H, Lou H, Ye F, Lu S, Zhang L,"Security in Mobile Ad-hoc Networks: Challenges and Solutions", IEEE Wireless Communications 2004,11(1), pp. 38–47.

[17] Raja Mahmood RA, Khan AI:,"A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks," Paper presented at the International Symposium on High Capacity Optical Networks and Enabling Technologies, Dubai, United Arab Emirates, 18–20 November 2007 2007.

[18] Chlamtac, Conti, Liu,"Mobile ad-hoc networking: imperatives and challenges," Elsevier Ad-hoc networking, USA, Texas, pp. 13-64, 2003

[19] B. D. Johnson, D. A. Maltz,"Dynamic source routing in ad hoc wireless networks," In Mobile Computing, Vol 5, pp. 153-181, 1996.

[20] B. D. Johnson, D. A. Maltz,"Dynamic source routing in ad hoc wireless networks," In Mobile Computing, Vol 5, pp. 153-181, 1996.