ISSN 2047-3338

Detection of Misbehavior nodes using Efficient Comparison of Multiple Route Set in Performance Routing Protocols in WSN

Vishakha Kale[1] and Veena Gulhane[2]

[1]Department of Wireless Communication and Computing, G.H. Raisoni College of Engineering, Nagpur University, India
[2]Department of Computer Science and Engineering, G.H. Raisoni College of Engineering, Nagpur University, India

***Abstract*– In WSN, Nodes in the network act as routers and forward messages on behalf of the other nodes. This paper presents a comprehensive simulation study of well know On-demand routing protocols Ad hoc On demand Distance Vector (AODV), Table-driven routing protocol Destination Sequenced Distance Vector (DSDV) with the consideration of the node misbehavior. This problem of node misbehavior can be detected and controlled by different techniques such as Multiple Route Set (MRS) discussed in this paper which is more efficient than other general techniques.**

***Index Terms*– AODVM, MRS, Misbehavior Node, Ad-hoc Routing Detection Techniques and WSN**

I. INTRODUCTION

IN WSN technologies have enabled the development of mobile ad hoc networks (MANETs), in which different types of mobile nodes with different goals share their resources in a network wide area. A node is able to communicate with another node within its range through other nodes if the destination node is not in the immediate neighborhood. However, there may be misbehaving nodes that can rather easily disrupt the network operation and damage the communication within the network area. Hence, providing secure data communication through misbehavior detection and mitigation in MANETs is an important and critical research topic.

A wireless sensor network is a large collection of sensor nodes with limited power supply and constrained computational capability. Due to the restricted communication range and high density of sensor nodes, packet forwarding in sensor networks is usually performed through multi-hop data transmission. Multipath routing has drawn extensive attention in MANETs and WSNs recently. The dense deployment of nodes in MANETs/WSNs makes the multipath routing and promising technique to cope with the frequent topological changes and consequently unreliable communication services. Research efforts have also been made using multipath routing to improve the robustness of data delivery to balance the traffic load and balance the power consumption among nodes [3] to reduce the end-to-end delay and the frequency of route discoveries [11] and to improve the network security etc. Two primary technical focuses in this area are, (a) the multipath routing protocols that are able to find multiple paths with the desired properties, and (b) the policies on the usage of the multiple paths and the traffic distribution among the multiple paths, which very often involve coding schemes that help to split the traffic. Dynamic nature of MANETs requires performance of proper routing protocols, which should be compliant to frequent changes in network topology and the nodes should be able to exchange information regarding topology changes to establish routes. Such frequent changes very often bring about the security issues in ad hoc networks.

Traditional routing protocols cannot be useful to determine these security issues in ad hoc networks due to its recurrently changing network dynamics. As a result of recurrent topology changes, packets exchanged between a pair of wireless nodes may track different routes at different instants of time, and thereby may be exposed to attacks. At the same time, unlike in wired networks, it is difficult to substantiate the node of a MANET in the absence of on line servers [1], [11]. The group of commonly encountered attacks may include replay attack, Denial of Service (DoS), routing table overflow, imitation, energy utilization. A number of solutions have been proposed to protect routing message from being modified by the attackers or harmful messages being injected to the network [4], [6].

The Dynamic Source Routing (DSR) Protocol [10] lists three types of node misbehavior in routing as experienced by MANETs. It is suggested that network operation and maintenance can be easily jeopardized and network performance will be severely affected as a result. In this paper, it is intended to compare the performance of DSR under security attacks with that of DSDV (Destination Sequenced Distance Vector) [1], [8] and AODV (Ad hoc On-

[1]Vishakha D .Kale is with the Department of Wireless Communication and Computing, M.E. Student G.H. Rasoni College of Engineering, Nagpur University, India (Email: vishuakhre@gmail.com)

[2]Asst. Prof. Vina. Gulhane is with the Department of Computer Science and Engineering, Asst. Prof. G.H. Rasoni College of Engineering in Nagpur, India (Email: vina.gulhane@gmail.com)

demand Distance Vector) [9] protocols and AOMDV (Ad Hoc On-Demand Multipath Distance Vector) Routing Protocol .

II. RELATED WORK

In this section, discuss some related work for nodes cooperation in MANETS which is currently a very active and demanding research area. The solutions to the problem falls into two categories: Based on Prevention methods and based on detection and removal methods. In [2] Baolin Sun, Xiaocheng Lu, Chao Gui, Ying Song and Hua Chen Network Coding-Based On-Demand Multipath Routing in MANET. They demonstrated in NCMR routing protocol with AODVM routing protocol, in terms of the packet delivery ratio, packet overhead, and average end-to-end delay when a packet is transmitted. The simulation results show that the NCMR routing protocol provide an accurate and efficient method of estimating and evaluating the route stability in dynamic MANETs. In [3] Prokopios C. Karavetsios and Anastasios etc. evaluated the performance comparison of distributed routing algorithms in Ad-Hoc Mobile Networks. They demonstrated in AODV and DSDV protocols using NS2. In [4] Sree Ranga Raju and Jitendranath Mungara presented performance evaluation of AODV, DSR and ZRP using QualNet Simulator and concluded that ZRP performed poorly throughout all the simulation sequences. In [5] V. Kanakaris, D. Ndzi and D. Azzi focus on AODV, DSDV, DSR and TORA using NS-2. AODV and DSR produce high-quality results, AODV has an excellent throughput in all the scenarios but TORA performs poorly. In [6] Isha V. Hatware1, Atul B. Kathole2, Mahesh D. Bompilwar etc evaluated the Detection of Misbehaving Nodes in Ad Hoc Routing compare the behavior of routing protocols DSDV, DSR and AODV and IDS, with the consideration of the node misbehavior. Cooperative Intrusion Detection, watchdog and path rater discussed in this paper which is more efficient than other general techniques**.** In [7] Sankalp Bahadur Singh and Bharat Pesswani a Performance analysis between AODV & DSR Routing Protocol presented performance evaluation of AODV, DSR using NS-2 As their exists only one path and if a dead node occurs along the path it would receive the packets and cause packet loss. In [8] Savita Gandhi SMIEEE1, Nirbhay Chaubey MIEEE2, Naren Tada3, Srushti Trivedi Scenario-based Performance Comparison of Reactive, Proactive & Hybrid Protocols in MANET presented performance evaluation of AODV, DSR and ZRP using QualNet Simulator and concluded that ZRP performed poorly throughout all the simulation sequences. In [9] Fubao Yang, Shengzhi Ling, Hui Xu, and Baolin Sun Network Coding-based AOMDV Routing in MANET presented performance evaluation of NC-AOMDV routing protocol with AODVM routing protocol, in terms of the packet delivery ratio, packet overhead, and average end-to-end delay when a packet is transmitted. In [10] Mahesh K. Marina and Samir R. Das Ad hoc on-demand multipath distance vector routing present performance evaluation of propose multipath extensions to a well-studied single path routing protocol known as ad hoc on-demand distance vector (AODV). The resulting protocol is referred to as ad hoc on-demand multipath distance vector (AOMDV). The protocol guarantees loop freedom and disjointness of alternate paths. Performance comparison of AOMDV with AODV using ns-2 simulations shows that AOMDV is able to effectively cope with mobility-induced route failures. In particular, it reduces the packet loss by up to 40% and achieves a remarkable improvement in the end-to-end delay (often more than a factor of two). AOMDV also reduces routing overhead by about 30% by reducing the frequency of route discovery operations.

III. AOHOC ROUTING PROTOCOL

A. Routing Protocols

The routing protocols implemented in MANETs are globally classified into two categories: proactive or table driven protocols and reactive or on-demand protocols. Table driven protocols rely on a table, which maintains consistent up-to-date information concerning routes to all possible destinations, whereas on-demand routing protocols implement source-initiated route organization, where a route is created when desired by the node. In this paper, compare the performance of a table-driven protocol DSDV with two most popular on-demand routing protocols such as DSR [7], [8] and AODV. Proactive routing protocol DSDV operates with a table driven algorithm, based on routing mechanism. In this approach, every mobile node in the network maintains routes to all possible destinations with number of hops in between. Each entry is marked with a sequence number as assigned by the destination node. With the help of sequence numbers, mobile nodes can be able to distinguish stale routes for the new ones, and as a result, routing loops can be avoided.

Reactive routing protocol DSR comprises two mechanisms: route discovery and route maintenance. It enables the mobile nodes in an ad hoc network to discover routes to arbitrary destinations as per requirement. In the beginning, the source node initiates a Route Discovery mechanism comprising two phases; Route Request and Route Reply.

On successful completion of these two phases, a route is established between the source and destination following which the source node appends the destination address to its data packets and sends them along the route. The intermediate nodes act as routers of the packets and do not maintain any up-to-date routing information. Reactive routing protocol AODV [7] is an enhancement of DSDV, which significantly minimizes the number of broadcasts required during route establishment by creating routes on demand basis. It does not need to maintain all possible routes unlike DSDV, which convincingly reduces the required storage capacity at a node in the MANET. As suggested by authors of AODV, it is a perfect on-demand routing protocol, since nodes not belonging to a route, do not necessarily participate in route discovery, neither maintain up-to-date routing information. A source node needs to initiate a route discovery mechanism, when it has to send to a required destination.

B. Ad Hoc On-Demand Distance Vector (AODV)

Ad hoc On-Demand Distance Vector Routing AODV [4], [5] is an on-demand, single path distance vector protocol. It combines the on-demand route discovery mechanism in DSR with the concept of destination sequence numbers from DSDV. However, unlike DSR which uses source routing, AODV takes a hop-by-hop routing approach. The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multi-hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. AODV builds routes using a route request / route reply messages. When a source node seeks a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ). Packets across the network nodes receiving this packet update their information for the source node and store the information in the routing table.

C. Ad hoc On-Demand Multipath Distance Vector Routing (AOMDV)

The AODV protocol to compute multiple node-disjoint paths in a route discovery. That every node has a unique identifier (UID) (e.g., IP address), a typical assumption with ad hoc routing protocols. For simplicity, we also assume that all links are bidirectional, that is, a link exists between a node *i* to *j* if and only if there is a link from *j* to *i*. AOMDV can be applied even in the presence of unidirectional links with additional techniques to help discover bidirectional paths. AOMDV [10] shares several characteristics with AODV. It is based on the distance vector concept and uses hop-by-hop routing approach. Moreover, AOMDV also finds routes on demand using a route discovery procedure.

In AOMDV, RREQ propagation from the source towards the destination establishes multiple reverse paths both at intermediate nodes as well as the destination multiple RREPs traverse these reverse paths back to form multiple forward paths to the destination at the source and intermediate nodes. AOMDV also provides intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency [9]. The core of the AOMDV protocol lies in ensuring that multiple paths discovered are node-disjoint, and in efficiently finding such paths using a flood-based route discovery. To achieve these two desired properties. Next subsection deals with incorporating those ideas into the AOMDV protocol including detailed description of route update rules used at each node and the multipath route discovery procedure. AOMDV relies as much as possible on the routing information already available in the underlying AODV protocol.

IV. NODE MISBEHAVIORS

Identification of misbehaving nodes in ad hoc networks is critically important to detect security attack in the network. Two types of misbehaving nodes such as selfish and malicious nodes are taken into consideration in [6]. Selfish nodes do not intend to directly damage other nodes, but however, do not cooperate, saving battery life for their own communications. But malicious nodes do not give priority to saving battery life, and aim at damaging other nodes. It is introduced that two different types of selfish nodes. The nodes in MANETs are battery powered, energy becomes a precious resource, and thus, role of selfish nodes draws more attention.

V. THE SELFISH AND MALICIOUS NODES

Malicious nodes, also called attackers, They are capable of discarding or altering control and data packets, preventing route discovery between two nodes, make data packets unable to arrive at their destinations consume energy and available bandwidth of the network . Selfish nodes establish their own communication. Selfish nodes can drop data packets or refuse to forward routing control packets for other nodes. Current ad hoc routing protocols are basically exposed to two different types of attacks: active attacks and passive attacks. An attack is considered to be active when the misbehaving node has to bear some energy costs in order to perform the threat, whereas passive attacks are mainly due to lack of cooperation, with the purpose of saving energy selfishly.

Nodes that perform active attacks with the aim of damaging other nodes by causing network outages are considered to be malicious whereas nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be selfish. Malicious nodes can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information, and by impersonating other nodes. On the other side, selfish nodes can severely degrade network performance and eventually partition the network by simply not participating to the network operation [6].

VI. EVALUATION METRICS

A. Network Throughput

This is the ratio of total number of packets received successfully by the destination nodes to the number of packets sent by the source nodes [2]. Network Throughput is an important metric as it describes the loss rate. Thus, Network Throughput in turn reflects the maximum throughput that the network can support.

$$\text{Network Throughput} = \frac{\text{No. of packets received by destination}}{\text{No. of packets sent by source}}$$

B. End to End Delay

This is the average of the time taken by the packets to reach the destination in the network [2]. In order to provide quality delivery to delay sensitive applications such as voice and video, it is extremely important that mobile Ad hoc networks provide quality of service (QOS) support in terms of delay. The proposed approach tries to minimize this end to end delay.

VII. ANALYSIS AND MODELLING

The proposed mechanism is a model of secure and reliable multi-path reactive routing protocol for mobile ad hoc networks. It is divided into three modules in order to facilitate its analysis. Module I comprises of identification of misbehaving nodes. Module II will remove the threats imposed by misbehaving nodes. Module III explains optimization of network performance. The modus operandi of these modules is explained in detail as follows:

A. Model for Mechanism to Identify Misbehaving Nodes

In this module, the first step is the route discovery so as to obtain the set of node disjoint routes.

Route Discovery

Proposed routing protocol uses an Multiple Routes Set (MRS) comprising node-disjoint paths, determined using the AOMDV protocol [10]. MRS of node disjoint routes is constructed by successively calculating the node-disjoint, shortest in number of hops, routes, using the network connectivity information provided by the route discovery. Ad Hoc On-Demand Multipath Distance Vector Routing Protocol is one of the most used Ad-Hoc routing protocol. It is a reactive routing protocol based on DSDV. The main idea in AOMDV is to compute multiple paths during route discovery. When single path on-demand routing protocol such as AODV is used in such networks, a new route discovery is needed in response to every route failure. Each route discovery is associated with high overhead and latency. This inefficiency can be avoided by having multiple redundant paths available.

The AOMDV protocol has two main components:

1). A route update rule to establish and maintain multiple loop free paths at each node.

2). A distributed protocol to find node-disjoint paths that is route discovery.

In AOMDV a new route discovery is needed only when all paths to the destination break. A main feature of the AOMDV protocol is the use of routing information already available in the underlying AODV protocol as much as possible. Thus little additional overhead is required for the computation of multiple paths [10].

The route discovery process has two major phases: route request phase and route reply phase. The route discovery process computes the multiple loop free paths. The route discovery process will be initiated when a route is requested by a source node and there is no information about the route in its routing table. First, the source node generates an RREQ (route request packet) and then floods the packet to networks. The RREQ's are propagated to neighbors within the source's transmission range. They also broadcast the packets to their neighbors. The process is repeated until the destination receives the RREQ. When an intermediate node receives the RREQ, it performs the following process:

1). When an intermediate node receives the information of RREQ, either it sends the route reply if the node is destination, or it rebroadcasts the RREQ to it neighbors.

2). The node reads the information from the RREQ. In order to transmit route reply packets to the source, the node builds a reverse path to the source. The node will insert the path to its multiple path lists. Otherwise, the node will ignore the path and discard the RREQ. Once the route discovery ends, MRS is now filled with node- disjoint paths that are to be used for data communication.

Mechanism to Identify Misbehaving Nodes

Path Discovery: Multiple routes between two nodes can be either link-disjoint or node disjoint. In the node disjoint method, nodes on the routes should not be common, whereas, in the link disjoint method, links on the routes should not be common [2]. Thus, traffic load on the shared node in link disjoint route will be much higher than the other nodes of the routes. As a result, this node tends to die much earlier than the other nodes, leading to the routes to break down much earlier. Thus, the presence of node disjoint routes prolongs the network lifetime by reducing the energy depletion rate of a specific node [6]. In the proposed protocol, multiple routes are used for sending data from source to destination and thus making data transfer faster and achieving load balancing in situations where the data traffic is heavy.

- *Multiple Route Set (MRS)*

The MRS is filled with node disjoint routes, a unique id is assigned to each node disjoint route from 0 to n. Here two types of control packets viz. PATH DISCOVERY PACKET packet and PATH SHIFT PACKET are used. PATH DISCOVERY Packet is consisting of five fields as follows:

(i) Total number of routes obtained in route discovery i.e., n. (ii) The route id of the route over which that particular PATH DISCOVERY Packet is sent. (iii) Source node Id (iv) Destination node Id (v) Timeout value which is the time threshold for which the destination will wait for PATH DISCOVERY Packet s to arrive at it.

PATH SHIFT PACKET packet contains following field (i) Ids of failure routes (ii) Alert identifiers for failure routes. This alert identifier indicates type of misbehavior i.e., its value is 0 if node misbehavior is packet delaying, and if it is packet dropping then its value is 1.

The overall mechanism to identify misbehaving nodes works as follows:

Initially the PATH DISCOVERY Packet s are sent over all routes in MRS, one PATH DISCOVERY Packet per route. Each PATH DISCOVERY Packet contains total count of the routes obtained in route discovery. Whenever first PATH DISCOVERY Packet reaches to destination, the destination node extracts it to obtain two important values i.e. total number of routes and timeout value. The value 'total number of routes' gives destination, the total count of all node disjoint routes obtained during route discovery, between source node and destination node, over which it is supposed to get PATH DISCOVERY Packet s. The second value i.e. timeout value gives destination, the time threshold for which the destination node should wait for PATH DISCOVERY Packet s to arrive at it. If any PATH DISCOVERY Packet reaches to destination after this timeout value, then it is concluded that the route over which that PATH

DISCOVERY Packet arrived, contains misbehaving node who is delaying the packets.

Now when destination obtains any PATH DISCOVERY Packet, it extracts that packet to get the route id over which it has arrived and records that route id. If any PATH DISCOVERY PACKET control packet is lost or delayed in middle of its route, then corresponding route id will not be reported to the destination within particular time threshold, which means that the route over which that PATH DISCOVERY Packet is suppose to arrive, has dropped or delayed it. After waiting for particular time threshold i.e. timeout value, destination sends PATH SHIFT PACKET packet to source containing the ids of failure routes and the alert identifiers, over the shortest route chosen among the routes in MRS. As soon the source obtains PATH SHIFT PACKET packet, it starts data transmission over all routes except the failure routes reported by PATH SHIFT PACKET packet. At the same time, it triggers the behavior check mechanism over failure routes, one by one.

B. Model for Mechanism to Eliminate Misbehaving Nodes

The source node receives PATH SHIFT PACKET packet then in addition to commencement of data transmission, it also trigger behavior check mechanism that will check failure node in the failure route for two conditions as follows: (i) whether its energy is depleted, (ii) whether its buffer has overflowed. If its energy is depleted or its buffer is overflowed, it means that it is loyal node but because of the above reasons, it is not able to forward the data packets. Such nodes are avoided temporarily but not blacklisted. But if neither the energy of node is depleted, nor its buffer is overflowed, then the node is declared as 'misbehaving node', which intentionally programmed to misbehave and thus it is blacklisted. As the behavior check mechanism points out packet dropper/delaying node it informs about misbehaving nodes to source. Source will put misbehaving node in the blacklist maintained at source. Those nodes which are blacklisted are avoided in next route discovery. By doing this, their presence in future routes is eliminated. Now the MRS has reliable routes.

But it is also possible that any node in the reliable route may starts misbehaving in the middle of communication. In such cases, source won't be getting acknowledgement for dropped packet within retransmission time out (RTO). Here source will point out failure route from routing table, stops further data transmission over the same. Also, it redirects traffic of failure route over next available route and triggers behavior check mechanism over failure route so as to check this route for misbehaving reasons and to blacklist the misbehaving nodes if any. The packet that was dropped over this failure route is retransmitted over new route which was recently selected for data transmission so as to avoid packet loss.

C. Model for Mechanism to Optimize Network Performance

There may be packet dropping because of several reasons like low energy and buffer overflow. Hence even though the node is not misbehaving intentionally still it is declared as packet dropping/delaying node and this leads to false detection. Due to false detection, reliable nodes are ignored which minimizes the total number of nodes taking part in data communication [6]. This result into less number of routes or long routes obtained in route discovery and thus may degrade the overall performance of the Network. The proposed protocol avoids this degradation due to false detection with the help of behavior check mechanism. The routes are checked at the beginning of the data transmission by dispersing PATH DISCOVERY Packet s and then sending data packets over it. In the first round itself, reputation of the node is identified. Thus, there is no need to employ reputation base system where the reputation index of the node is calculated throughout the promiscuous overhearing [9]. Hence computational complexity, control overhead, consumption of processing power, and excessive delay is minimized.

D. PATH DISCOVERY PACKET and PATH SHIFT PACKET Packet Structure

PATH DISCOVERY Packet:

Source ID	Timeout Value	Route ID	Total No. Of Routes	Destination ID

Fig. 1. PATH DISCOVERY Packet structure

PATH SHIFT PACKET Packet:

Alert Identifiers	Failure Route IDs

Fig. 2. PATH SHIFT PACKET packet structure

VII. SIMULATION

This section discusses the details of simulation and results.

A. Simulation Environment

To evaluate the performance efficiency, the Event driven simulator NS-2.34 is used for simulations of proposed protocol. Below is the list of parameters used in this study simulation work.

Table 1: Simulation parameters

Network size	900m ×900m
Number of nodes	21
MAC	802.11
Average speed of nodes	1m/s, 5m/s, 10m/s and 15m/s
Source transmission rate	4 packet/sec
Packet size	512 bytes
Simulation Time	160 sec
The propagation Model	TwoRayGround
Mobility model	Random Waypoint

We have examined the system for cases: (1) Network with no misbehaving nodes, (2) Network with misbehaving nodes and no detection. (3) Network with misbehaving nodes and AOMDV-MRS protocols and, (4) Network with misbehaving nodes and cooperative approach.

B. Simulation Snapshots

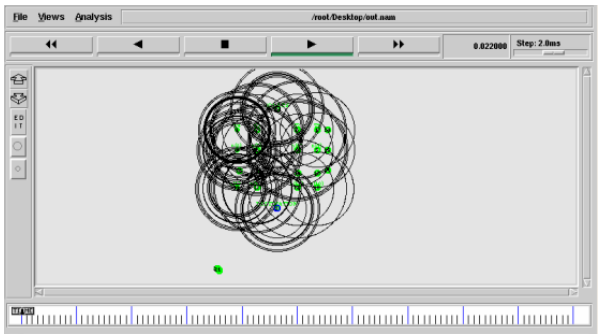

Fig. 4. Network Simulator

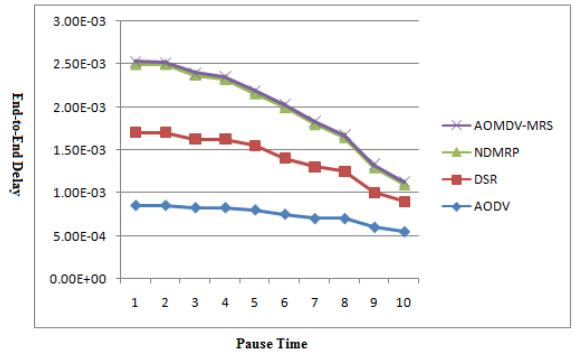

Fig. 5. End-to-End Delay Vs Pause Time

From the Fig. 5 obtained for delay, it can be observed that the end-to-end delay i.e. average time taken by packets to reach from source to destination is considerably reduced with AOMDV-MRS protocols, when compared with NDMRP, DSR and AODV protocols. It is because, a whener packet fails to reach to destination, it is informed to source within a particular time threshold. This time threshold is greater in NDMRP, DSR, and AODV. Hence, in the incurred is more.

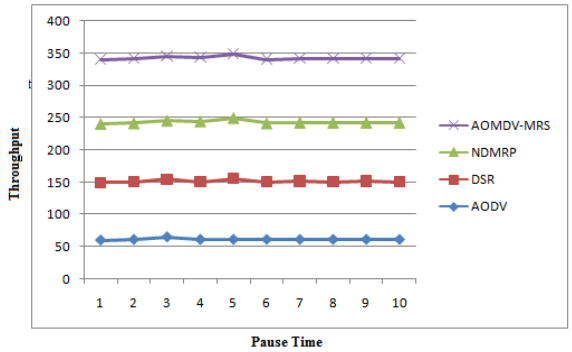

Fig. 6. Throughput Vs Pause Time

From Fig. 6 obtained for Throughput when the AOMDV-MRS protocols is compared with NDMRP, DSR and AODV .It shows that the proposed multi-path routing protocols throughput improvement. It is because, whenever there packets are dropped, the most of missing packets are retransmitted again over some another reliable route. Hence, packets loss is kept minimum. The AOMDV-MRS protocols avoid false detection and computational complexity.

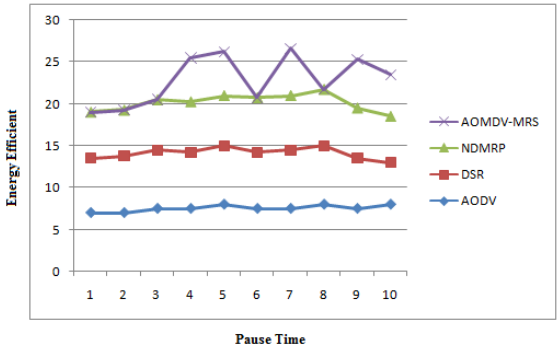

Fig. 7. Energy Efficient Vs Pause Time

From Fig. 7 obtained for Energy Efficient, it can be observed that the energy efficiency i.e., that the multipath routing protocols is considerable energy efficiency is stable and has little impact by the increase of the network size, while the performance of other schemes degrades with larger network size. When compared with NDMRP, DSR and AODV protocols. It is because; whenever packet fails to reach to destination, as the node density increase. When node density is high, there are more nodes available for data forwarding, and this increases the data transmission and buffer overflow, as the node density decrease. When node density is low, there are no more nodes available for data forwarding, and this decreases the data transmission. The AOMDE-MRS protocol has maintained constant delivery rates throughout the simulated scenarios because the nodes are selected based on the energy availability.

VIII. CONCLUSION AND FUTURE SCOPE

It can be observed that the end to end delay i.e. average time taken by packets to reach from source to destination is considerably reduced with proposed protocol, when compared with AOMDV. It is because, whenever packet fails to reach to destination, it is informed to source within a particular time threshold. This time threshold is greater in AOMDV. Hence, in AOMDV, the delay incurred is more. Throughput, when the proposed approach is compared with AOMDV, it shows that the proposed multipath routing protocol gives considerable throughput improvement. It is because, whenever there packets are dropped, the most of missing packets are retransmitted again over some another reliable route. Hence packet loss is kept minimum. The proposed protocol action in the form of TPI-PATH SHIFT PACKET control packet communication so that even the misbehaving node succeeds in being part of any route, still it

can be detected before the actual data transfer. The node co-operates in the beginning of data transfer to indicate that it is loyal node but then abruptly starts misbehaving in the middle of data transfer. The proposed approach avoids false detection and computational complexity and thus makes the overall network operation robust. There is one more dimension of misbehavior, i.e. packet altering misbehavior where the packet contents are altered. This dimension can be addressed by implementing encryption and decryption or hashing technique and it is the future scope of the proposed protocol.

REFERENCES

[1] Wenjing Lou, Wei Liu and Yanchao Zhang, "Performance Optimization using Multipath Routing in Mobile Ad Hoc and Wireless Sensor Networks", OMBINATORIAL OPTIMIZATION IN COMMUNICATION NETWORKS Maggie Cheng, Yingshu Li and Ding-Zhu Du (Eds.), 2005, Kluwer Academic Publishers.

[2] Baolin Sun, Xiaocheng Lu, Chao Gui, Ying Song and Hua Chen, "Network Coding-Based On-Demand Multipath Routing in MANET", 978-0-7695-4676-6/12 $26.00 © 2012 IEEE DOI 10.1109/IPDPSW.2012.191.

[3] Prokopios C. Karavetsios and Anastasios A. Economides, "Performance comparison of distributed routing algorithms inad hoc mobile networks", International Conference onTELEINFO - Mobile Computing and Mobile Networks,WSEAS Transactions on Communications, Vol. 3, Issue 1, pp. 12-15, May 2004.

[4] Sree Ranga Raju and Jitendranath Mungara, "Performance evaluation of zrp over aodv and dsr in mobile adhoc networks using qualnet", European Journal of Scientific Research ISSN 1450-216X, Vol. 45, No. 4, pp. 658-674, 2010.

[5] V. Kanakaris, D. Ndzi and D. Azzi, "Ad-hoc networks energy consumption: a review of the ad-hoc routing protocols", Journal of Engineering Science and Technology Review 3 (1), pp. 162- 167, 2010.

[6] Isha V. Hatware1, Atul B. Kathole, Mahesh D. Bompilwar, "Detection of Misbehaving Nodes in Ad Hoc Routing", Vol. 2, Issue 2, February 2012.

[7] Sankalp Bahadur Singh and Bharat Pesswani, "Performance analysis between AODV & DSR Routing Protocol presented performance evaluation of AO", Int. J. Computer Technology & Applications, Vol. 3 (4), pp. 1521-1527.

[8] Savita Gandhi SMIEEE, Nirbhay Chaubey MIEEE, Naren Tada, Srushti Trivedi, "Scenario-based Performance Comparison of Reactive, Proactive & Hybrid Protocols in MANET:, (ICCCI -2012), January 2012, Coimbatore, India.

[9] Fubao Yang, Shengzhi Ling, Hui Xu, and Baolin Sun, "Network Coding-based AOMDV Routing in MANET", Wuhan, Hubei, China; March, 2012.

[10] Mahesh K. Marina and Samir R. Das, "Ad hoc on-demand multipath distance vector routing", Wirel. Commun. Mob. Comput. 2006; Vol. 6, pp. 969–988.

[11] Manoj Kumar Mishra, Binod Kumar Pattanayak, Alok Kumar Jagadev, Manojranjan Nayak, "Measure of Impact of Node Misbehavior in Ad Hoc Routing", A Comparative Approach. In IJCSI International Journal of Computer Science Issues, Vol. 7, No. 8, July 2010.

[12] C. E. Perkins and P. Bhagwat, "Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers", In ACM SIGCOMM'94, pp. 234–244, London, England, August 1994.

[13] C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector routing". In IEEE WMCSA'99, pages 90–100, New Orleans, 1999.

[14] Nor Surayati Mohamad Usop, Azizol Abdullah and Ahmad Faisal Amri Abidin "Performance evaluation of aodv, dsdv dsr routing protocol in grid environment", IJCSNS International Journal of Computer Science and Network Security, Vol. 9, No. 7, July 2009.

[15] Marjan Radi, Behnam Dezfouli1, Kamalrulnizam Abu Bakar and Malrey Lee, "Multipath Routing in Wireless Sensor Networks: Survey and Research Challenges", Sensors 2012, 12, 650-685; doi:10.3390/s120100650.

[16] T. Kagi and O. Takahashi, "Efficient Reliable Data Transmission Using Network Coding in MANET Multipath Routing Environment", 12th International Conference on Knowledge-Based Intelligent Information and Engineering Systems (KES 2008), Zagreb, Croatia, September 3-5, 2008, pp. 183–192.

[17] B. Waxman, "Routing of Multipoint Connections," IEEE Journal on Selected Areas in Communications, Vol. 6, No. 9, 1988, pp 1617–1622.

[18] The Network Simulation ns-2, http://www.isi.edu/nsnam/ns/.