International Journal of Computational Intelligence and Informatics, Vol. 3: No. 2, July - September 2013

A Novel Routing Scheme Based on Protection Mechanism to Discover Unconventional Disjoint Path in Ad Hoc Wireless Networks

S S Suthaharan
Department of Physical Science
Vavuniya Campus of the University of Jaffna
Vavuniya, Sri Lanka
s.shelton4@yahoo.com

***Abstract*- The performances of the routing protocols are important since they compute the primary path between source and destination. In addition, routing protocols need to detect failure within a short period of time when nodes move to start updating the routing table in order to find a new primary path to the destination. Meantime, loss of packets and end-to- end delays will increase thereby reducing throughput and degrading the performance of the network. This paper proposes a new algorithm, DBRT (Determined Backup Routing Table), to improve the existing proactive protocols such as DSDV (Destination Sequenced Distance Vector) protocol by creating a backup routing table to provide multiple alternative routes. The DBRT algorithm identifies adjacent nodes for each node in the same range and then selects one of these as a backup next hop according to the available path to the destination. The results show that loss of data packets, throughput and end-to-end delay times between source and destination are improved. The results show that the new protocol does not degrade the network's performance despite sending extra messages to construct and update the new backup routing table. Simulations (using an NS2 simulator) are undertaken to demonstrate the difference between using a DSDV protocol with or without the proposed schema.**

Keywords- Network Protocols, DSDV, Wireless Network, Mobile Ad Hoc Network

I. INTRODUCTION

In Mobile Ad Hoc Networks (MANET) is unlike the wired networks, because there is no central infrastructure between the nodes. Each node can exchange data dynamically without the need to a fixed base station or a wired back- bone. Some limitations of the MANET network have been researched, such as, transmission power limitation and multiple hops. This is because MANET Uses intermediate nodes to exchange information to pass its traffic to its destination. Hence, route discovery and maintenance in MANET networks is an essential issue. The nodes in wireless ad hoc networks can move frequently and instantaneously from area to area without notification, which leads to various problems, such as, loss of connectivity and an increase in the holding time, during which a new shortest path between source and destination is computed for the routing table[1].

When a loss in connectivity occurs, not all the nodes on the topology will be informed. This will generate loops in the network, which degrade its performance and reduce throughput. IP recovery will discover a backup path within a short period to alleviate loss of packets, reduce end-to- end delay and avoid loop in the network [3]. In MANET ad hoc networks, there are various kinds of main routing protocol tables. In table-based protocols, each node constructs a routing table that includes all routes to all nodes on the topology. The routing protocol needs to send periodic messages that contain routing information to keep the routing table for each node up to date. In on demand-protocols, nodes compute routes when they are needed.

Ad hoc wireless networks are frequently affected by failures when nodes move in and out and of radio propagation range. It is, therefore, highly desirable to develop a recovery mechanism to improve the quality of service (QoS) of the network. In the meantime, loss of data packets and end-to-end delays will increase. Many different types of routing protocols have been used to solve this routing problem, including DSDV, Dynamic Source Routing (DSR) and Optimized Link State Routing (OLSR) protocols [4]. In wired networks, the routing protocol generally uses distance vectors or link state routing algorithms. Both are proactive mechanisms as they send extra messages to keep the nodes up-to-date in case any information on the network changes, such as, if a node joins the network or it fails.

ISSN: 2349 - 6363

When failure occurs, these protocols inform all the nodes and they start to re-compute a new routing table. More holding time is then required in order to re-send the traffic along the new route. In this paper, A new algorithm called Determined Backup Routing Table (DBRT) to improve the existing proactive routing protocols such as, DSDV and OLSR to construct a backup routing table based upon its original that consists of a backup path for each node to its destination on the topology. When nodes fail or changed their positions by moving out of range, DSDV and LS (Link State) protocols demand that a routing advertisement be broadcast between the nodes on the network. In DSDV, when the nodes receive these advertisements, each one knows the route from its neighbor and its distance to all the other nodes on the network. On the other hand, OLSR protocols compute the shortest path based on the complete picture for each adjacent node on the network.

The DBRT mechanism aims to recover the network from failure in a shorter period by pre-computing a backup routing table by considering more than one node that have moved or change their positions. The backup routing table has alternative paths along which to pass the traffic when failure occurs. The pre-computed alternative path can be used immediately without waiting for the routing protocol to re-compute a new one. This paper concentrate on the scenario when more than one node moves on the primary path. The main contribution of this paper is towards the development of an alternative and fully disjointed pathway, which is computed. By using a backup routing table and is based upon the number of adjacent nodes and their ranges.

This paper is organized as follows: Section 2 discusses related work, Section 3 illustrates the originality and the basic concept for the DBRT algorithm in detail, Section 4 shows the performance evaluation via simulation and concluding remarks are given section 5.

II. RELATED WORK

Several routing protocols have been published for use in different environments to improve network performance when nodes move or fail, causing a loss in connectivity [7]. In [8] the author studies the QoS and reliability in the MANET networks. There are two categories of routing protocols for MANETs namely proactive and reactive. A proactive routing protocol updates pairs of nodes by flooding via a periodic broadcast. This brings routing tables up-to-date for each node in the network. However, a reactive routing protocol detects a new route only when it is required. Some proactive routing protocols (such as DSDV, OLSR, CGSR and WRP) trigger messages that can detect links when they fail [9, 10].

Based on these messages, the routing protocol can construct and maintain routes to the destination. Reactive protocols, such as, DSR, AODV (Ad - hoc on demand Distance Vector) and TORA will reduce overhead because new paths between nodes will be created only when failures occur. The DSDV routing protocol is based on the Bellman-Ford algorithm. It is similar to a DSR protocol [11]. This is because they both use a similar algorithm. Multipath routing has been introduced and considered in wireless ad-hoc networks for improving QoS and reliability of network performance [12]. In [13] a new algorithm for wired networks called the Alternative Routing Table (ART) algorithm sends messages to enquire if neighboring nodes have an alternative and disjointed pathway from the primary node to its destination.

The number of data packets sent to each node will depend on the number of adjacent nodes that are not connected to the primary path [6]. An efficient routing protocol algorithm has been constructed in terms of achieving robustness and fast convergence in case a node goes down. As such, this work enhanced the ART algorithm to make it work on wireless ad-hoc networks by constructing a primary routing table based on the propagation range with the number of hops and a backup routing table based upon the number of adjacent nodes to select the best path. In [14–16], the OLSR routing protocol is shown to be proactive in ad-hoc networks. The OLSR has Multi Point Relay (MPR) nodes, which are used to send link state messages to construct a routing table [17]. In OLSR, two kinds of broadcasts are sent: HELLO and Topology Control (TC) messages [2]. Each node will send HELLO message to its neighbours to check if connectivity is up or down every two seconds but its waiting time of six seconds is considered too long. The TC message is thus based on the information collected by the HELLO messages. The interval time is five seconds and the time to detect failure is fifteen seconds.

In [18, 19], the source node knows the complete rout hop-by-hop to the destination. The route from source to destination is stored in a route cache. The OLSR routing protocol will re-route data packets only after re-computing a new routing table and updating the information to all nodes on the topology. Depending upon the HELLO message interval times, the re-routed traffic will take longer and this will lead to an increased loss of data packets and reduced throughput [20]. Internet Protocol recovery emphasizes two cases. First, the time required to detect failure and secondly, the time taken to compute the shortest path. In [21], the authors mention how a network recovery can be achieved within a short time when failure occurs. The aim of IP recovery is to offer a loop free protection mechanism in the network. Loops in a network are one of the main problems with some existing techniques.

The constraint-based routing protocols use metrics instead of the shortest path between nodes to find a suitable route. In QoS routing schema, the Core Extraction Distributed Ad hoc Routing (CEDAR) algorithm has been introduced for a medium size Ad - hoc Network. The idea behind the multiple paths QoS routing schema is

to try to find a number of paths between source and destination based on high capacity bandwidth requirements. Service providers guarantee a network's performance via a set of measurements, such as, delay, jitter and loss of data packets [22, 23]. These parameters are part of QoS that can optimize along the network to invest in the provisioning of resources in cases of increased traffic or node failures.

III. PROPOSITION

The basic principle of the DBRT algorithm is how to construct a backup routing table by computing an alternative path to the destination by investing the original routing table, which is computed by the routing protocol. Our proposition leads to reduce holding times for source nodes until the routing table is updated. The backup routing table is restricted because it depends on the adjacent nodes having a disjoint path to their destination. This gives each node has the ability to offer its path for its traffic reaches its destination. However, the backup path is pre computed in advance in order to reroute data packets in case of failure.

In addition, when a node on the primary path goes down or moves from the region, the adjacent nodes will detect a link break by receiving a link layer feedback signal from the HELLO data packets, which will confirm the failure because it does not receive any acknowledgement during the interval time. The DBRT algorithm, via the backup routing table, will pass the traffic to the destination D without waiting to re-compute a new routing table. However, assume here that each node has at least one adjacent and one unconnected node to the primary path but within the same range. The DBRT algorithm involves choosing one of them as a backup node to re-route a packet through it when a failure occurs. The work performed a different number of topologies each having a different number of nodes. In each topology, each node with at least two neighbors that can reroute data packets through them when failure occurs.

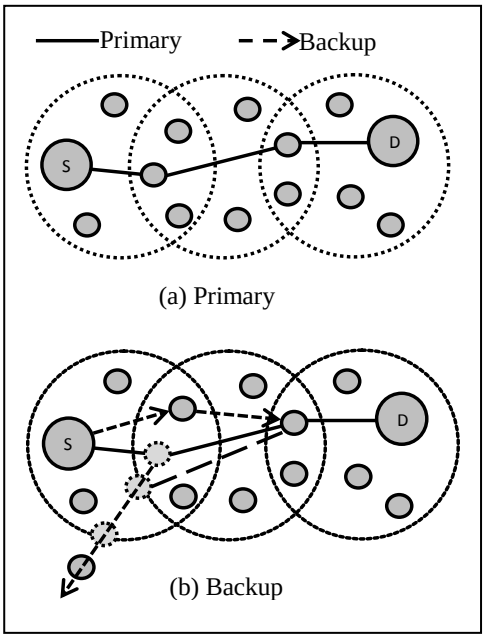

Figure 1. Primary and Backup Path

A. Algorithms Overview

In our schema, the pre computed second paths provide a good solution for when failures occur. DBRT evaluates the backup routing table from the primary one to ensure that any alternative path will be disjointed from the primary one. Figure 1 shows the primary and backup path. When the routing protocol determines the primary path the DBRT algorithm will start to check each node to determine how many adjacent nodes are within range and not connected to the primary path. The DBRT computes the backup routing table from the passing traffic. In Figure 1, the primary path from source to destination is computed by a routing protocol. By using the radio propagation range the DBRT can discover any adjacent nodes by which to compute the backup path to the destination, which is based upon the number of hops.

When there is more than one adjacent node, the DBRT will start to check which adjacent node has a disjointed path to the destination (i.e. to construct a backup path). In addition, the DBRT algorithm evaluates an appropriate backup route using the primary routing table. Any nodes connected to the primary path will be excluded from the next hop in the backup route. Each node randomly takes a position (X, Y) in the radio propagation range for the area 1000m by 800m. In DBRT, the nodes on the topology will start broadcasting a

small message to enquire from adjacent nodes if they have a disjointed path from the primary (with regard to the primary routing table) to the destination.

Because DBRT considers all nodes as a source and destination then each node will check the acknowledgements from adjacent nodes to see if there is any available route to the destination and if one of the adjacent nodes become the intended node it will then insert it into the backup routing table as a first hop. If no adjacent node has a disjointed path, then each adjacent node will check other nodes from its list of adjacent nodes to determine if they have a neighboring node that has a disjointed route to the destination. Hence, the adjacent node will start checking its route hop-by-hop to the destination.

If this route is not connected to any node on the primary path then it will inform the source whether a disjointed path is available. Hereafter, the source node uses the node in the backup routing table, as a first next hop to re-route the traffic through the backup routing table should a node on the primary path fail. If more than one alternative path exists, then the node will select the best one based upon the number of hops that have a greater history for reliability.

The process at each node on the topology can be described as follows:

Step 1 : Each node inserts her adjacent in the adjacent list from the primary routing table but excluding nodes that are connected in the primary path.
Step 2 : Each node broadcasting to her adjacent nodes a mini packet to enquire if they have a unique route to destination not overlap with the primary one.
Step 3 : When all adjacent nodes received these packets then they will start to check from their routing table if their route to destination not connected with primary path. If "Yes" then will insert all these next hops to the backup routing table.
Step 4 : If the adjacent nodes do not have any disconnected route then they will start checking their neighbors to see if they have available path or not. The DBRT will return to step 1 until all nodes make a full view for the topology and created the backup routing table.

IV. Simulation Experiment

A. *Simulation Experiment*

Network simulation (NS2) was used to evaluate the proposed algorithm. This work compared the simulation results of the DSDV protocol with and without our schema. NS2 offers good support for node mobility in ad-hoc networks. Different network scenarios were created, each having a different number of mobile nodes to demonstrate the effect of node movement or failure during simulation time. The simulation is configured in 1000 m by 800 m. Nodes could move randomly by any node on the primary path. A radio propagation range with transmission power of 0.28 watt was used, allowing each node to send or receive a packet to or from its neighbors for a distance of up to 250 m. For each scenario, the simulation executed for 250 seconds.

In the free space model, the signal power is weakness by a factor 1/d2 where d is the distance between radios. The movement type was of a Two Way Ground Model with a channel capacity of 2Mb/s. The packet size was 512 bytes. DBRT with DSDV because they are both proactive protocols [5]. IEEE 802.11 Distributed Coordination Function (DCF) is used as the wireless channel can share in an ad-hoc configuration.

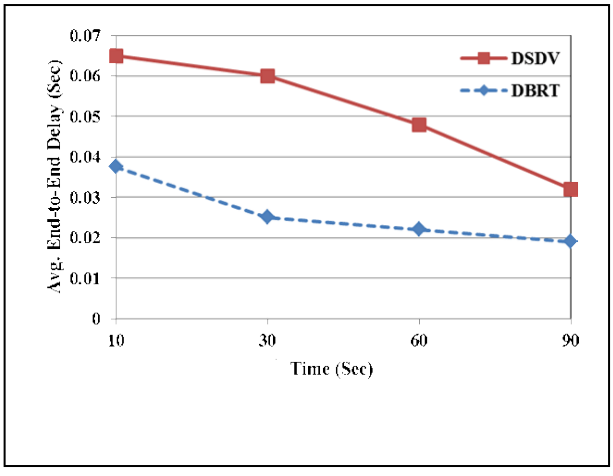

Figure 2. End to End Delay

B. Results and Analysis

Figure 2 shows the results for the end-to-end delay measured against a different time intervals. The end-to-end delay in DSDV with a DBRT algorithm was less than the DSDV protocol, because the latter has to retain all its routes in a static routing table. When any node on the primary path moved out of range or failed, the DSDV routing protocol needed to re-compute a new routing table by flooding packets to update it. In DBRT, the backup path is pre-computed in case any nodes on the primary path moves or fails. In this case, the node that is connected to the newly failed or moved node will re-route the traffic according to the backup routing table.

Figure 3 shows the amount of the congestion occurred in the network. Congestion in DSDV is less compared to DSDV with a DBRT algorithm [2, 5], because DBRT needs to generate extra data packets so that it can construct a new backup routing table. These packets show that an increase in network overheads does not degrade network performance with respect to the time for the certain number of nodes that are involved.

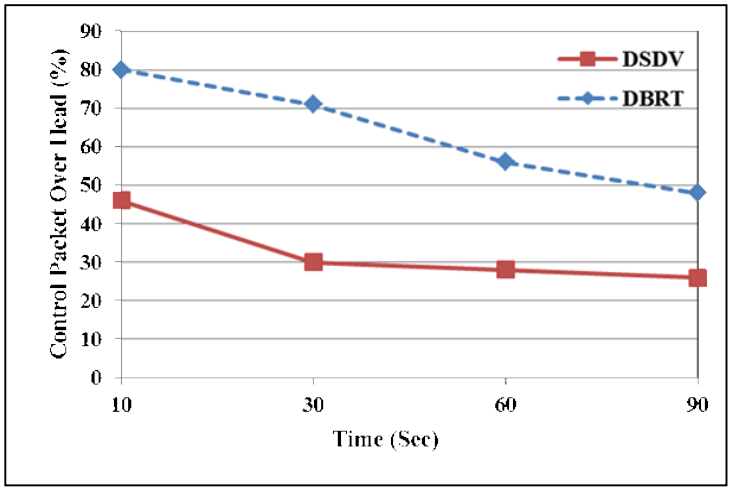

Figure 3. Packet Overhead

Figure 4 shows the average loss of data packets for DSDV and DBRT for a different number of nodes in different time (10, 30, 60, 90s). Traffic is re-routed along an Alternative path, which is computed by the DBRT protocol. The DSDV protocol shows that the loss of data packets increases based upon the number of nodes and hops to the destination. The DSDV protocol generates messages that maintain the routes that offer the greatest probability for collision to occur in the network.

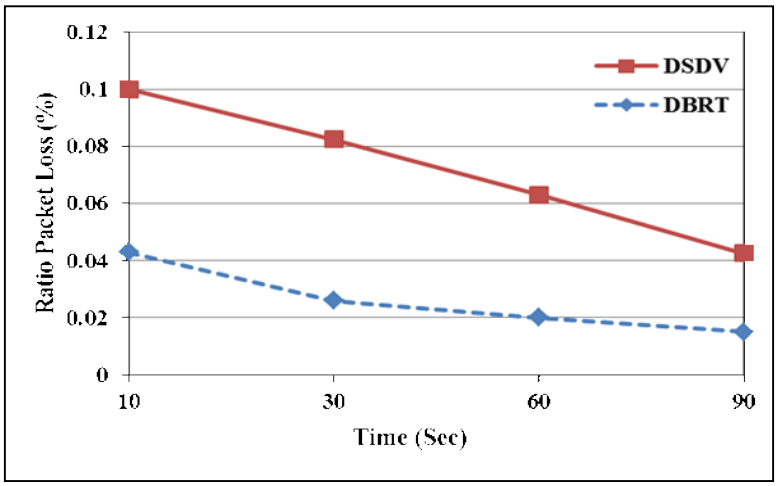

Figure 4. Loss Of Packets

Figure 5 shows the throughput for both DSDV with a DBRT algorithm and DSDV protocols. The packets will send from source to destination hop-by-hop. The DSDV protocol with a DBRT algorithm achieved a higher throughput compared to the DSDV. When a collision occurred, through- put was decreased in both. The IEEE 802.11 sending RTS packets can reduce collisions in the network. However, the DSDV protocol needs a certain amount of time to re-route the traffic. The length of this period remains undesirable. It takes two seconds for each node to re-compute a new routing table and a medium topology will take fifteen seconds.

The backup routing table will start to be calculated after the primary one has been computed. Therefore, DBRT will re-route the traffic directly to an adjacent node on the backup routing table if any node on the primary path moves out of range or fails. This will lead to an increased throughput between the source and destination.

Figure 6 shows average traffic load versus time, (10, 30, 60 and 90s) of a 50 node network. The degree of traffic load using the DSDV protocol shows that it is satiable for their network topologies regarding the amount of packets send to update the routing table when nodes move. On the other hand, DSDV with a DBRT algorithm shows that the load is reduced when the nodes become more stable as the time become larger. If the time is 10 sec, the DBRT needs to send extra packets every 10 sec to re-update the backup routing table until the node stops. During this process, the DSDV with a DBRT will pass the traffic through an alternative path to its destination. Hence, the traffic load will increase when nodes move frequently and within a short time and vice-versa.

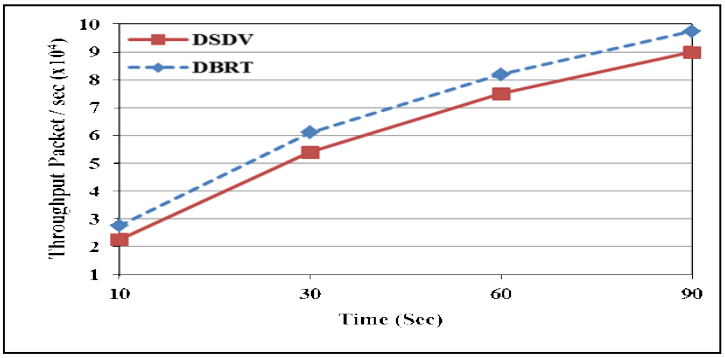

Figure 5. Throughput

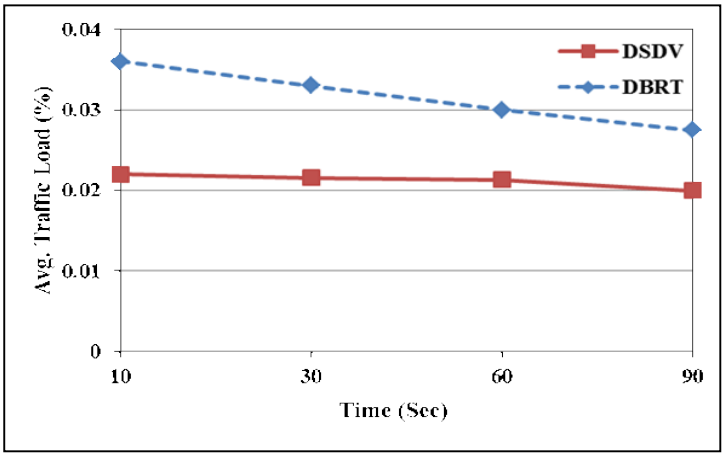

Figure 6. Traffic Load

V. CONCLUSION

This paper has presented a new protocol for computing an alternative backup routing table which finds an alternative path for each node on the network. The DBRT algorithm computes a backup routing table based on the distance between nodes and number of hops to the destination. The backup routing table includes alternative and disjointed next hop to destination for all nodes on the topology. The DSDV protocol with DBRT provides a recovery path that gives the shortest distance between source and destination. This paper shown that the backup paths contain fewer numbers of hops compared with those produced by the DSDV protocol. For real traffic, the results show that the DSDV protocol with DBRT reduces the loss of data packets and delay between source and destination nodes. In future work, the DBRT algorithm will be designed to deliver a backup routing table that contains more than one backup path between the source and destination, in order to improve the QoS when more than one node moves or fails. In addition, the reducing of sending extra packets will increase the reliability of our algorithm through creating a super node that can make updating with reduce flooding in the network.

REFERENCES

[1] Poonam, K. Garg, and M. Misra, "Trust enhanced secure multi-path dsr routing", International Journal of Computer Applications, Published By Foundation of Computer Science, pp. 63–69, May 2010.

[2] R. Rashidi, M.A.J. Jamali, A. Salmasi, and R. Tati, "Trust routing protocol based on congestion control in manet", In Application of Information and Communication Technologies, AICT International Conference, pp. 1–5, 2009.

[3] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector routing protocol", IETF Internet RFC 3561, 2003.

[4] C.E Perkins and P.Hhagwat, "Highly dynamic destination sequence vector routing for mobile computers", Computer Communication, pp.234–244, 1994.

[5] Mohanchur Sarkar, K.K.Shukla, and K.S.Dasgupta, "performance analysis of proactive and reactive transport protocols using a proactive congestion avoidance model", International Journal of Computer Applications, pp.10–17, September 2010.

[6] Sung ju Lee and Mario Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks", 2001.

[7] Saeed Shahbaz, Gholamreza Ghassem-Sani, Hamidreza Rabiee, and Mohammad Ghanbari, "A distributed intelligent ad-hoc network", Vol. 4308–2006, Springer- Link, 2006.

[8] D. Kim, J. Garcia, and K. Obraczka, "Routing mechanisms for mobile ad hoc networks based on the energy drain rate", Vol.2, pp. 161–173, 2003.

[9] V.D. Park and M.S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks", IEEE International Conference on Computer Communications (INFOCOM), pp. 1405–1413, 1997.

[10] J. Moy, "Link-state routing in routing in communications networks", M.E. Steenstrup, Prentice Halls, pp. 135 – 157, 1995.

[11] Subir Kumar Sarkar T.G. Basacvaraju and C Puttamadappa, "Impact of mac layer on the performance of routing protocols in mobile ad hoc networks", International Journal of Information and Communication Engineering, Vol.3:8, pp. 541– 548. 2007.

[12] S.J. Lee and M. Gerla, "Aodv-br: backup routing in ad hoc networks", In Wireless Communications and Networking Conference, WCNC. 2000 IEEE, Vol. 3, pp. 1311 – 1316, 2000.

[13] Radwan Abujassar and Mohammed Ghanbari, "An efficient algorithm to create a loop free backup routing table", International Conference on Computer Science, Engineering and Applications, Dubai, UAE, Springer, 2011.

[14] Prayag Narula, Sanjay Kumar Dhurandher, Sudip Misra, and Isaac Woungang, "Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing", Computer Communication.,Vol. 31, pp.760–769, March 2008.

[15] Juan Antonio Cordero Emmanuel Baccelli, "Ospf over multi-hop ad hoc wireless communications", IJCNC, 2(5):37–56, September 2010.

[16] C. A. Dhote, M.A.Pund, R.S. Mangrulkar, and Makarand R. Shahade, "Hybrid routing protocol with broadcast reply for mobile ad hoc network", International Journal of Computer Applications, 1(10):108–113, February 2010.

[17] Marti S., Giuli T. J., and Baker, "Mitigating routing misbehavior in mobile ad hoc networks", pp. 255–265. In Proceeding of Sixth Annual International Conference Mobile Computing and Networking (MobiCom) New York, 2000.

[18] H. Yong, C. Chuanhe and Wenming, "hahaTrusted dynamic source routing protocol", pp. 1632–1636. Wireless Communications, Networking and Mobile Computing WICOM, 2007.

[19] David B. Johnson and David A. Maltz, "Dynamic source routing in ad hoc wireless networks mobile computing", Kluwer Academic Publishers, pp. 153 – 181, 1996.

[20] Broch J., Maltz D. A., Johnson D. B., Hu Y.C., and Jetcheva "A performance comparison of multihop wireless ad hoc network routing protocols", Proceeding of International Conference Mobile Computing and Networking (MobiCom) ACM Press, pp. 85–97, 1998.

[21] C.E. Perkins and E.M. Royer, "Ad-hoc on-demand distance vector routing", Workshop Mobile Computing Systems and Applications (WMCSA), pp. 90–100, 1999.

[22] W. H. Liao et al., "A multi-path qos routing protocol in a wireless mobile ad hoc network", IEEE ICN, 2001.

[23] E. M. Royer and C.-K. Toh, "A review of current routing protocols for ad-hoc mobile wireless networks", IEEE Pers, pp. 46–55, 2001.