International Journal of Latest Trends in Engineering and Technology
Vol.(10)Issue(1), pp.292-297
DOI: http://dx.doi.org/10.21172/1.101.51
e-ISSN:2278-621X

CLASSIFICATION OF ROUTING PROTOCOLS IN MOBILE ADHOC NETWORKS

Dheer Dhwaj Barak[1]

Abstract- Routing protocol is the necessary and fundamental factor for performing various operations in MANETs. The routing protocols are customized to handle the nodes with limited resources in MANETs. Routing protocols have huge impact on network performance. In this paper, classification of routing protocols is discussed. Mainly two types of protocols, Static and Dynamic protocols, and their further categorization are discussed.

1. INTRODUCTION

In a Mobile adhoc network, Routing is basically a process by which a call is connected from its origin node to its destination node. It also takes part in architecture, design and operation of networks. Routing in ad-hoc networks has become a quite difficult task for the researchers due to the ever changing behavior of nodes in MANETs. Various protocols are created to manage the mobility of nodes. Routing process fundamentally uses, two sub processes: first is, to determine best possible routes and second is to transfer the data packets to the designated nodes via a network. Routing protocols are also used to choose the best suited path for delivering the packets to the destination node. Routing algorithm is used to find this optimal path. Static and Dynamic protocols are the two protocols which are discussed in this paper. Dynamic protocols are further classified into proactive, reactive and hybrid routing protocols which are further classified in the figure 2. DSDV, WEP, GSR, OSLR and LANMAR are Proactive protocols. Flooding, AODV, LMR, DSR, ABR, LAR and CEDAR are Reactive protocols and ZRP and ZHLS are hybrid routing protocols [Park, 2001] [Layuan, 2007] [Boukerche, 2004].

2. ROUTING PROTOCOLS IN MANETS

Routing protocols used in MANET are basically of two types, which are Static Routing and Dynamic Routing [Abolhasan, 2004] [Zhang, 2006].

Static routing: It is simply the procedure of physically loading paths as soon as the routing device is started either into "routing table" through a "configuration file" of a device or by a NA (network administrator) who designs these paths manually. Since these paths are configured manually, so these can't be altered once they are configured unless ns until these are altered by a human himself, hence called as 'static' routes which is the humblest routing form. But, less than five devices can be configured by it and only when a NA knows that these paths will perhaps never have alteration. It also doesn't handle "failures in external networks" very well as any manually configured path needs to be updated or reconfigured manually for fixing or repairing any gone astray connectivity [Dhenakaran, 2013] [Kumari, 2016].

Dynamic Routing: Its protocols are braced by software solicitations which are running on the router that dynamically acquire destination nodes in the network as well as how to reach there and then it advertises those destination nodes to all the routers in the network which then knows about all the existing destination nodes in the networks as well as how to reach them. Also, the same router will learn paths from other routers in the network which are running similar routing protocol such as "RIP, RIP2, EIGRP, OSPF, IS-IS, BGP etc". Then, every router will do sorting of the list of paths thereby selecting one or more "best"' possible paths for every network destination which the router has knowledge about.

Finally, "Dynamic routing protocols" will then dispense this "best route" info to other routers which run the similar "routing protocol" and this will extend the info on entire network [Clausen, 2002] [Santos, 2005] [Johnson, 2003].

Since research on numerous features of MANETs has been a hot theme of research for a long time and that too primarily on preservation of the "routing protocols" [Toh, 1997] [Park, 2001] [Layuan, 2007] [Boukerche, 2004] [Salehi, 2012]. Consequently, it becomes imperative to define the present "routing protocols" of MANET. Although several "routing protocols" are projected for MANETs but the best and widely acknowledged taxonomy is: reactive, proactive and hybrid routing protocols, shown in figure 1.

[1] Resource person in CSE Deptt., UIET, MDU, Rohtak

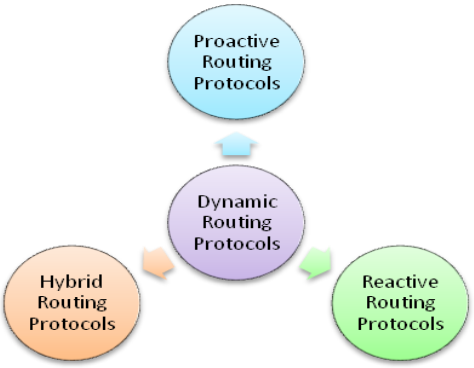

Figure 1: Types of Dynamic Routing Protocols in MANETs

Proactive Routing Protocols: In these protocols, routes to all the nodes are maintained irrespective of the fact which packets to those nodes are delivered or not. An illustration of this type of routing protocols in adhoc networks is Destination Sequenced Distance Vector routing protocol (DSDV), Optimized Link State Routing protocol (OLSR) and Wireless Routing Protocol (WRP). Thus some bandwidth is exhausted for maintaining the continuous complete routing information regarding the whole network [Lee, 2003] [Broch, 1999]. The protocols of an area vary with the information and the updates available in each of the table.

Reactive Routing Protocols: In these protocols, route amid two nodes is established then only when data packets are exchanged amid two nodes. These types of routing protocols are Dynamic Source Routing Protocol (DSR), AdhocOn Demand Distance Vector Routing Protocol (AODV) and Temporally Ordered Routing Algorithm (TORA) [Perkins, 2003] [Park, 2001] [Johnson, 2007]. These protocols are totally demand based. As they are demand based so they do not have to update route information. Also, there is no need to maintain the route in the absence of traffic. When traffic is low, it is also possible in this protocol to remarkably decrease the overhead routing, so the structure does not change frequently [Satav, 2016] [Abolhasana, 2003] [Kakkar, 2016].

Hybrid Routing Protocols: In these protocols, route amid two nodes is formed by mixing the concept of both proactive routing and reactive routing protocols. The Zone Routing Protocol (ZRP) is an example of hybrid reactive/proactive routing protocols. The only dissimilarity between reactive routing protocols is path finding and path optimizing method. In Hybrid methods, proactive and reactive methods are combined for efficient route finding technique [Walikar, 2016] [Mittal, 2009] [Park, 2001].

Hybrid routing protocols can be illustrated by ZHLS. In ZHLS, the entire network is fragmented into separate zones. If the traffic terminal and origin share the same source then ZHLS is proactive. It is reactive as a location search is required to find the zone ID of the destination. Routing protocols are classified in Figure 2. For this study some protocols investigations are required at network layer, for which routing protocol is required at network layer [Mittal, 2009]. Due to some appealing features, AODV & DSR routing protocol is an appropriate option for it [Royer, 1999] [Nguyen, 2008] [Boukerche, 2004].

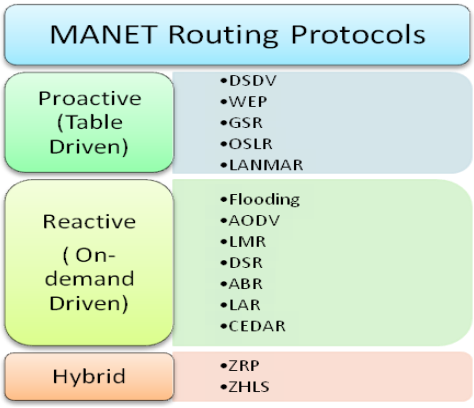

Figure 2: Classification of MANET Routing Protocols.

3. ADHOC ON DEMAND DISTANCE VECTOR PROTOCOL

MANETs and other wireless adhoc networks use this protocol for routing. This protocol is used for unicast as well as for multicast routing. It is a "reactive routing protocol" which is totally demands based by which it routes to a terminal node only when requested [Perkins, 2003]. The most popular routing protocols are proactive where path finding does not depend on path usage. AODV is a distance-vector routing protocol which thwart "counting-to-infinity problem" of other distance-vector

protocols by using sequence number on path updates and network is active only when a path to destination is required by broadcasting a RREQ. AODV node sends request and address of the node sending request; it also creates a pool of transitory paths to the needy node. As soon as a node receives a request message, it checks its route table for the desired path, if it has the path needed; it sends an acknowledgement message along with path info is send back to needy node through the transitory path available to it. Needy node chooses the path with lowest number of hops and then starts using it. After some time, node receives a route error message in case of link failure and the process is repeated. Complex structure of the protocol helps to reduce number of messages which in turn saves the network capacity. As an illustration, a sequence number is assigned to every route request. Repetition of the route request is prevented by a node using this sequence number. Another important attribute of this protocol is time-to-live-number (TTL), which decides the number of times a route request can be regenerated [Lee, 2003]. The other important attribute is in the case of route request failure, double time period than the previous request is provided for accomplishment of this request, then only other request will be forwarded. AODV routing protocol is demand based protocol, in which path finding and connecting are carried out only when requested. Latest path is identified using the destination sequence numbers.

In AODV, corresponding to every data flow, the next-hop information is stored in origin node and intermediate nodes. Route request and route query cycles are used by AODV for constructing routes. In a demand based routing protocol, when a route to the terminal node is unavailable then RouteRequest (RREQ) packet is broadcasted by needy node in the network. A single RREQ can be used to obtain many routes to many destinations. AODV uses a destination sequence number (DestSeqNum) to obtain the current path to the destination while other demand based routing protocols do not. After receiving a DestSeqNum, node compares it with the last DestSeqNum, if it is larger than the previous one, then only node will update its path information to the destination. Each RREQ has the following identifier fields: broadcast identifier (BcastID), source identifier (SrcID), the source sequence number (SrcSeqNum), the destination identifier (DestID), the destination sequence number (DesSeqNum), and the time to live (TTL) field. DestSeqNum also indicates newness of the path to the destination on the basis of which it is approved and used by source. After receiving a RREQ, intermediate node searches its route table for a valid route to valid destination. If route is available, a RouteReply(RREP) is send to the needy node otherwise RREQ is forwarded.

The sequence number of the intermediate node and the DesSeqNum provided by RREQ are compared to check the validity of the path provided by intermediate node. BcastID and SrcID pair is used to check and discard multiple copies of a RREQ, if it is received multiple times. RREP packets are sent to the needy node only by those intermediate nodes which are able to provide valid paths to the destination, or the terminal node. Each intermediate node has to send earlier node ID and its BcastID, when it sends a RREQ to the next node. RREP should be received within the time bound otherwise this entry is deleted.

AODV doesn't use source routing for transmitting data packets, so this time bounding technique is quite helpful to store latest valid path to intermediate node. When a RREP is received by a node, address of the intermediate node sending RREP is also stored so which information can be sent to this node in the next hop forwarding data to the terminal node? A "route error (RERR)" message is sent to the source node by the intermediate node (onwards which path is damaged) to inform the destination that could not be reached. A route discovery can be restarted, if even after receiving RERR node needs the path to the destination [Ehsan, 2012] [Santos, 2005]. Major roles of AODV routing protocol are Path Discovery, Reverse Path Setup as well as Forward Path Setup which affects the path establishment and path maintenance. These are described one by one:

Path Discovery: Path finding is started by source node only when node is desirous to exchange information. It is carried out by broadcasting a "route request (RREQ) packet" towards the adjacent nodes. Two distinct counters namely "Sequence number (SeqNum) and Broadcast-Id (BcastID)" are preserved by each node. The adjacent node either further broadcasts RREQ or satisfies the source node by sending RREP to it. After receiving RREP, subsequent copies of RREQ are dumped.

Reverse Path Setup: Intermediate nodes store the address of the source node sending RREQ to set up a reverse path reflexively. When time period exceeds the time bound, entries are automatically discarded.

Forward Path Setup: Finally, after reaching the node having route to destination unicasts RREP as reply to a RREQ. The RREP is sent along the automatic reverse path available towards source node. A forward pointer is set up at every node along the RREP journey. Also time-out method is practiced and the DesSeqNum of requested destination is recorded.

3.1. AODV Characteristics

AODV Routing Protocol possesses various important characteristics. Out of those some are outlined as follow:

- Protocol searches the route on-demand.
- Information is validated by using a Sequence number assigned uniquely.
- Record of only next hop to the destination is kept instead of the complete route.
- HELLO messages are used to trace neighbors at regular intervals.

3.2. AODV Advantages:

- It is a highly scalable efficient algorithm for Mobile Adhoc Networks.
- It gives quick response in any link breakage in the active routes.
- The routes are established on demand.

- The connection setup delays amid nodes are less.

3.3 AODV Disadvantages:

- Due to multiple RREP as reply to a single RREQ, sometime leads to heavy traffic in the network.
- A lot of extra bandwidth is consumed by this periodic HELLO message.
- If the sequence number of the source is old and the neighboring node has higher but not the latest "destination sequence number", then intermediate nodes can lead to interrupted path, therefore may have corrupt entries.

4. DYNAMIC SOURCE ROUTING PROTOCOL (DSR)

It is specially created to work in a multi-hop wireless adhoc network. It is self-managing, self-assembling; demand based routing protocol which doesn't need any of the pre-existing network infrastructure or a centralized administrative system. DSR protocol has two mechanisms: First is Route Discovery, which manages route formation and second is Route Maintenance, which updates route information in the route table. In DSR, data packets are not send periodically and instead they are sent only when demanded which in-turn reduces data traffic as well as overhead packages [Kurkowski, 2005] [Johnson, 1996] [Valarmathi, 2011]. Before starting the packet transmission, whole route must be known to the routing protocol and this information regarding the route is stored as route cache. The two DSR mechanisms are:

Route Discovery: When a data packet is send by a source node A to the destination node C, firstly it tries to find its "route cache" for the most suited path. If there is no path readily existing, then source node A begins "Route Discovery" by broadcasting a "ROUTE REQUEST (RREQ)" message to fashion a route to C whose fields are given in Table 1.

Table 1: Route request (RREQ) message fields.

Fields	Elucidation
Origin/Initiator ID	Origin/Initiator node's address.
Destination/Target ID	Destination/Target node's address.
Unique request ID	A unique ID to recognize the message.
Address List	Address list of connected nodes of a route from its source to its destination.
Hop Limit	Limits the number of nodes through which message circulates.
Acknowledgement bit	The receiver returns an acknowledgement bit, when a packet is received.

The origin/initiator node set the "address list" to an empty list thereby fixes initiator ID, target ID as well as unique request ID and then broadcasts message. With this it becomes possible for the nodes to receive the packet within the wireless communication area. A copy of the RREQ packet is kept by the sending node in the send buffer. If the route was discovered within specific time, the packet is dropped from the send buffer. After receiving a RREQ message, node checks out target ID to find destination node of the message. If the node itself is not the destination of the message then it tries to find a route to the destination node in its own cache. Message is sent directly if address is found in the route cache otherwise the nodes own id is attached to the address list for broadcasting the RREQ packet. A "ROUTE REPLY (RREP)" message is sent to the initiator node if the node itself is the destination node. The gathered route information from the RREQ message is also provided in this message. The destination node tries to find a route to the sending node in its route cache, because it might require a bidirectional link. In case of unavailability of route in the route cache, route discovery protocol is run and a RREQ message is sent.

Route Maintenance: Since, it is possible which nodes may join or leave the transmission range of the network, so it becomes mandatory to conserve the route information stored in the route cache.

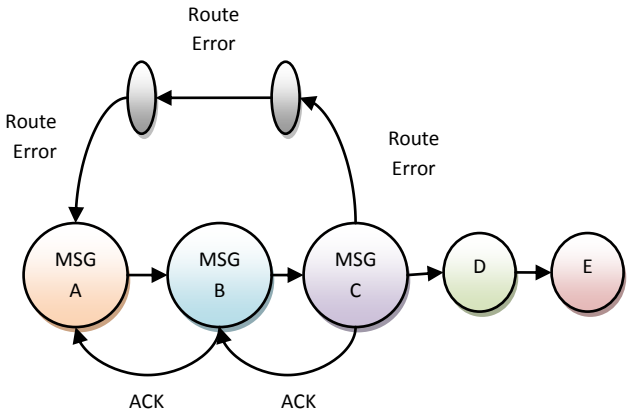

Figure 3: Route maintenance mechanism.

After receiving a packet it is responsibility of which node to ensure which packet is delivered to the next node of the route. In figure 3, it can be seen clearly which system works as a chain where each link ensures which next link is enact. It is also illustrated which the node C can consider another path to communicate with node A. The sending node can acknowledge by setting a bit in the packet header. If a node sends a message and it is not acknowledged, it will retransmit only a fix number of times. If even after which it does not get any acknowledgement then a "ROUTE ERROR (RERR)" message is sent to the sending node of the packet, having the information about the broken link in its message [Broch, 1999] [Johnson, 2007] [Johnson, 1996].

The sending node removes this broken path from its "route cache" and attempts to find another path in its "route cache" for transmitting the packet. If it does not find any path in "route cache", then a RREQ message is transmitted to construct a new path.

5. CONCLUSION

Routing plays most important role in data transfer from the source node to the destination node, which is the most fundamental role of any network. This function is carries out using various techniques. AODV and DSR protocols have both advantages and disadvantages. The researchers may focus on developing such protocols which are more secure than that of AODV and DSR protocols.

6. REFERENCES

[1] Abolhasan (2004), Mehran, Tadeusz Wysocki, and Eryk Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," Ad hoc networks, vol. 2, no. 1, pp 1-22.

[2] Boukerche (2004), Azzedine, Khalil El-Khatib, Li Xu, and Larry Korba, "SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks," In Proceedings of 29th Annual IEEE International Conference on Local Computer Networks, pp 618-624.

[3] Broch (1999), J, D. Johnson, and D. Maltz, "The Dynamic Source Routing Protocol for Mobile Adhoc Networks," IETF Internet draft, pp 1-49.

[4] Clausen (2002), Thomas, Philippe Jacquet, and Laurent Viennot., "Comparative study of routing protocols for mobile ad hoc networks," Med-hoc-Net, INRIA, Projet Hipercom, pp 1-10.

[5] Dhenakaran (2013), S.S, A. Parvathavarthini, "An Overview of Routing Protocols in MANETs," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 2, pp 251-258.

[6] Ehsan (2012), Humaira, Farrukh Aslam Khan, "Malicious AODV," In Proceedings of IEEE 11th International Conference on Trust Security and Privacy in Computing and Communications, pp 1181-1187.

[7] Johnson (1996), David B, and David A. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile computing, pp 153-181.

[8] Johnson (2003), David B, "The dynamic source routing protocol for mobile ad hoc networks," draft-ietf-manet-dsr-09.txt.

[9] Johnson (2007), D,Y. Hu, D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," RFC 4728.

[10] Kakkar (2016), Parveen, Krishan Saluja, "Performance investigations of reactive routing protocols under flooding attack in MANET," In Proceedings of 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp 623-627.

[11] Kumari (2016) , Neelu , Sandeep Kumar Gupta , Rajni Choudhary , Shubh Laxshmi Agrwal, "New performance analysis of AODV, DSDV and OLSR routing protocol for MANET," In Proceedings of 3rd IEEE International Conference on Computing for Sustainable Global Development (INDIACom), pp 33-35.

[12] Kurkowski (2005), Stuart, Tracy Camp, Neil Mushell, and Michael Colagrosso, "A visualization and analysis tool for ns-2 wireless simulations: inspect," In Proceedings of 13th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, pp 503-506.

[13] Layuan (2007), Li, Li Chunlin, and Yaun Peiyan, "Performance evaluation and simulations of routing protocols in ad hoc networks," Computer Communications, vol. 30, no. 8, pp 1890-1898.

[14] Lee (2003), Sung-Ju, Elizabeth M. Belding-Royer, and Charles E. Perkins, "Scalability study of the ad hoc on-demand distance vector routing protocol," International journal of network management, vol 13, no. 2, pp 97-114.

[15] Mittal (2009), S, P. Kaur, "Performance Comparison of AODV DSR and ZRP Routing Protocols in MANET'S," In Proceedings of International Conference on Advances in Computing Control & Telecommunication Technologies ACT '09, pp 165-168.

[16] Neeraj Sharma, B.L. Raina, Prabha Rani, Yogesh Chaba, YudhvirSingh,"Attack Prevention Methods for DDoS Attacks in MANETs", Asian Journal Of Computer Science And Information Technology, ISSN – 2249-5126,Vol 1, Issue 1, pp. 18 – 21 (2011).

[17] Nguyen (2008), Hoang Lan, and Uyen Trang Nguyen, "A study of different types of attacks on multicast in mobile ad hoc networks," Ad Hoc Networks vol.6, no. 1, pp 32-46.

[18] Park (2001), Vincent, "Temporally-ordered routing algorithm (TORA) version 1 functional specification," Internet Draft, draft-ietf-manet-tora-spec-04.

[19] RenuDalal, Manju Khari, Yudhvir Singh, "Survey of Trust Schemes on Ad-hoc Network", Springer - Lecture Notes of the Institute for Computer Sciences, Social Informatics & Telecommunications Engineering (LNICST) Series 84, Springer, NETCOM-3, CCSIT-2012,pp 170-180,(2012).

[20] Perkins (2003), C.E, E. Belding Royer, S.R. Das, "Ad hoc On demand distance vector (AODV) routing," IETF RFC 3561.

[21] Pooja, Manisha, Yudhvir Singh, "Security Issues and Sybil Attack inWireless Sensor Networks", International Journal of P2P Network Trends and Technology,ISSN: 2249-2615, Volume3, Issue1, pp7-13, 2013.

[22] Prabha Rani, Yogesh Chaba, Yudhvir Singh, "Hybrid Approach for Detection and Prevention of Blackhole Attack in Mobile Adhoc Network",International Journal of Wireless Communication, ISSN 0974-9640, pp 885-890, August, 2011.

[23] Preeti, Yogesh Chaba, Yudhvir Singh, "Review of Detection and Prevention of DDOS attack in MANET", Proc. National Conference on Challenges &Opportunities in Information Technology(COIT –2008), India, pp. 56-59 (March 29,2008).

[24] Rahul Rishi, Dheer Dhwaj Barak, Yudhvir Singh, Prabha Rani, "Mobility Analysis of Blackhole Node Attacks in Mobile Adhoc Networks", International Conference on"Recent Trends in Computing, Mechatronics and Communication, India,pp 93-97, February 25-26, 2012.

[25] RenuDalal, Manju Khari, Yudhvir Singh, "Survey of Trust Schemes on Ad-hoc Network", Springer - Lecture Notes of the Institute for Computer Sciences, Social Informatics & Telecommunications Engineering (LNICST) Series 84, Springer, NETCOM-3, CCSIT-2012,pp 170-180,(2012).

[26] Royer (1999), Elizabeth M, and Chai-Keong Toh, "A review of current routing protocols for adhoc mobile wireless networks," IEEE personal communications Vol. 6, no. 2. pp 46-55.

[27] Salehi (2012), Mahmood, and Hamed Samavati, "DSR vs OLSR: Simulation based comparison of ad hoc reactive and proactive algorithms under the effect of new routing attacks," In Proceedings of 6th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST), pp 100-105.

[28] Santos (2005), Rául Aquino, Arthur Edwards, R. M. Edwards, and N. Luke Seed, "Performance evaluation of routing protocols in vehicular ad-hoc networks," International Journal of Ad Hoc and Ubiquitous Computing, vol. 1, no. 1-2, pp 80-91.

[29] Satav (2016), Pravin R, Pradip M. Jawandhiya, "Review on single-path multi-path routing protocol in manet: A study," In Proceedings of International Conference on Recent Advances and Innovations in Engineering (ICRAIE), pp 1-7.

[30] Toh (1997), Chai-Keong, "Associativity-based routing for ad hoc mobile networks," Wireless Personal Communications, vol.4, no. 2, pp 103-139.

[31] Valarmathi (2011), A, and R. M. Chandrasekaran, "Performance of improved dynamic source routing algorithm for military communication logistics," International Journal of Enterprise Network Management , vol. 4, no. 3, pp 302-310.

[32] VikashSiwach,Yudhvir Singh, Seema,DheerDhwaj Barak, "An approach to optimize QoS routing protocol using genetic algorithm in MANET", IJCSMS, ISSN: 2231-5268, Vol 12, Issue 3, pp 149-53, (Sept 2012).

[33] Walikar (2016), Gyanappa A. ,Rajashekar C. Biradar, "A survey on hybrid routing mechanisms in mobile ad hoc networks," Journal of Network and Computer Applications, vol 77, pp48-63.

[34] Yogesh Chaba, Yudhvir Singh, Prabha Rani, "Comparison of Various Passive Distributed Denial of Service Attack in Mobile Adhoc Networks" Proc. WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communication(EHAC 10),Cambridge,UK (ISBN: 978-960-474-155-7), pp 49-53(2010)

[35] Yogesh Chaba, Yudhvir Singh, KP Singh, Prabha Rani, "Performance Modeling of MANET Routing Protocols with Multiple Mode Wormhole Attacks", Communications in Computer and Information Sciences, Springer [Online : Springer Digital Library] (2010) Volume 101, Part 3, pp 518-527, (2010).

[36] Yogesh Chaba, Yudhvir Singh, Aarti, "Performance Analysis of Scalability and Mobility on Routing Protocols in MANETs" International Journal of IT & Knowledge Management (ISSN: 0973-4414) Vol. 1, No. 2, pp. 327-336 (July-Dec, 2008).

[37] Yudhvir Singh, AvniKhatkar, Prabha Rani, Deepika, DheerDhwaj Barak, "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks" Third IEEE International Conference on Advanced Computing & Communication Technologies, 2012.

[38] Yudhvir Singh, Yogesh Chaba, Prabha Rani, "Integrating – VPN and IDS – An approach to Networks Security", International Journal of Computer Science & Security(ISSN: 1985-1533), Vol. 1, Issue 3, pp. 1-13(2007)

[39] Yudhvir Singh, Amit Kumar, Prabha Rani, and Sunil Kumar Kaushik, "Impact of CBR Traffic on Routing Protocols in MANETs", IEEE UKSim-AMSS 16th International Conference on Computer Modelling and Simulation, [Online: IEEE Xplore Digital Library], University of Cambridge, United Kingdom, 26-28, March 2014.

[40] Yudhvir Singh, DheerDhwaj Barak, VikashSiwach,Prabha Rani,"Attacks on wireless sensor networks: a survey", IJCSMS, ISSN: 2231-5268, Vol 12, Issue 3, pp 143-148, (Sept 2012).

[41] Zhang (2006), Yanchao, Wei Liu, Wenjing Lou, and Yuguang Fang, "MASK: anonymous on-demand routing in mobile ad hoc networks," IEEE transactions on wireless communications , vol.5, no. 9, pp 2376-2385.