ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

A Survey on Routing Protocols in Mobile Ad-hoc Networks

Sherjung[1], Dr. R. K.Sharma[2]

Research Scholar, Department of Computer Science and Engineering, Al Falah School of Engineering and Technology, Faridabad, India[1]

Assistant Professor, Department of Computer Science and Engineering, FET,Agra College, Agra, India[2]

ABSTRACT: In this digital era mobile ad-hoc network is an emerging technology that will allow user to access the services without knowing their geographical position. In ad-hoc networks all nodes are mobile and can be connected dynamically in an arbitrary manner. All nodes of mobile ad-hoc networks behave like routers and participate in discovery and maintenance of routes to other nodes in the network. Ad hoc networks are very useful in emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in inhospitable terrain. Because of the nature of ad hoc networks, there are special demands for ad-hoc routing protocols. In this paper we have presented the characteristics and different aspects of routing protocol for MANET.

KEYWORDS: Ad Hoc Networks, routing protocol, performance, DSDV, DSR, AODV

I. INTRODUCTION

A mobile ad hoc network (MANET) sometimes called a *wireless ad hoc network* or a *mobile mesh network* is a wireless network, comprised of mobile computing devices (nodes) that use wireless transmission for communication, without the aid of any established infrastructure or centralized administration such as a base station or an access point [1, 2, 3, 4]. Unlike traditional mobile wireless networks, mobile ad hoc networks do not rely on any central coordinator but communicate in a self organized way. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those far apart rely on other nodes to relay messages as routers. In ad hoc network each node acts both as a host (which is capable of sending and receiving) and a router which forwards the data intended for some other node. Ad hoc wireless networks can be deployed quickly anywhere and anytime as they eliminate the complexity of infrastructure setup.

Applications of ad hoc network range from military operations and emergency disaster relief, to commercial uses such as community networking and interaction between attendees at a meeting or students during a lecture. Most of these applications demand a secure and reliable communication.

Mobile wireless networks are generally more vulnerable to information and physical security threats than fixed wired networks. Vulnerability of channels and nodes, absence of infrastructure and dynamically changing topology, make ad hoc networks security a difficult task [4]. Broadcast wireless channels allow message eavesdropping and injection (vulnerability of channels). Nodes do not reside in physically protected places, and hence can easily fall under the attackers' control (node vulnerability). The absence of infrastructure makes the classical security solutions based on certification authorities and on-line servers inapplicable. In addition to this, the security of routing protocols in the MANET dynamic environment is an additional challenge. Most of the previous research on ad hoc networking has been done focusing only upon the efficiency of the network. There are quite a number of routing protocols proposed [5, 16, 21] that are excellent in terms of efficiency. However, they were generally designed for a non-adversarial network setting, assuming a trusted environment; hence no security mechanism has been considered. But in a more realistic setting such as a battle field or a police rescue operation, in which, an adversary may attempt to disrupt the communication; a secure ad hoc routing protocol is highly desirable. The unique characteristics of ad hoc networks present a host of research areas related to security, such as, key management models, secure routing protocols,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

instruction detection systems and trust based models. This thesis work is based on the research done in the area of secure routing.

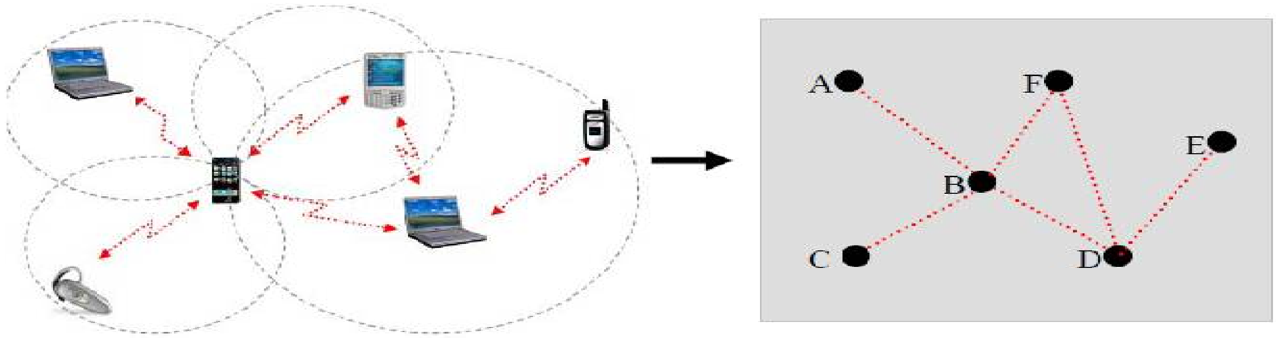

Figure 1: A typical Model of Mobile Ad-hoc Network

Paper Outline

The rest of the paper is organized as follows: Section II presents routing in MANETs. Section III presents classification of various routing protocols. Section IV presents comparison between Routing Protocols, V presents the conclusion.

Routing Protocols

Since the advent of Defense Advanced Research Projects Agency (DARPA) packet radio networks in the early 1970s [1], numerous routing protocols have been developed for ad hoc mobile networks [2, 5]. As shown in Figure 2, these are generally categorized as table-driven or proactive, on-demand or reactive and hybrid routing protocols.

II. CLASSIFICATION OF ROUTING PROTOCOLS

Table-driven or Proactive Protocols: Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating, proactively, route updates at fixed intervals. As the resulting information is usually maintained in tables, the protocols are sometimes referred to as table-driven protocols. Representative proactive protocols include: Destination-Sequenced Distance- Vector (DSDV) routing [7], Clustered Gateway Switch Routing (CGSR) [8], Wireless Routing Protocol (WRP) [9], and Optimized Link State Routing (OLSR) [10].

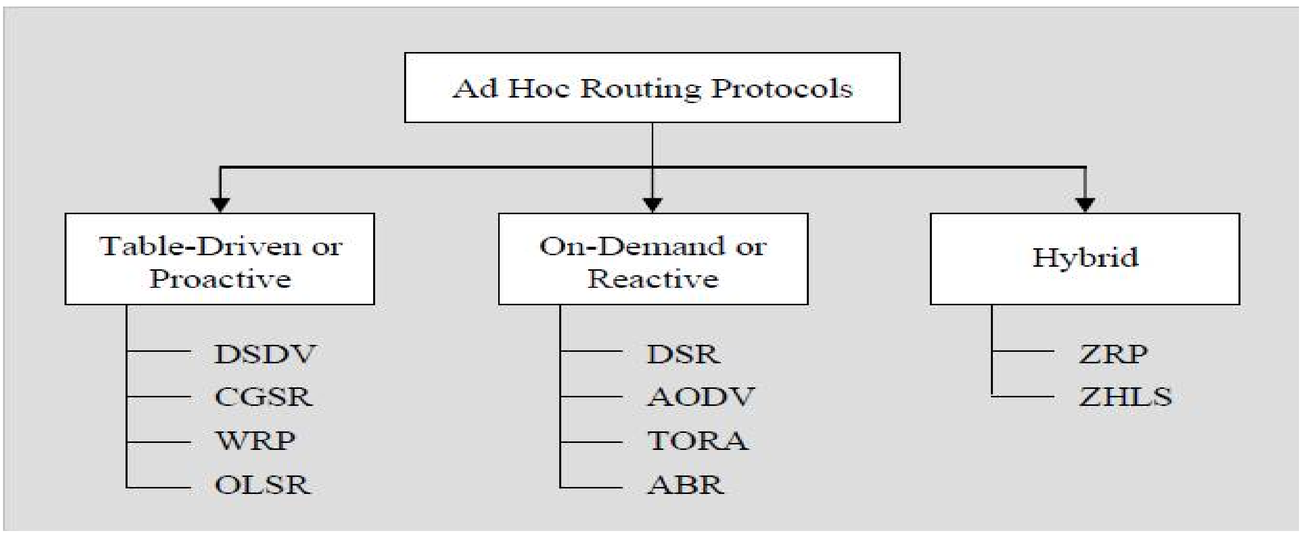

Figure 2: A classification of Ad-hoc Routing Protocols

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

a) **Destination Sequenced Distance Vector (DSDV):** DSDV is proposed by Perkins and Bhagwat. The Destination-Sequenced Distance-Vector (DSDV) [14] Routing protocol is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements such as making it loop-free. The distance vector routing is less robust than link state routing due to problems such as count to infinity and bouncing effect. In this, each device maintains a routing table containing entries for all the devices in the network. In order to keep the routing table completely updated at all the time each device periodically broadcasts routing message to its neighbour devices. When a neighbour device receives the broadcasted routing message and knows the current link cost to the device, it compares this value and the corresponding value stored in its routing table. If changes were found, it updates the value and re-computes the distance of the route which includes this link in the routing table.

b) **Clustered Gateway Switching Routing Protocol (CGSR):** The Cluster head Gateway Switch Routing protocol differs from the other protocols as it uses hierarchical network topology, instead of a flat topology. As proposed by Chiang, it organizes nodes into clusters, which coordinate among the members of each cluster entrusted to a special node named cluster head. Least Cluster Change (LCC) algorithm [21] is applied to dynamically elect a node as the cluster head. Each node must keep a cluster member table where it stores the destination cluster head for each mobile node in the network. These cluster member tables are broadcast by each node periodically using the DSDV algorithm. CGSR is an extension of DSDV and hence uses it as the underlying routing scheme. It has the similar overhead as DSDV. However, it modifies DSDV by using a cluster (hierarchical) routing approach to route traffic from source to destination. CGSR improves the routing performance by routing packets through the cluster heads and gateways.

c) **Wireless Routing Protocol (WRP):** WRP is a loop free protocol. Every node in the network uses four tables:

- Distance table(DT)
- Routing table (RT)
- Link-cost table (LCT)
- Message retransmission list (MRL) table[18]

The protocol being proactive maintains the routing information of the entire network in the tables. The protocol forces every node to perform check on consistency of predecessor information which is reported by all of its neighbors. Due to this, it faces the count-to-infinity problem. However, the looping conditions get eliminated due to these consistency checks. Hello messages get exchanged time to time for neighbor sensing and update messages are exchanged between neighbors in case of link failures.

d) **Optimized Link State routing (OSLR):** Clausen and Jacquet proposed the Optimized Link State Protocol, a point-to-point proactive protocol that employs an efficient link state packet forwarding mechanism called multipoint relaying [24, 25]. Here, route information always stored in table. Therefore, route is always available when needed. Thus, being proactive delay is less as no waiting will be there for route discovery. Link state packets are being forwarded for topology information which is called Multi point relay (MPR). Here, each node selects its MPR from neighbour nodes. Periodic exchange of link state packets will be done in order to gather information about the nodes and their topology. OLSR uses two types of packets:

- HELLO Message
- TOPOLOGY CONTROL (TC) Message[21]

Hello message is used as beacon message *i.e.*, checking the presence of the neighbors and also used for MPR selection. TC message is used for route calculation.

On-demand or Reactive Protocols: A different approach from table-driven routing is reactive or on-demand routing. These protocols depart from the legacy Internet approach. Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network. Once a route has been established, it is maintained by the node until either the destination becomes inaccessible or until the route is no longer used or has expired. Representative reactive routing protocols include: Dynamic Source Routing (DSR) [12], Ad hoc On Demand Distance Vector (AODV) routing [13], Temporally Ordered Routing Algorithm (TORA) [14] and Associativity Based Routing (ABR) [15].

a) Dynamic Source Routing (DSR): DSR is an on-demand protocol designed by D. B. Johnson, Maltz and Broch to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

periodic table update messages required in the proactive routing protocols. The distinguishing feature of Dynamic Source Routing (DSR) [28] is the use of source routing. DSR is a reactive protocol i.e. it doesn't use periodic updates. It computes the routes when necessary and then maintains them. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass, the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host.
The protocol basically consists of two steps [26], [27]

- Route Discovery
- Route Maintenance

Route Discovery: Since DSR is a reactive protocol, route discovery is required *i.e.*, route is made available when required. For Example, node A wants to communicate to node B, then node A will start route discovery by forwarding the packet to its neighbours. The packet will be forwarded until packet reaches to its intended destination. There will be more than one path available for the destination. The Path will be chosen based upon required condition like shortest distance, collision free.
Route Maintenance: Since nodes are continuously roaming in the network, their topology keeps changing. Thus, the alternative routes can be used. If route is not available, then route discovery is invoked. This scenario is known as Route Maintenance.

b) Ad-hoc On-demand Distance Vector (AODV): The basic operation of AODV can be divided into three phases:

- Route discovery
- Route maintenance
- Acknowledge messages

The message types defined by AODV are Route Request (RREQ), Route Reply (RREP) and Route Error (RERR).

AODV is a widely accepted on-demand routing protocol in ad hoc networks proposed by C. E. Perkins and E. M. Royer. Ad hoc On-demand Distance Vector (AODV) [25] is a combination of both DSR and DSDV. It follows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV. It uses destination sequence numbers to ensure loop freedom at all times and by avoiding the Bellman-Ford "count-to infinity" problem offers quick convergence when the ad hoc network topology changes. AODV finds routes only when required and hence is reactive in nature.

c) Temporally-Ordered Routing Algorithm (TORA): The Temporally-Ordered Routing Algorithm (TORA) was developed by Park and Corson. Temporarily ordered routing algorithm **(**TORA) is highly adaptive, loop-free, distributed routing algorithm based on the concept of link reversal. It uses directed acyclic graphs (DAG) to define the routes either as upstream or downstream. This graph enables TORA to provide better route aid for networks with dense, large population of nodes. TORA involves four major functions: creating, maintaining, erasing and optimizing routes. Since every node must have a height, any node which does not have a height is considered as an erased node and its height is considered as null. Sometimes the nodes are given new heights to improve the linking structure. This function is called optimization of routes.

d) Associativity Based Routing Protocol (ABR): The Associativity Based Routing (ABR) protocol is a new approach for routing .ABR defines a new metric for routing known as the degree of association stability. It is free from loops, deadlock, and packet duplicates. In ABR, a route is selected based on associativity states of nodes. The routes thus selected are liked to be long-lived. All node generate periodic beacons to signify its existence. When a neighbour node receives a beacon, it updates its associativity tables. For every beacon received, node increments its associativity tick with respect to the node from which it received the beacon. Association stability means connection stability of one node with respect to another node over time and space. A high value of associativity tick with respect to a node indicates a low state of node mobility, while a low value of associativity tick may indicate a high state of node mobility. Associativity ticks are reset when the neighbors of a node or the node itself move out of proximity. The fundamental objective of ABR is to find longer-lived routes for ad hoc mobile networks. The three phases of ABR are:

- Route discovery

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

- Route reconstruction (RRC)
- Route deletion

Hybrid Routing Protocols: Purely proactive or purely reactive protocols perform well in a limited region of network setting. However, the diverse applications of ad hoc networks across a wide range of operational conditions and network configuration pose a challenge for a single protocol to operate efficiently [3]. For example, reactive routing protocols are well suited for networks where the call-to-mobility ratio is relatively low. Proactive routing protocols, on the other hand, are well suited for networks where this ratio is relatively high. The performance of either class of protocols degrades when the protocols are applied to regions of ad hoc networks space between the two extremes.

a) Zone Routing Protocol (ZRP): Haas and Pearlman proposed Zone Routing Protocol. ZRP [29] is a hybrid routing protocol for mobile ad hoc networks which localizes the nodes into sub-networks (zones). Every node's routing zone is described by zone radius which is expressed in terms of hops. Inside the zone Proactive Routing is used provided by Intra Zone Routing protocol (IARP). Thus routes are easily available using IARP. Outside the zone Reactive routing is used provided by Inter Zone Routing Protocol (IERP). The special feature that ZRP uses is *border-casting i.e.*, if a node wants to communicate a node which is outside its zone, then instead of broadcasting the packets it border-cast it to the peripheral (border) nodes using information provided by IARP. The border-casting technique is provided by Border-cast Resolution Protocol (BRP).

b) Zone-Based Hierarchical Link State Routing Protocol (ZHLS): ZHLS is based on hierarchical structure in which the network is divided into non-overlapping zones. According to Joa and Lu [30], each node is assigned one unique node ID and a zone ID, which are calculated using geographical information. Hence the network follows a two-level topology structure: node level and zone level. Respectively, there are two types of link state updates: the node level LSP (Link State Packet) and the zone level LSP. A node level LSP contains the node IDs of its neighbours in the same zone and the zone IDs of all other zones. A node periodically broadcast its node level LSP to all other nodes in the same zone. Before transmission, the source node first checks its intra-zone routing table. If the destination lies in its zone, the routing information is already present. Otherwise, the source sends a location request to all other zones through gateway nodes, which in turn replies with a location response containing the zone ID of the desired destination. The header of the data packets originated from the source contains the zone ID and the node ID of the destination node.

III. COMPARISON BETWEEN ROUTING PROTOCOLS

In this section we have discussed the parameters based comparison of three types of routing protocols.

Parameters	Proactive	Reactive	Hybrid
Memory Overhead	More as table is maintained	Less as no table is maintained.	Depends whether routing is inside and outside the zone.
Availability of Route	Always available	On demand, Route Discovery will be done	Both
delay	Low	High	Low for local destinations and high for Interzone
Scalability	100 Nodes	>100 nodes	>1000 nodes
Network structure	Flat and Hierarchical	Flat	Mostly Hierarchical
Routing information	Stored in table	Doesn't stored information.	Inside the zone information is stored in table; outside the zone no information is stored.
Traffic control	High	Low.	Lower than both
Periodic updates of information	Required for table maintenance	Not required	Required inside the zones.
Network structure	Flat and Hierarchical	Flat	Mostly Hierarchical

Table 1 Comparison between the three types of Routing Protocols

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

IV. CONCLUSION

In this paper, we have discussed the taxonomy of routing protocols in mobile ad hoc networks and provided comparisons between them. The protocols are divided into three main categories: (i) source-initiated (reactive or on-demand), (ii) table-driven (pro-active), (iii) hybrid protocols. For each of these classes, we reviewed and compared several representative protocols. While there are still many challenges facing Mobile ad hoc networks related to routing and security. Each routing protocol has unique features. Based on network environments, we have to choose the suitable routing protocol. The analysis of the different proposals has demonstrated that the inherent characteristics of ad hoc networks, such as lack of infrastructure and rapidly changing topologies, introduce additional difficulties to the already complicated problem of secure routing. At last we have provided the overall characteristic features of all routing protocols and described which protocols may perform best in large networks. Almost all the protocols we discussed in this paper have their own characteristic features and performance parameter combinations where they out perform their competitors.

REFERENCES

[1] C. Siva Ram Murthy and B. S Manoj, "Ad Hoc Wireless Networks, Architecture and Protocols", Prentice Hall PTR, 2004.
[2] Stefano Basagni, Macro Conti, Silvia Giordano and Ivan Stojmenovic, "Mobile Ad Hoc Networks" , IEEE press, A john Wily & Sons, INC. publication, 2003
[3] George Aggelou, "Mobile Ad Hoc Networks", 2nd edition, Mc GRAW Hill professional engineering, 2004
[4] Imrich Chlamtac, Marco Conti, Jenifer J.-N. Liu, "Mobile Ad Hoc Networking: Imperatives and Challanges", Elsevier Network Magazine, vol. 13, pages 13-64, 2003
[5] E.M. Belding-Royer and C. K. Toh, "A review of current routing protocols for adhoc mobile wireless networks", IEEE Personal Communications Magazine, pages 46–55, April 1999.
[6] Behrouz A. Forouzan, "Data communication and Networking," 2nd edition, Tata McHill publication, 2001
[7] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Comp. Commun. Rev., Oct. 1994, pp. 234–44.
[8] C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. IEEE SICON '97, Apr. 1997, pp. 197–211.
[9] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183–97.
[10] P. Jacquet, P. Muhlethaler, A. Qayyum, "Optimized Link State Routing Protocol", Internet Draft, draft-ietf-manetolsr- 00.txt, November 1998.
[11] A. Laouiti, A.Qayyum, and L.Viennot, "Multipoint Relaying; An Efficient Technique for Flooding in Mobile Wireless Networks," in Proceeedings of the 35th Annual Hawaii International Conference on System Science (HICSS' 2002), Waikoloa, HI, January 2002.
[12] D.B. Johnson, D.A. Maltz, "Dynamic source routing in adhoc wireless networks", in: T. Imielinski, H. Korth (Eds.), Mobile Computing, Kluwer Academic Publishers, Dordrecht, 1996, pp. 153–181.
[13] C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector routing", In IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, Feb. 1999.
[14] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," Proc. INFOCOM '97, Apr. 1997.
[15] C-K. Toh, "A Novel Distributed Routing Protocol to Support Ad-Hoc Mobile Computing", Proc. 1996 IEEE 15th Annual Int'l. Phoenix Conf. Comp. and Commun., Mar. 1996, pp. 480–86.
[16] Haas Z. J., Pearlman M. R., and Samar P., "The Zone Routing Protocol (ZRP)", IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.
[17] Jan Schaumann, "Analysis of Zone Routing Protocol", Course CS765, Stevens Institute of Technology Hoboken, New Jersey, USA, 8th December 2002
[18] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: "Intrazone Routing Protocol (IARP)", IETF Internet Draft, draft-ietf-manet-iarp-01.txt, June 2001
[19] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: "Interzone Routing Protocol (IERP)", IETF Internet Draft, draft-ietf-manet-ierp-01.txt, June 2001
[20] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: "The Bordercast Resolution Protocol (BRP) for Ad Hoc Networks", IETF Internet Draft, draft-ietf-manet-brp- 01.txt, June 2001
[21] M.Joa-Ng and I. T. Lu, "A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks," IEEE journal on Selected areas in Communications, vol. 17, no. 8, pp. 1415- 1425, August 1999
[22] L. Zhou and Z. J Haas, "Securing Ad Hoc networks," IEEE Network Magazine, vol. 13, no. 6, December 1999
[23] M. O. Pervaiz, M. Cardei, and J. Wu, "Routing Security in Ad Hoc Wireless Networks," Network Security, S. Huang, D. MacCallum, and D. -Z. Du (eds.), Springer, 2008.
[24] L. Abusalah, A. Khokhar and M. Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols", "*IEEE Communications Surveys& Tutorials"*, vol. 10 no. 4, 4th Quarter 2008.
[25] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum, L.Viennot, "Optimized link state routing protocol for ad hoc networks," in: "*Proceedings of IEEE INMIC"*, December 2001, pp. 62–68.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

[26] Bounpadith Kannhavong, Hidehisa nakayama, Yoshiaki nemoto, and Nei kato, "A survey of routing attacks in mobile ad hoc networks", IEEE Wireless Communications, vol. 14, Issue 5, pp.85-91, 2007
[27] Bhavyesh Divecha, Ajith Abraham, Crina Grosan and Sugata Sanyal, "Analysis of Dynamic Source Routing and Destination-Sequenced Distance-Vector Protocols for Different Mobility models" First Asia International Conference on Modeling and Simulation, pp. 224-229, 2007
[28] D. B. Johnson, D.A Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks," "*Ad Hoc Networking"*, C.E. Perkins, Ed., Addison-Wesley, 2001, 139- 172.
[29] Z. J. Haas and M. R. Pearlman, .ZRP: a hybrid frame work for routing in ad hoc networks, pp. 221.253, 2001.
[30] M. Joa-Ng, I.-T. Lu, "A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks," "*IEEE Journal on Selected Areas in Communications* 17 (8) (1999) 1415–1425".