A SURVEY OF ENHANCED ROUTING PROTOCOLS FOR MANETs

Vivek Arya and Charu

Department of Computer Science and Engineering,
Jaypee Institute of Information Technology
Sector 128, Noida
88vivekarya@gmail.com,
charu.kumar@jiit.ac.in.

ABSTRACT

Mobile Ad Hoc Networks (MANETs) form a class of dynamic multi-hop networks consisting of a set of mobile nodes that intercommunicate on shared wireless channels. MANETs are self-organizing and self-configuring multi-hop wireless networks, where the network structure changes dynamically due to the node mobility. There exists no fixed topology due to the mobility of nodes, interference, multipath propagation and path loss. Hence efficient dynamic routing protocols are required for these networks to function properly. Many routing protocols have been developed to accomplish this task. In this paper we survey various new routing protocols that have been developed as extensions or advanced versions of previously existing routing protocols for MANETs such as DSR, AODV, OLSR etc.

KEYWORDS

Wireless, Mobile Ad Hoc networks, Routing protocols

1. INTRODUCTION

Mobile Ad Hoc Networks are wireless networks where nodes communicate with each other using multi-hop links. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/from other nodes. Routing in ad hoc networks has been challenging ever since wireless networks came into existence. The major reason for this is the constant change in the network topology because of the high degree of node mobility. A number of routing protocols have been established or proposed for efficient routing in Mobile Ad Hoc networks.

The traditional routing protocols developed for wired networks do not meet the demands of routing in mobile ad hoc networks due to frequent change in topology of mobile nodes and power constraint. Existing distance-vector and link-state based routing protocols are unable to catch up with frequent link changes in ad hoc wireless networks, resulting in poor route convergence and very low communication throughput. Therefore new routing protocols have been developed or proposed to address the concerns of routing in mobile ad hoc networks.

The paper is organized as follows. Section 2, explains the routing concept in MANETs and classifies them according to path searching strategies. Section 3, discusses various existing proactive and reactive routing protocols. In Section 4, we review new routing protocols that have

DOI : 10.5121/ijans.2013.3301

been proposed to enhance and overcome shortcomings that exist in these existing protocols. We study them in detail discussing the techniques used, their advantages and disadvantages. In Section 5, we conclude our paper.

2. ROUTING IN MANETs

Routing protocols for Ad Hoc networks can be classified into two main categories: proactive and reactive routing. Hybrid protocols also exist which use a combination of both proactive and reactive. Proactive protocols are directly inspired by routing protocols deployed in the internet and are thus adaptations of link state routing and distance vector routing protocols. Their common characteristic is that each ad hoc network node locally maintains a routing table for sending data to any node in the network. With these protocols, terminals periodically exchange information beyond their direct neighborhood for permanently maintaining routing tables describing network topology. They are also called table-driven ad hoc routing protocols. The disadvantage of proactive protocols is the excessive consumption of bandwidth by passing a large number of control messages due to frequent topology changes. Ad hoc reactive routing algorithms minimize the use of control messages to a minimum to save bandwidth. The information vital to the calculation of a route between two network nodes is only researched when a request for this route is created. The major drawback of this type of protocols is the important delay between a request for message transmission and the actual transmission when the route has not yet been created. Hybrid MANET routing protocols combines the best features of both proactive and reactive routing protocols. However, several routing protocols have been developed for ad hoc networks, still efficient routing which takes into consideration energy, bandwidth, mobility, multipath, Quality of Service (QoS), security etc is an area of research.

3. PROACTIVE, REACTIVE AND HYBRID ROUTING PROTOCOLS

Routing is the act of moving information from a source to destination in an inter-network. Ad Hoc Routing protocols can be categorized as proactive (table-driven) and reactive (source-initiated). We discuss the most widely used traditional proactive and reactive routing protocols.

Destination Sequenced Distance Vector (DSDV) [1] is a proactive routing protocol which is a modification of the conventional Bellman Ford routing algorithm. This protocol adds a new attribute, sequence number, to each route table entry at each node. Each node in the network maintains a routing table for transmission of packets and also for connectivity to different stations in the network. The routing entry is tagged with a sequence number which is originated by the destination station. The usage of sequence numbers provides loop freedom. In order to maintain consistency each station transmits and updates its routing tables periodically. DSDV protocol requires that each mobile station in the network, must constantly advertise to each of its neighbor, its own routing table. DSDV provides an option of route updates using the full or incremental update strategies. However, it becomes difficult to maintain routing table's advertisements for large networks using this technique.

Optimized Link State Routing (OLSR) [2] is a proactive (table driven) protocol which can be considered as an adaptation to the ad hoc network world of the OSPF (Open Shortest Path First) protocol deployed in wired internet. AODV employs periodic exchange of messages to maintain topology information of the network at each node. OLSR is an optimization over a pure link state

protocol optimizing the global broadcast operation or flooding. The OLSR protocol defines the multipoint relay concept (MPR) [3] to limit the number of message retransmissions during the necessary flooding operations. OLSR works best for large and dense ad hoc networks. However, OLSR being a a reactive routing protocol suffers from excessive routing overhead.

Temporally Ordered Routing Algorithm (TORA) [4] is a highly adaptive, loop-free, distributed routing algorithm based on the concept of link reversal. TORA is designed to operate in highly dynamic mobile networking environment. It is source initiated and provides multiple routes for any source/destination pair. The key design concept of TORA is the localization of control messages to a very small set of nodes near the occurrence of a topological change. To accomplish this, nodes need to maintain routing information about adjacent (one-hop) nodes. During the route creation and maintenance phases, nodes use a height metric to establish a DAG (directed acyclic graph) rooted at the destination. Thereafter links are assigned a direction (upstream or downstream) based on the relative height metric of neighboring nodes. Information may flow from nodes with higher height to nodes with lower height. By maintaining a set of totally-ordered heights at all times, TORA achieves loop free multipath routing, as information cannot flow upstream and so cross back on itself.

Dynamic Source Routing (DSR) [5] protocol is one of the most efficient reactive routing protocols in mobile ad hoc networks. The DSR protocol uses a process of route discovery between two network nodes when it is necessary for a specific communication. When a node wants to send a data message to another node, it searches for a route in its local cache. If no route for this terminal is found, a process of route discovery is activated in order to find the path to the destination node. The node wanting route discovery generates a route request (RREQ) control message. This control message is broadcast to all its neighbors. This message contains the identity of the initiating node, destination node and a unique sequence number determined by the initiating node. When a node receives a RREQ message, it generates a response message, a route reply (RREP), if it is the recipient of the route request; if not, it adds its identity at the end of the intermediate nodes list and rebroadcasts this modified message over the radio interface.

Ad Hoc On Demand Distance Vector (AODV) [6] protocol is a reactive protocol in which the routes are created only when required. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up-to-date and to prevent routing hops. AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes. However, AODV retains the desirable features of DSR, that routes are maintained only between nodes which need to communicate. Route Requests are forwarded in manner similar to DSR. When a node re-broadcasts a route request (RREQ) it sets up a reverse path pointing towards the source. AODV assumes symmetric (bi-directional) links. When the intended destination receives a Route Request, it replies by sending a route reply (RREP). Route reply travels along the reverse path set-up when route request (RREQ) is forwarded.

Zone Routing Protocol (ZRP) [7] provides a hybrid proactive/reactive routing framework in an attempt to achieve scalability. In ZRP, the network is divided into zones. A proactive table driven strategy is used for establishment and maintenance of routes between nodes of the same zone, and a reactive on demand strategy is used for communication between nodes of different zones. When a destination is out of the zone, on-demand routing search is initiated. In this situation, control

overhead is reduced, compared to both the route request flooding mechanism employed in on demand protocols and periodic flooding of routing information packet in table driven protocol.

The above discussed routing protocols have certain disadvantages such as in DSDV wastage of bandwidth occurs due to unnecessary routing. DSDV is not suitable for large networks. In DSR the packet header length grows with route length due to source routing. Increased contention occurs if too many route replies come back due to nodes replying using their local cache. This is also known as the Route Reply Storm Problem. Stale caches also lead to increased overhead. Although AODV being an efficient protocol than DSR has a few disadvantages. Intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence numbers, thereby having state entries. Also, multiple RouteReply packets in response to a single RouteRequest packet can lead to heavy control overhead. Unnecessary bandwidth consumption is also prevalent in AODV due to periodic beaconing. OLSR protocol also suffers certain disadvantages such as lack of security, routing overhead and no support for multicast. ZRP being a hybrid also requires proper query control, without which ZRP can actually perform worse than most flooding based protocols.

However although efficient in transporting packets from source to destination these routing protocols do not address issues like security, trust/reputation of neighbor nodes, energy constraints, bandwidth, congestion in the network etc. The new routing protocols we study in this paper take into consideration certain above factors and try to improve these existing routing protocols.

4. IMPROVEMENTS TO EXISTING ROUTING PROTOCOLS

Various new routing protocols have been developed and proposed that try to overcome certain but not all limitations that exist in previous routing protocols. The new protocols are an improved extension of the standard MANET routing protocols. In this section we discuss few of these routing protocols.

Bandwidth Aware Weight Based DSR Protocol for Mobile Ad Hoc Networks (BAWB-DSR) [8] is an improvement to the existing DSR protocol and the weight based DSR. The weight based DSR (WBDSR) [9] is an improvement to the existing DSR protocol. This protocol solves the problem of energy efficiency in DSR. It also takes into account the stability of nodes. It does not consider the bandwidth of links between nodes and each node inserts its node weight in RREQ packet thus increasing the packet size resulting in overhead to each intermediate node. The BAWB-DSR solves the routing problem by taking bandwidth into account along with stability and battery power of routing nodes. The bandwidth parameter is calculated using the link utilization factor and the throughput. The stability parameter is decided based on the frequent changes in the relative position of a node with its neighborhood. The BAWB-DSR protocol solves partly the energy efficiency routing problem in mobile ad hoc networks. It incorporates bandwidth in its routing algorithm which is necessary to satisfy the quality of service (QOS) demands such as in multimedia applications and video conferencing.

Cumulative Congestion State Routing Protocol (CCSR) [10] is an improvement of existing DSR protocol which takes congestion into account. Congestion is the main reason for packet loss in mobile ad hoc networks. The CCSR protocol performs routing by distributing load between

multiple paths according to the congestion status of the whole path. It also tries to prevent congestion occurring in the first place. CCSR uses congestion status of whole path (congestion status of all the participating in the route path) and the source node maintains a table called the Congestion Status Table (CST) that contains the congestion status of every path from source node to destination node. The protocol assigns threshold values to the congestion status parameter. And the source node distributes more packets towards the path with less congestion status while sending less or no packets to a path with more congestion status. It calculates congestion status of a particular node using its available buffer size or queue length and no of packets. CCSR protocol thus solves the congestion routing problem in mobile ad hoc networks and outperforms both AODV and DSR based on performance.

Reputation-Aware Multi-Hop Routing Protocol (RAMP) [11] performs routing in a mobile ad hoc network based on DSR protocol and takes advantage of congestion control in TCP for reputation/trust management. In multi-hop routing protocols in mobile ad hoc networks, all the nodes are assumed to be cooperative. However, this assumption does not hold when the nodes selfishly behave to reduce their own resource to utilization. This severely hinders the routing process. Therefore, RAMP tries to enforce node cooperation by quantifying the reputation/trust value of each node. RAMP is the first protocol to employ the Additive Increase Multiplicative Decrease (AIMD) algorithm to evaluate each node's routing behaviors and integrity on the evaluation of other nodes. RAMP significantly performs better than its closest counterpart CONFIDANT [12] which uses a complex Bayesian estimate to compute the reputation values in each node. RAMP performs better than existing schemes since the monitored behavior are detected and discouraged in RAMP more efficiently and with less communication overhead.

AODV with Sufficient Bandwidth Aware Routing Protocol (AODV-SBA) [13] is an advancement of AODV routing protocol that improves the performance of on-demand routing protocols by discovering better routes to avoid congestion and reducing excessive routing overheads. The protocol uses a light weight mechanism to determine network congestion. It measures local network congestion using information from the MAC layer. Hence, preventing the discovery of routes over which it is undesirable to carry additional data and routing traffic over those hops that are already busy. It uses Channel Free Time as a metric in route establishment phase. The channel free time is determined using the status flags in IEEE 802.11. The CFT is assigned a threshold value and the packet forward or drop status is decided on its basis. AODV-SBA thus retains the essential features of AODV while significantly increasing the performance in networks with high congestion by selecting routes by avoiding the congested area. It also reduces the routing overhead as well as the battery power consumption to enhance the network lifetime.

Robust Cluster Based Routing Protocol (CBRP-R) [14] is a self-repair cluster based routing protocol based on ad hoc on demand distance vector (AODV) routing. It also uses a Third Party Route Reply thus benefitting the overall network performance. In CBRP-R nodes are organized into hierarchical structure of multi hop clusters. Each cluster comprises of a distinguished node called the cluster head, several gateway nodes which are located between multiple clusters and a number of ordinary nodes. Intra cluster routing is performed using reactive routing protocol while inter cluster routing is performed via proactive routing protocols. The protocol tries to repair a broken route rather than sending error messages. The intermediate nodes start performing route repair as soon as a link break is detected. The route repair process is performed within a threshold time-to-live (TTL) period. On failing a route repair fail (RPF) message is send to the previous

hop. The process is repeated for every node up till the source till a repair is not performed hence acting as a self-repair technique. The protocol thus provides an efficient routing technique that saves considerable amount of network bandwidth for larger mobile ad hoc networks.

Cluster-Based Trust-Aware Routing Protocol (CBTRP) [15] is a wireless routing protocol that protects forwarded packets from intermediary malicious nodes. It is a significant improvement over cluster based routing protocol and the 2 ACK based trust scheme [16]. CBTRP ensures trustworthiness of cluster-heads by replacing them as soon as they become malicious and dynamically updates the packet path to avoid malicious routes. It calculates trust based on vital information regarding other nodes such as by analyzing the received, forwarded and overheard packets. It uses a simple concept of positive and negative events to calculate trustworthiness of a node. A positive event for a node is measured based on certain information such as timely forwarding of packets, generation of successful replies, generation of successful acknowledgements etc. A negative event can be generated if a node refuses to forward a packet to save its energy or out of malicious behavior, forwarding route requests or route replies abnormally, modifying data etc. Thus CBTRP provides improved connectivity in MANETs in the presence of malicious nodes. It ensures the passage of packets through trusted routes only by making nodes monitor the behavior of neighbor nodes.

Energy-Aware Optimized Link State Routing (EOLSR) [17] is an energy efficient version of the optimized link state routing protocol. It aims in reducing the energy spent in the transmission of packets from source to destination. EOLSR uses an energy consumption model for path selection. It uses efficient algorithms to select energy aware multipoint relays, compute energy efficient routes and to optimize broadcasts. The main feature of EOLSR is that, instead of using the number of hops metric between source to destination to select the shortest route, as done in OLSR, it uses a certain COST(flow) as the criterion to choose the best path. COST(flow) is calculated using sum of all energies spent in transmitting packets plus all sum of all energies spent in receiving packets. It defines the notion of energy aware multipoint relays (EMPRs) which are selected on the basis of energy threshold levels. Thus, EOLSR is able to reduce the problem of energy efficiency bei=ng faced in crucial wireless ad hoc and sensor networks and further maximizing network performance.

Secure Efficient AODV Routing (SEAODV) [18] is a reactive routing protocol based upon AODV routing algorithm. It provides secure routing and protection of packets. SEAODV requires one-way hash function in each node and HEAP [19] authentication scheme for protecting sequence number and hop count and authenticating routing packets of AODV such as RREQ, RREP and RERR. SEAODV is the first protocol that uses the HEAP mechanism. HEAP is an effective authentication mechanism based on the HMAC algorithm [20]. In HEAP intermediate node can authenticate received packets and decide whether to forward or drop. SEAODV uses symmetric cryptography and addresses attacks like packet forgery and denial of service (DoS).

Trust Aware Routing Protocol (TARP) [21] is a reactive routing protocol that provides secure routing in mobile ad hoc networks. It uses DSR protocol for finding the shortest path to the destination. TARP

Classification Parameter	Routing Protocols Studied										
	BAWB-	CCSR	RAMP	AODV-	CBRP-	CBTRP	EOLS	SEAOD	TARP	EPA	AD

S	DSR			SBA	R		R	V		OMDV	SR
Class	Reactive	Reactive	Reactive	Reactive	Reactive	Reactive	Pro Active	Reactive	Reactive	Reactive	Reactive
Extension of Routing Protocol	DSR	DSR	DSR	AODV	AODV + CBRP	CBRP	OLSR	AODV	DSR	AODV	DSR
Bandwidth Aware	✓	✓	×	✓	✓	×	✓	×	✓	×	×
Energy Aware	✓	×	×	×	×	×	✓	×	✓	✓	×
Congestion Control	×	✓	✓	✓	×	×	×	×	×	✓	✓
Reputation/Trust Aware	×	×	✓	×	×	✓	×	×	✓	×	×
Secure	×	×	✓	×	×	✓	×	✓	✓	×	×
Multipath	×	✓	×	×	×	×	×	×	×	✓	×

Table 1: Classification of Protocols based on routing parameters

selects routes to the destination based on certain security parameters. These security parameters are the software configuration, hardware configuration, battery power, exposure and organizational hierarchy. Each node evaluates the trust level of its neighbors based on above parameters and includes it in computing the next hop node in the overall shortest path computation. In TARP, power and software configuration are the main contributing features towards routing. It modifies the RREQ packet fields to incorporate node power levels and type of encryption technique used. It denotes power value as low, medium, high and very high. Encryption techniques can be any one of the following: RSA, DES/3DES, BLOWFISH, IDEA, SEAL RC2/RC4/ RC5/RC6). TARP is thus able to improve security as well as reduce routing traffic in a mobile ad hoc network.

Enhanced Power Based Multipath Protocol (EPAOMDV) [22] is an improved version of AODV. It allows AODV to store multiple paths which are node disjoint (i.e. no nodes are same for a given path) from source to destination. However the multiple paths stored in EPAOMDV are decided based on signal strength between intermediate nodes on the path. While performing route discovery (i.e dissemination of Route Request-RREQ packets) an intermediate node computes the power loss experienced at it after the reception of the RREQ packet. If the power loss is less than a specified threshold value only then the RREQ packet is broadcasted. This mechanism ensures that the route computed does not contain links that are unstable. EPAOMDV allows preemptive link breakage as for an ongoing transmission over a certain selected path; an intermediate node sends power loss calculated by it to the previous upstream node in an acknowledgement packet. If in case the specified value of power loss is below the threshold the source is notified and communication is transferred on the next stable link thus decreasing the process of route discovery and maintenance. EPAOMDV is shown to be better than AODV and AOMDV [23] (a multipath version of AODV) in terms of delay, throughput and routing overhead involved.

Advanced Dynamic Source Routing (ADSR) [24] is an extension to the DSR routing protocol. ADSR selects routes based on calculating the link state and dynamic delay detection. It calculates

the link stability between two nodes based on node velocities and distance among nodes. In ADSR when a source node floods RREQ packets, it appends its location, speed and direction in the control packet. It also sets a maximum expiration time to a corresponding field. When a relay node receives a RREQ, it predicts the link expiration time between itself and the previous hop and insert it in RREQ while further forwarding the packet. When a relay node receives multiple packets with different link expiration times, it selects the minimum among them and sends its own routing table with the chosen link expiration time attached. The ADSR routing protocol achieves better packet delivery ratios and lesser end-to-end delay while routing packets.

5. CONCLUSION

In this paper, we discussed new advancements and improvements being made in existing efficient routing protocols to make them more efficient and to meet the challenges being faced in routing in ad hoc networks. Most of the routing protocols studied such as BAWB-DSR, CCSR, EOLSR, TARP etc. take into consideration network bandwidth and congestion control which are important factors in efficient routing. However, they do not consider energy and security while performing dynamic routing which cannot be neglected in case of routing in mobile ad hoc networks. Only few protocols such as RAMP, CBTRP, SEAODV etc were found to be secure but they lacked multipath feature and energy unaware. Hence we come to the conclusion that still no silver bullet exists for routing in mobile ad hoc networks that deals with every particular concern. The security aspect which is most crucial for communication in ad hoc networks is found missing in most of the routing protocols being proposed. Therefore new efficient, multipath, QoS aware and energy aware routing protocols that address security concerns need to be developed.

REFERENCES

[1] Charles E. Perkins and PBhagwat, "A Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," In Proceedings of the SIGCOMM'94 Conference on Communication Architectures, Protocols and Applications, pg. 234-244, Aug 1994.

[2] C.Adjih, T.Clausen, P.Jacquet, A.Laouiti, P.Minet, P Muhlethaler, A.Qayyum, L.Viennot, "Optimized Link State Routing Protocol," RFC 3626, IETF, 2003.

[3] ETSI STC-RES 10 Committee, Radio Equipment and Systems: High Performance Radio Local Area Network (HIPERLAN) Type 1, Functional Specifications, June 1996, ETS 300-652.

[4] V.Park and M. Scott Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," In Proceedings of IEEE INFOCOM'97, March 1996.

[5] David B. Johnson and David A. Maltz, "Dynamic Source Routing in Ad-hoc Wireless Network," The Kluwer Series in Engineering and Computer Science, 1996, Volume 353, 153-181, DOI:10.1007/978-0-585-29603-6_5.

[6] C. Perkins, E.Belding-Royer, and S.Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, 2005.

[7] Z. J, Haas and M. R. Pearlman, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," Internet Draft draft-zone-routing-protocol-01.txt, Aug 1998.

[8] H. Tiwari, A. Vajpayee, A. Singh, "A Bandwidth Aware Weight Based DSR Protocol for Mobile Ad Hoc Networks," COMPUTE'11: Proceedings of the Fourth Annual ACM Bangalore Conference, MARCH 2011.

[9] B. Kadri, M. Feham and A. M'Hamed, "Weight Based DSR for Mobile Ad Hoc Networks," in 3rd International Conference on Information and Communication Technologies: From Theory to Applications, 2008 ICITTA pp 1-6, 7-11 April 2008.

[10] R. Yerajana, A.K Sarje, "An Adaptive Multipath Source Routing Protocol for Congestion Control and Load Balancing in MANETs,".ICAC3'09: Proceedings of the International Conference on Advances in Computing, Communication and Control, pg 456-459.

[11] H. Tan, "RAMP – A Reputation – Aware Multi-Hop Routing Protocol in Wireless Ad Hoc Networks," ISABEL'11: Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, Article No.60.

[12] S. Buchegger and Jean Y.Le Boudec, "Performance Analysis of the CONFIDANT protocol," in Proceedings of MobiHoc '02, pages 226-236., New York, USA, 2002, ACM.

[13] P. Wannawilai, C. Sathitwiriyawong, "AODV with Sufficient Bandwidth AwareRouting Protocol," IWCMC'10: Proceedings of the 6th International Wireless Communications and Mobile Computing Conference, pg 281-285.
[14] S. Sethi, A. Rout, D. Mishra, Satabdinalini, "A Robust Cluster Based Routing Protocol for MANET," ICCCS'11 Proceedings of the 2011 International Conference on Communication, Computing and Security, pg 26-31.
[15] H. Safa, H. Artail, D. Tabet, "A Cluster Based Trust-Aware Routing Protocol for Mobile Ad Hoc Networks," Journal of Wireless Networks, Volume 16 Issue 4, May 2010, pg 969-984.
[16] Liu, K. Dey, J., Varshney, P.K., & Balakrishnan, K. (2007, May), "An Acknowledgement Based Approach for the Detection of Routing Misbehavior in MANETs,".IEEE Transactions on Mobile Computing, 6, 536-550.
[17] S. Mahfoudh, P. Minet, "Energy Aware Routing in Wireless Ad Hoc Networks and Sensor Networks," IWCMC'10: Proceedings of the 6th International Wireless Communications and Mobile Computing Conference, pg 1126-1130.
[18] M. Mohammadizadeh, A. Movaghar, Seyad M. Safi, "SEAODV: Secure Efficient AODV Routing Protocol for MANETs Networks," ICIS'09: Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, pg 940-944.
[19] R.Akbani, T Korkamaz, G.V.S Raju, "HEAP: A Packet Authentication Scheme for Mobile Ad Hoc Networks," Ad Hoc Networks, Volume 6, No. 7, pg 1134-1150, 2005.
[20] M.Bellare, R Canetti, H Krawczyk, "Keying Hash Functions for message authentication," Annual International Cryptology Conference on Advances in Cryptology, Vol. 1109, pages 1-15, 1996.
[21] L.Abusalah, A Khokhar, G. BenBrahim, W. Elhajj, "TARP: Trust Aware Routing Protocol," IWCMC'06 Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing, pg 135-140.
[22] Sujatha P.Terdal, V.D. Mytri, A. Damodaran, "A Preemptive Multipath Routing Protocol for Mobile Ad Hoc Networks," International Journal of Computing Science and Communication Technologies, Vol. 2, No. 1, July 2009.
[23] M. K. Marina, S.R. Das, "On Demand Multipath Distance Vector Routing in Ad Hoc Networks," Proceedings of the Ninth International Conference on Network Protocols (ICNP) 2001, IEEE Computer Society, pp. 14-23.
[24] Youyuan Liu, "Advanced Dynamic Source Routing with QoS Guarantee," Proceedings of the Second Symposium International Computer Science and Computational Technology (ICSCT'09), pp. 504-506.

AUTHORS

Dr. Charu Gandhi is a Ph.D in Computer Science from Kurukshetra University, Haryana, India. She has more than 6 years of teaching experience. She is currently Assistant Professor at Jaypee Institute of Information Technology, Noida, India. She has published several papers in national and international conferences and journals. Her areas of interest include wireless networks, mobile ad hoc networks, QoS routing in MANETs, clustering techniques, energy efficiency and secure routing for MANETs, distributed and parallel computing.

Vivek Arya received his B.Tech in CSE in 2010 from USIT, GGSIPU, India. He completed his M.Tech in CSE from Centre of Development of Advanced Computing (CDAC), GGSIPU, Noida, India in 2012. He is currently a research scholar and pursuing his Ph.D from Jaypee Institute of Information Technology. He has presented several papers in various international and national conferences. His research areas include cybercrime, cyber-security, wireless mobile ad hoc networks, energy efficiency and scalable routing in MANETs.