

Efficient Path Selection Routing based on Traffic-Size for Mobile Ad Hoc Networks

Bijay Guragain
Final Year, B.E. / ECE
Sona College of Technology
Salem, TN, INDIA

R.Vinod Kumar
Professor / ECE
Sona College of Technology
Salem, TN, INDIA

R.S.D.Wahidabanu, Ph.D
Principal
Government College of Engg.
Salem, TN, INDIA

ABSTRACT

Routing in Mobile Ad hoc Networks (MANETs) is a complex one due to the absence of any central coordinator and infrastructure. Congestion is one of the prominent reasons for link-failure in network due to the heavy traffic which leads to failure of nodes, network partition and topology change. Due to power drainage among nodes, network topology changes and the nodes should be well adaptive to respond quickly to the changes. Various existing routing protocols forward the data packets towards the destination through the path having less number of hop counts. However, these protocols do not minimize the traffic load in the network and thus causes congestion which reduces the network operation. A routing protocol called Efficient Path Selection (EPS) is proposed which enhances the quality of services' issues such as Packet Delivery Ratio, End to End delay, Energy Consumption and also provide secure transmission of data packets. This paper provides secure and efficient path routing. The simulation signifies that proposed protocol provides reliable secure transmission than the existing Implicit Source Routing (ISR) protocol.

General Terms

Routing, nodes, power, packets transmission, simulation

Keywords

MANETs, link-failure, hop count, traffic load, quality of service, efficient path, security

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) consists of a set of wireless mobile nodes communicating to each other without any centralized control or fixed network infrastructure [1]. MANETs have a number of applications that rely on multi-hop wireless infrastructures and can be deployed quickly. There are various applications which include emergency situations, battlefield, disaster relief, mining operations and health monitoring. Inefficient and un-adaptive routing is the major challenging issue for such networks. Efficient routing operations require collective cooperation of all nodes [2]. Routing protocols should be more dynamic to respond faster with respect to the topological changes [3].

Several routing protocols have been proposed for MANETs based on the routing table update mechanism. They are proactive or table-driven routing protocol and reactive or on-demand routing protocol. In table-driven routing protocols

every node maintains the network topology information rapidly in the form of routing tables by periodically exchanging routing information [4]. Routing information is flooded in the whole network. On the other hand, on-demand

routing protocols do not maintain the network topology information. They obtain the necessary path when it is required, by using a connection establishment process. Hence, they do not exchange routing information periodically. All these protocols use shortest path to forward packets to the destination. Shortest path is the path having minimum number of hop counts. But the selection of shortest path to route packets does not reduce traffic on the network, and creates congestion [5]. These crowded nodes decline the protocols' potential by reducing Packet Delivery Ratio, increasing End to End delay and Energy Consumption. Increasing traffic in a certain node depletes the battery power at a faster rate which is a serious problem in MANETs [6].

This paper explains the proposed routing protocol called Efficient Path Selection (EPS) which considers the traffic-size of a node and its neighboring nodes for path selection. This routing protocol EPS is used to reduce traffic around the nodes and eliminates congestion. In this protocol, nodes that forward packets keep record of traffic size in bytes of itself as well as the surrounding nodes of one hop count. The path load of packets which traverses more than one hop counts is the sum of all traffics along that path. It provides an efficient approach than the existing Implicit Source Routing (ISR) protocol [7]. The path load is calculated for all the nodes along the network and also the neighboring nodes to compare different paths. It represents traffic load that is experienced by packets which are to be routed on the path. The path having minimum load value is selected to route the packets. If the loads of multiple paths are same, then path having minimum number of hop counts will be chosen for broadcasting packets. Thus, EPS routing protocol selects efficient path with minimum path load.

Security is a major concern in wireless networks. Sequence number is provided to all the transmitted packets so that the secure reliable transmission can be achieved. Security is obtained by observing the transmission time of the forwarded packets.

2. RELATED WORK

Several load balanced routing protocols for MANETs have been proposed till date which focuses on various parameters like energy consumption, time delay, packet delivery ratio, accuracy etc. Most of the approaches are on-demand based protocols; that is, they combine load balancing strategies with path discovery. A path with the least load among multiple possible paths from source to destination is usually chosen [8]. A great challenge in the design of ad hoc network is the development of efficient routing protocols that can provide high quality communication between two mobile nodes [9]. The load balancing routing protocols for ad hoc wireless

networks can be classified into two types. One is based on "Traffic-Size" and the other is "Delay" [10].

Traffic-Size based protocols are Dynamic Load Aware Routing Protocol (DLAR) [11], Load Balanced Ad hoc Routing Protocol (LBAR) [9], and Load- Sensitive Routing Protocol (LSR) [12]. Among all these protocols, the load in a node is the number of packets stored in the node queue length and the path load is sum of loads of all the nodes along that path. The drawback of these protocols is that they cannot provide the actual load due to varying size of packets stored in a queue. But the proposed protocol EPS calculates the traffic size in bytes and hence actual load can be determined. Delay based protocols are Delay-Oriented Shortest Path Routing Protocol (DOSPR) [13] and Load-Aware On- Demand Routing Protocol (LAOR) [14]. These two protocols use the total path delay to select a path. Total path delay is the sum of time taken to generate route request packets (RREQ), route reply packets (RREP) and propagation delay along the path. The disadvantage of these existing protocols is that there is more delay in transmitting packets from source to destination. But the proposed protocol overcomes delay through efficient path.

Source routing provides simple, accurate and flexible transmission of packets by sender and there is no need to update routing table by the intermediate nodes [15]. Packet overhead increases in source routing since the packets should contain next feasible neighboring nodes information while broadcasting. This increases power drainage of nodes reducing life time of the network and increases bandwidth. Dynamic Source Routing (DSR) protocol maintains path by broadcasting RREQ packets from source to the destination through the neighboring nodes. Here, intermediate nodes rebroadcast RREQ adding overhead till it reaches the destination. Transmission acknowledgement is obtained by sending RREP from the destination. Hence path discovery and maintenance is achieved in DSR. By broadcasting simple BEACON signal periodically the protocol checks nodes' connectivity, network partition, node mobility, and traffic size so that nodes remind their existence without link-failure. Implicit Source Routing (ISR) is an advanced version of DSR in which the transmitting packets contain both the source and destination address [7]. An efficient path is established to transmit a packet between source and destination which is

simply the number of nodes that are involved along the path to forward packets. Each node of any given path knows its past and future nodes on the path. The entire broadcasted packets through any path contain an address that solely identifies the path through intermediate nodes that hand over the packets to

the neighboring node on the path till they reach the destination. In MANETs, every node acts as a router; a node should be able to route packets through more than one path. Every node which is forwarding packets keeps record of routing table of all possible paths. This table keeps updating the available paths and provides efficient path based on comparison. The path is created by two ways. The first is Finding Path, where the source node uses a flooding technique to determine the path to the destination and there may be various paths to route packets to the destination node [16]. In every path the intermediate nodes forward the packets to reach from source to destination. The second is Initializing Path among all the intermediate nodes based on routing table information. Each node provides an entry to the routing table for new path selection. In case of any node failure due to power drainage or by any other means, the path will be broken changing network topology due to partition, and then the protocol removes the existing path from all the available nodes.

Security in MANETs is mainly focused on providing secure transmission for forwarding the packets to destination to prevent from any middle attacks [17]. It is uncertain that an intermediate node may remove or add extra nodes in the packets forwarding path in source routing protocols. To prevent any intermediate attack each node must be able to predict the transmission time around the neighboring nodes [18]. This problem is overcome by the proposed method.

3. EFFICIENT PATH SELECTION

The proposed routing protocol, Efficient Path Selection (EPS) measures the traffic size in bytes and also provides secure communication by observing the transmission time between source and destination. The existing protocols measure the traffic load in number of packets present in a node's queue length and it does not measure accurate load because packets are of different size. EPS routing protocol finds routes on-demand and makes use of hop-by-hop technique to maintain routing table updates at every intermediate nodes. Sequence numbers are used to prevent looping, multiple transmissions and provides secure reliable transmission. Route Request (RREQ) packets are sent to make a route request, Route Reply (RREP) packets are used to send back the route and simple BEACON signal is sent at regular intervals by the intermediate nodes to find the correct information of the neighboring nodes in case of any link failure. Implicit Source Routing (ISR) protocol is an improved type of Dynamic Source Routing (DSR) which provides efficient packet transfer between the nodes than DSR [4]. The major issue in ISR is the path allocation process that cannot repair a broken path.

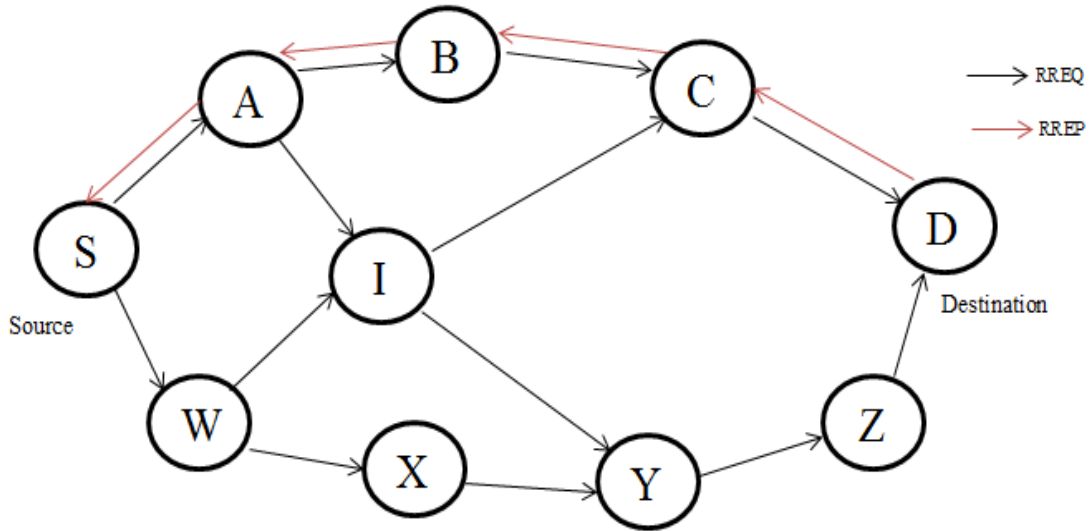


Figure 1: Packets routing through efficient path

The frequent path breakage forces the intermediate nodes to drop packets as there are no other available paths to destination. There is delay in connection establishment between the nodes and the protocol performance is poor at higher mobility of nodes. This overall reduces Packet Delivery Ratio (PDR), increases End to End delay and Energy Consumption.

Figure 1 illustrates the efficient path for packets routing from source 'S' to destination 'D' using EPS protocol. Every time an intermediate node receives a RREQ, it will calculate the traffic load and compares with the previous one to provide efficient path. Therefore the path selection of a node is variable and changes adaptively according to the load status of the network. Source node 'S' forwards the data packets to the destination node 'D' through the nodes 'A', 'B', and 'C' with least hop count. In EPS routing protocol, the node records both number and size (in bytes) of the packets that transmits in a particular path. Any packets routed in a path possess information about the time of entrance, its number and traffic size. Thus the Entry Load (EL) of the path 'i' at any node of the network is obtained as [5],

$$EL_i = \frac{ETS_i + (PN_i \times MHS)}{ECT_i} \quad (1)$$

Where, ' ETS_i ' is buffered Traffic Size (bytes) of entry 'i'.

' PN ' is the number of packets at entry 'i'.

' MHS ' is the MAC Header size (WLAN).

' ECT ' is ' i^{th} ' entry creation time(s).

' EL_i ' is the traffic load (bytes per second) of a single entry 'i' at any given node. The term ($PN * MHS$) in the equation (1) provide MAC contention as a traffic size. If the number of packets increases, MAC contention and entry load also increases. The Local Load (LL) of a node 'n' is calculated as,

$$LL_n = \sum_{i=1}^k EL_i \quad (2)$$

Where, ' k ' is the number of entries at node 'n'.

' LL_n ' is the sum of the load at node 'n' for all the 'k' entries that signifies the total traffic load present in the node 'n'. A load at any node depends on the traffic that is routed through the node itself as well as the traffic that is routed through its surrounding nodes. Thus, the Neighboring Load (NL) of node 'n' is obtained as,

$$NL_n = \sum_{\forall g} LL_g \quad (3)$$

Where, ' g ' is the number of neighboring nodes of node 'n'. Hence, the Total Load (TL) at node 'n' is the sum of Local Load and Neighboring Load which can be obtained from equations (2) and (3).

$$TL_n = LL_n + NL_n \quad (4)$$

' TL_n ' is the actual traffic load along and around the node 'n' which is the fundamental parameter for measuring traffic load in MANETs according to the proposed protocol EPS.

If ' P ' denotes the path between source and destination node then the Path Load function ' $PL(P)$ ' to calculate the load of that path is obtained as,

$$PL(P) = \sum_{j=1}^n TL_j \quad (5)$$

Where, ' n ' is the number of nodes on the path ' P ' excluding the source and destination node. For example; if ' P ' is the path between source 'S' and destination 'D', then there are three intermediate nodes 'A', 'B', and 'C' whose path load function is to be computed. The path load function on any path ' P ' represents the traffic load that has been experienced by the packets on that path. Path selection by a node is obtained by observing path function of all the available paths. The path having least load value is preferred to route the traffic. If there are multiple paths having the same value, then path having least hop count is chosen.

Among various attacks in MANETs, the prominent one is route reply (RREP) attack where an intruder takes control of RREP packets and causes network poisoning or jamming. To prevent such threats, network protocol should identify such injected delayed packets and ignore them. The proposed protocol adds this feature and provides secure reliable transmission. The time (t_i) taken by packets to reach from source to destination securely is obtained as,

$$t_1 = t_{src} + t_{des} + t_{del} + t_{seq} \quad (6)$$

Similarly, the time (t_2) taken by packets to reach from source to destination after attack is obtained as,

$$t_2 = t_{src} + t_{des} + t_{del} \quad (7)$$

Where,

' t_{src} ' is source request time.

' t_{des} ' is destination response time.

' t_{del} ' is transmission delay.

' t_{seq} ' is packet sequence number check time.

When there are no threats the packets sequence number gets updated regularly thus decreasing delay time. But when there are threats, packets reach the destination after some delay and hence the packets sequence number is not considered for delayed and injected packets in equation (7). This discards such delayed packets and provides secure transmission.

4. SIMULATION RESULTS

The performance of ISR and EPS has been evaluated in terms of Packet Delivery Ratio, End to End delay, Energy Consumption per packet and Security with different Pause Time for simulation. NS-2 with CMU option performs wireless network simulation, and is used to conduct the simulation for 50 mobile hosts with transmission range of 250m. Constant Bit Rate (CBR) is used for simulation. The channel capacity of the mobile hosts is set to 2Mbps. For MAC layer protocol, IEEE 802.11 (WLANs) is used. The source and destination nodes are randomly selected obeying random waypoint model [19] with CBR packet size of 512 bytes and packets send rate of 5 bytes per second. Each node moves randomly in a square space of 800m x 800m with the speed of 0 to 20 m/s randomly. A node pauses for a certain period of time called Pause Time (s) when it reaches a new location and then again moves to another new location. Initial energy of 0.5J is set to all the nodes. The parameters used for simulation are depicted in Table 1.

Table 1: Parameters used in Simulation

Parameter	EPS	ISR
Buffer Size	64	64
Routing Table Size	64	30
Route Reply	OFF	ON
Queue Length	50	50
BEACON Signal Interval	Dynamic	-----
Lost BEACON Signal Limit	3	-----
Delay Limit	600ms	-----
MAC Header Size	30 Bytes	-----

4.1 PACKET DELIVERY RATIO

Packet Delivery Ratio (PDR) is calculated by taking the ratio of the number of data packets received at the destination to the number of data packets sent by the source. This specifies the maximum packets received at the destination. The maximum value of PDR indicates the improvement on Throughput. The higher delivery ratio signifies the advancement of routing protocol. The tabulation of PDR Versus Pause Time (s) for 50 nodes with different values of Pause Time is given below in Table 2. Six Pause Time values (0,100,200,300,400,500) are used to vary mobility of nodes. Here, 0s Pause Time indicates that the nodes are continuously moving and 500s shows that the nodes are stationary.

Table 2: Packet Delivery Ratio for ISR and EPS

Pause Time(s)	ISR	EPS
0	0.16	0.42
100	0.28	0.46
200	0.32	0.54
300	0.41	0.59
400	0.44	0.63
500	0.49	0.70

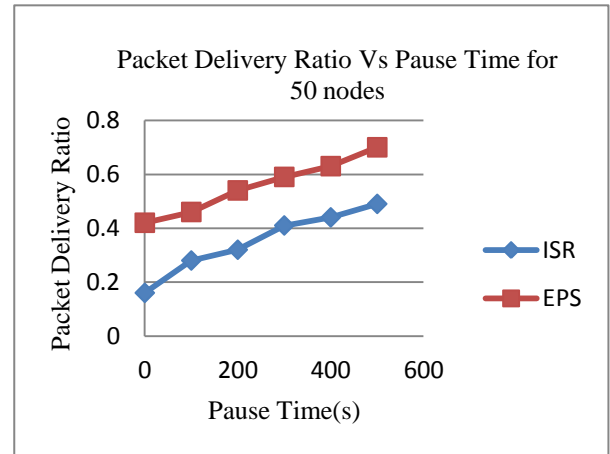


Figure 2: Packet Delivery Ratio Vs Pause Time for 50 Nodes

From figure 2, EPS has higher PDR than ISR. EPS has an average of 60% higher delivery ratio than ISR while transmitting packets to destination. ISR transmits less than 50% of data packets when the nodes become stationary while EPS transmits 70% of the data packets that were sent by the source. The reason is that at the central node traffic gets concentrated in ISR and interface queue length cannot store all the packets resulting loss of packets due to less available buffered space and collision of heavy packets.

4.2 END TO END DELAY

End to End delay is the time (second) taken by packets to reach the destination. It is calculated by subtracting time at which first packet was transmitted by source node from time at which the first data packet reached to destination. The least value of delay specifies the better performance. The tabulation of End to End delay Versus Pause Time (s) for 50 nodes with different values of Pause Time is given below in Table 3. Six Pause Time values (0,100,200,300,400,500) are used to vary mobility of nodes. Here, 0s indicates that the nodes are continuously moving and 500s shows that the nodes are stationary.

Table 3: End to End delay(s) for ISR and EPS

Pause Time(s)	ISR	EPS
0	8.8	3.4
100	5.2	2.9
200	6.3	2.5
300	5.4	2.3
400	5.7	2.4
500	6.5	1.8

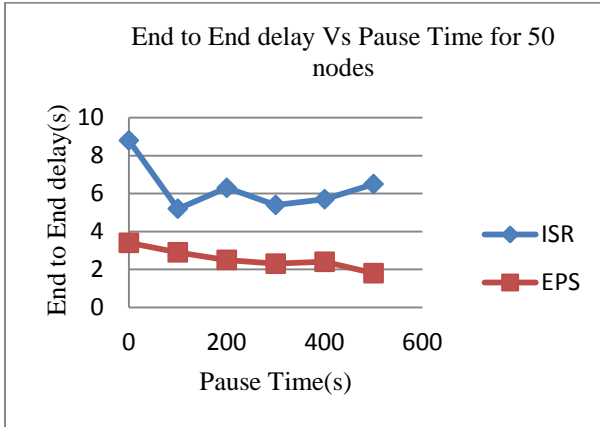


Figure 3: End to End delay(s) Vs Pause Time(s) for 50 nodes

Figure 3 illustrates better End to End Delay performance for EPS than ISR. The average value of End to End Delay is 6.32s for ISR and 2.55s for EPS. This depicts that EPS has about four seconds less delay than ISR. At the highest level of mobility i.e. lowest Pause Time (0s) the delay difference has highest margin. The reason is that there is heavy traffic in ISR resulting high congestion so that data packets have to wait for a longer time in the queue. This is eliminated in EPS by selecting path having least Load function.

4.3 ENERGY CONSUMPTION

Energy consumption is obtained by the ratio of the total energy consumed to the total number of nodes present in the deployed network. The Energy per Packet is calculated in Joules (J). The least value of Energy consumption per Packet specifies the better performance. The tabulation of Energy consumption per Packet Versus Pause Time (s) for 50 nodes with different values of Pause Time is given below in Table 4. Six Pause Time values (0,100,200,300,400,500) are used to vary mobility of nodes. Continuously moving nodes have 0s Pause Time and 500s Pause Time when they become stationary.

Table 4: Energy (J) /Packet for ISR and EPS

Pause Time(s)	ISR	EPS
0	0.40	0.04
100	0.18	0.06
200	0.10	0.08
300	0.07	0.05
400	0.12	0.09
500	0.05	0.02

Energy Consumption model for IEEE 802.11 WLAN pc card having 2 Mbps Bandwidth has Transmit and Receive Power of 0.660W and 0.395W respectively.

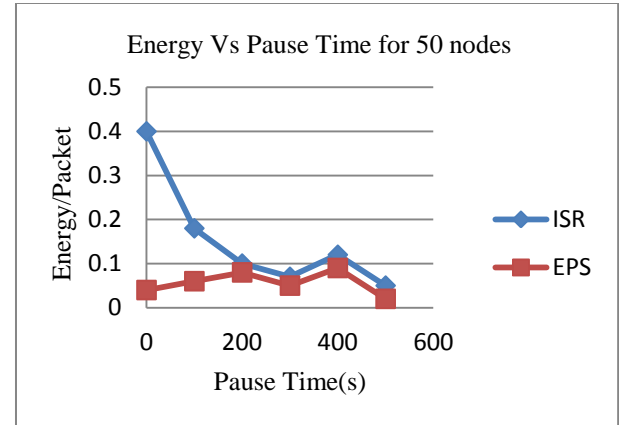


Figure 4: Energy (J) /Packet Vs Pause Time(s) for 50 nodes

Figure 4 shows lower Energy Consumption for ESP than ISR. The average Energy Consumption per Packet for ISR is 0.15J while it is 0.056J for EPS. This depicts that energy consumption of EPS is about 0.094J less than that of ISR. At the highest level of mobility i.e. lowest Pause Time (0s) the energy difference has highest margin. The reason is that there is an alternate path creation in ISR by flooding technique and has high energy consumption. This is eliminated in EPS by selecting path having least Load function.

4.4 SECURITY

Security is a major concern in MANETs because of absence of centralized network, topology change and low power as compared to traditional networks. Packet Delivery Ratio (PDR) can be increased by reducing the number of packets transmitted ignoring old and the injected malicious packets with the help of sequence number. The tabulation of PDR of both secure and insecure packets Versus Pause Time (s) for 50 nodes with different values of Pause Time is given below in Table 5. The higher delivery ratio signifies the advancement of routing protocol. The tabulation of PDR Versus Pause Time (s) for 50 nodes with different values of Pause Time is given below in Table 2. Six Pause Time values (0,100,200,300,400,500) are used to vary mobility of nodes. When the nodes have 0s Pause Time, then they move continuously and become stationary after 500s.

Table 5: PDR for Secure and Insecure packets

Pause Time (s)	Secure Packets PDR	Insecure Packets PDR
0	1	0.92
100	1	0.76
200	1	0.59
300	1	0.46
400	1	0.38
500	1	0.20

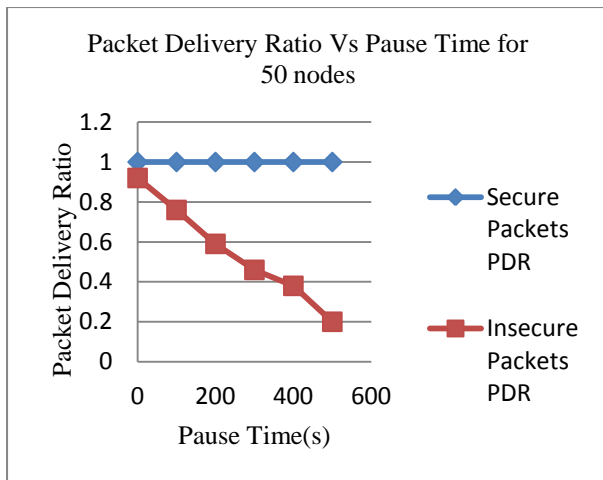


Figure 5: Packet Delivery Ratio Vs Pause Time for Secure and Insecure Packets

Figure 5 depicts that packets are delivered securely with 100% delivery ratio in EPS whereas in ISR there is drastic decrease at higher pause time. The difference is about 80% at highest pause time i.e. lowest mobility. On introducing packets sequence check time, only current packets are sent among the intermediate nodes. This reduces middle attacks and increases PDR.

5. CONCLUSION

This paper presents an efficient secure way of routing packets in ad hoc wireless networks. The proposed routing protocol EPS gives an ideal way of measuring traffic in bytes due to which reliable secure transmission is achieved in terms of Packet Delivery Ratio, End to End delay and Energy consumption. The packets sequence check time further enhances security and reduces transmission time. Thus, EPS provides the shortest secure path routing than the existing ISR protocol. The future work can be extended by comparing with other existing routing protocols and to provide secure reliable transmission in MANETs.

6. REFERENCES

- [1] Palanisamy and B. Renuka Devi (2012). MANET Routing Protocols Performance Evaluation in Mobility, Digital Communication, Prof. C Palanisamy (Ed.), ISBN: 978-953-51-0215-1. <http://www.intechopen.com/books/digital-communication/manet-routing-protocols-performance-evaluation>.
- [2] Suchita Baxla and Prof. Rajesh Nema, "Performance Analysis of AODV, OLSR, DSR AND GRP routing protocol of Mobile Ad-hoc network- A review" International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 2, Issue. 6, June 2013, pp. 359-362.
- [3] C. Perkins, E. Belding-Royer and S. Das, "Ad Hoc on Demand Distance Vector (AODV) Routing Protocol," IETF Internet RFC 3561, July 2003.
- [4] Anju Gill and Chander Diwaker, "Comparative Analysis of Routing in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012.
- [5] Abdulrahman H. Altalhi and Golden G. Richard, "Dynamic Routes Through Virtual Paths Routing for Ad Hoc Networks", 2011, Computer Science Department, University of New Orleans, LA, 70148 USA.
- [6] Ren-Hung Hwang, Chung-Ying Wang, Chi-Jen Wu and Guan-Nan Chen, "A novel efficient power-saving MAC protocol for multi-hop MANETs", International Journal of Communication Systems (2011).
- [7] Yih-Chun Hu and David B. Johnson, "Implicit Source Routes for On Demand Ad Hoc Network Routing", Department of Computer Science, Rice University, Houston, TX 770051892 USA.
- [8] Chai Keong Toh, Anh-Ngoc Le and You-Ze Cho, "Load Balanced Routing Protocols for Ad Hoc Mobile Wireless Networks", Communications Magazine, IEEE Publication Year: 2009, Page(s): 78 – 84.
- [9] H. Hassanein and A. Zhou, "Routing with Load Balancing in Wireless Ad Hoc Networks," in Proceedings of ACM MSWiM, Rome, Italy, July 2001.
- [10] Altalhi and G. Richard, III, "Virtual Paths Routing: A Highly Dynamic and Adaptive Routing Protocol for Ad Hoc Wireless Networks", 1st International Workshop on Mobile peer-to-peer Computing (MP2P'04), Orland, USA March 14-17, 2004.
- [11] S.-J. Lee and M. Gerla, "Dynamic Load-Aware Routing in Ad Hoc Networks," in Proceedings of IEEE ICC'01, Helsinki, Finland, June 2001.
- [12] K. Wu and J. Harms, "Load-Sensitive Routing for Mobile Ad Hoc Networks," in Proceedings of IEEE ICCCN'01, Scottsdale, AZ, October 2001.
- [13] S.-T. Sheu and J. Chen, "A Novel Delay-Oriented Shortest Path Routing Protocol for Mobile Ad Hoc Networks," in Proceedings of IEEE ICC'01, Helsinki, Finland, June 2001.
- [14] J.-H. Song, V. Wong, and V. Leung, "Load-Aware On-Demand Routing (LAOR) Protocol for Mobile Ad hoc Networks," in Proceedings of IEEE Vehicular Technology Conference (VTC Spring), Jeju, Korea, April 2003.
- [15] David B. Johnson, David A. Maltz, and Josh Broch, "The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks", In *Ad Hoc Networking*, edited by Charles E. Perkins, chapter 5, pages 139–172. Addison- Wesley, 2001.
- [16] Boukerche. A, Turgut. B, Aydin. N, Ahmad. M. Z, Bölöni. L and Turgut. D, Routing protocols in ad hoc networks: A survey, Elsevier Computer Networks, doi:10.1016/j.comnet.2011.05.010, Volume 55, Issue 13, 15 September 2011, Pages 3032-3080.
- [17] Y. Hao et al, "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, 2004.
- [18] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", ACM MOBICOM, 2002.
- [19] Esa Hyttia and Jorma Virtamo, "Random Waypoint Mobility Model in Cellular Networks", Networking Laboratory, Helsinki University of Technology, Finland.