# An Efficient Energy Method For Hybrid Routing In Manet Using Evolutionary Algorithm

Naveeta[1], Dr. Mahendra Kumar[2]
M.Tech (Scholar), Deputy Dean Research
Department of ECE
Guru Kashi University, Talwandi Sabo, Bathinda (Punjab)
*mohitkumar_09@yahoo.com[1], dei.mahendra@gmail.com[2]*

***Abstract*—** Manet network in which all movable nodes are free to shift in any position and connect to each other by WN. In order to create a data communication through the mobile nodes, the mobile nodes periodically construct the way among others. Every gadget in a MANET is allowed to move freely toward any path, and will, along these lines change its connects to different gadgets habitually. Each must forward movement inconsequential to its own particular utilize, and thusly be a switch. The essential test in building a MANET is preparing every gadget to constantly keep up the data required to legitimately course movement. Such systems may work without anyone else's input or might be associated with the bigger Web. The structure of some networks makes it attractive to several kinds of attackers. The wormhole attack is a kind of attack which is creating the various duplicates nodes in the MANET network. The tunnel exit between twice duplicate nodes is referred to as a WHA in the network, which are necessary so as to give secure data communication. In MANET security could be improved by using routing schemes and optimization methods. The routing scheme used to improve the security and performance of the network using DSR and DSDV routing method and EA. MANET research work, has mainly described in developing an effective routing schematic structure in luck as a High dynamic, resource constrained network. At present, various effective routing methods have been implemented for MANET. Most of these Routing schemes assume a trusted and supportive environment. The presences of duplicate nodes, which are attacker node in the networks are vulnerable to several types of attacks. In MANET network designed by the MATLAB simulation Tool uses accurate and correct values which could be utilized for comparison various routing schemes. After that the reviewing all the above graphs, it could be accurately calculated that the performance of HYBRID and EVOLUTIONARY algorithm is more efficient by the wormhole in terms of PDR, E2E delay, PL and Throughput etc.

***Keywords*—** *MANET(Mobile Adhoc Network), MATLAB (Matrix Laboratory), EA (Evolutionary Algorithm), WHA (Worm Hole Attack).*

## I. INTRODUCTION

MANET is Mobile Ad-hoc Network [1] It is a self-organized, infrastructure less networks. The non-attendance of a foundation in the specially appointed framework postures incredible difficulties in the usefulness of these systems. In this manner, a remote specially appointed system with versatile handles as a Mobile Ad Hoc Network. In a MANET, every one of the gadgets are connected by remote connections. Every device in a MANET is allowed to move freely in every one of the bearings. It can change its connections to different gadgets habitually. Hubs are arbitrarily associated with each other, utilizing optional topology. They can go about as the two switches. The essential test in building a MANET is preparing every gadget to persistently keep up the data which are important to legitimately course the activity. As MANETs are represented by constraining data transmission and handle portability, there is request to takings into account the vitality productivity of the hubs [2].

MANET (Mobile Ad-hoc Network) utilizes a multi-hop display. It is a kind of remote exceptionally selected framework, outline itself and don't each other to keep up the framework. All mechanisms can move thoughtlessly and also create themselves. In a MANET, the transmission exists using multi rebound course, where center points can share radio channels [1]. Every center point can meander openly all over and associations can similarly be exchanged in the meantime in MANET.

The two applied methodologies of MANETs are:

- Reactive routing protocols manage the huge amount of traffic on the internet when there is a call. Like DSR (Dynamic source routing) and AODV(Ad hoc on demand distance vector).
- Proactive routing protocols dynamically maintain the complete perception of topologies i.e., Babel, Optimized Link State Routing Protocol.

A few highlights that arrange MANETs not the same as associated system and need crisp approaches to execute organize capacities are:

- ***Wireless medium:*** A radio channel utilized by gadgets to reach each other has screwy properties, which is less proficient and helpless against impedance.

- ***Dynamic Topologies:*** Gadgets can move arbitrarily with one of a kind speed levels. Subsequently topologies change arbitrarily in any circumstances.[4]
- ***Infrastructure less Network:*** Stable foundation isn't vital.
- ***Power management:*** Delicate hubs rely upon batteries for control. Consequently component for such framework planned with control limitations.[5]
- ***Peer-to-peer nature:*** One of a kind attribute of an impromptu system require the methods not quite the same as associated lattice, particularly at bringing down layer to perform proficiently [6].

There are certain kind of issues are occurring in the MANET and MANETs are susceptible to airstrike's due to following reasons :-[7]

- ***Open Medium:*** Intruding is conceivably less demanding than associating organize.
- ***Deficiency of centralized monitoring:*** any combined framework is absent.
- ***Deficiency of clear LOD (line of defense):*** the line of barrier used to capture the showdown. Establishment of organized security is required to anchor the defenseless point.
- ***Co-operative Algorithm:*** MANET calculation requests responded certainty among hubs to abuse the system rule [10].
- ***Quality of Service (QoS):*** Providing diverse nature of benefit levels in an always showing signs of change condition forces a further test [8].

## II. RELATED WORK

**Parvinder Kaur, et al., (2017) [9]** examined and associated the implementation of ad hoc on demand distance vector, dynamic source routing and zone routing protocol (AODV, DSR and ZRP) in the presence of abundant wormhole assault nodes. A Mobile Ad hoc arranges had ascended as a self-decision, multi-bob, remote and short lived sort of framework which worked inside the impediments like transmission limit, power and imperativeness. MANET could be viewed as an open kind of framework where center points transform into a bit of any framework of whatever point that was the reason it was threatening to different sorts of strikes. Wormhole attack was most undermining security ambush in uniquely designated framework where an attacker's center point gets distributed, one territory and replay them at other region which was remotely arranged for. Contrasting circumstances were depicted as like ordinary of 50 runs and adaptability. By authentic position of various wormhole center points over the framework, the determination of the execution to the extent throughput, package, transport extent, allocate ordinary end to end delay and jitter. In conclusion, the investigation of the most impacted coordinating tradition to the extent framework estimations.

**Xuan Liu, et al., (2017) [31]** described the advancement over the ICN and give a brief explanation of its enhanced patterns. Later, interpret the improvement of ICMANET and framework a graph of it. As the future Internet building, data driven systems administration (ICN) could in like manner offer unrivaled outline strengthen for multipurpose uniquely substitute designing organization. In this way, data driven MANET (ICMANET), another crosscutting investigation locale, was well ordered to form. Subsequently, a description show for content guiding and arrange the substance coordinating into proactive, responsive and knowing composes, and a short time later detail the operator designs. In conclusion, the present issues were combined. The goal was to give the references and guidelines to pre-clients advancing toward contemplate on the new domain.

**Marco Conti, et al., (2014) [10]** determined the mobile multi hop networking. All these networks were linked to the orchestrations produced under the IETF. Therefore, it was called as mobile ad hoc networks. Regardless, it was not orchestrated. In this article, the beginning was from the reasons why the MANET perspective did not significantly influence of PC exchanges, and the main focal point was on the improvement of the multi-hop uniquely named designs organization perspective by developing the exercises picked up from the MANET asks about. The main research was on the four compelling designing organization perfect models, work, sensor, keen, and vehicular frameworks that inclined MANET world as a more practical utilization of the multi-bounce uncommonly delegated frameworks organization perspective. Furthermore, the exhibited another exploration bearing in the multi-jump exceptionally named frameworks organization field: people centric sorting out, actuated by the growing passageway of the mobile phones in the customary everyday presence, which was delivering a people-driven insurrection in handling and exchanges.

**Nai-Wei Lo, et al., (2013) [11]** invented a secure routing protocol to prevent the data and network resources from malicious assaults. The chief preventions were from the black hole attack. General MANETs was formed through powerful wireless mobile gadgets which access to restricted resources, reduced network bandwidth along with restricted power consumption. However, framework less focal base station, organize administration and tasks done agreeably by every cell phone in arrange. MANETs were inclined to assaults like: helpful dark opening assault requires no less than two malignant gadget hubs was a genuine security danger since it was anything but difficult to dispatch and difficult to distinguish. Examinations with Qual Net demonstrate that the proposed convention offers up to 2.6 times execution as far as the parcel conveyance proportion when contrasting and AODV convention under helpful dark opening assault.

## III. SEVERAL ROUTING PROTOCOLS

Routing Protocol is secondhand to discover reasonable courses between communication hubs. It is a self-coordinated variety of portable clients that talk temperately finished transfer speed limitation remote connection. Since the hubs are multipurpose, the framework topology may change randomly after some time. The system is de-unified and all the system exercises like deciding the topology and conveying correspondences must be executed by the hubs [12]. They don't utilize any

passageway to attach to different hubs.It must have the capacity to switch high versatility of the hubs. MANET directing conventions could be a comprehensive mystery into three noteworthy classifications: -

1. Proactive,
2. Reactive and
3. Hybrid routing protocols.

**Table no: 1 Routing Protocols**

| Routing Protocols | Pros | Cons |
|---|---|---|
| **Proactive or table driven directing conventions:** In proactive steering, every hub needs to save at least one table to store directing data, and any adjustments in organizing topology should be recreated by spreading advises all through the [4] arrange with a specific end goal to protect a dependable system see. | Always the presence of information in the network. A chief focus at the latency. | Higher chances of overhead. The information about routing creates a huge flood on the network. |
| **Reactive routing:** is otherwise called on-request directing convention along these lines they don't save directing data or directing movement at the system hubs if there is no message. In the event that a hub needs to send a parcel to another hub, then this convention investigations of the course in an on-request way and starts the association so as to transmit and get the bundle. The course disclosure rises by flooding the course, ask for parcels all through the system. | The accessibility of path creation is high in case of low chances of overhead. The data is free from the structure of various loops [13]. | Latency is a major challenge in the network. |
| **Hybrid Protocol:** They present a mixture display that associations re-dynamic and genius dynamic overwhelming conventions. The Zone Routing Protocol is a crossover directing convention that partitions the system into zones. ZRP gives an ordered engineering where every hub needs to keep up extra topological data requiring additional memory. | Best for selecting huge network. The information is always updated in the network. | Issues related to complexity due to the larger framework of network [14]. |

## IV. SECURITY THREATS AND ISSUES IN MANET

The military strategies and other security processes are still best application area of ad hoc networking. Though there is a tendency to acquire ad hoc networks for various purposes such as commercial utilization because of their high-class possessions. Although, like to other networks, MANET also threatens to huge number of security attacks. MANET isn't just getting all the security dangers tested in both wired and remote systems, yet it additionally introduced wellbeing attacks extraordinary with it. In a MANET, wellbeing is a testing issue because of the vulnerabilities that are connected with it.

Yet, these hubs can yet these handles can unobtrusively control their destructive activities in such a way, to the point that it winds up hard to proclaim a hub as malicious.

- **Black hole Attack**

In this assault, an aggressor publicizes a zero metric for all goals, making all hubs around it course bundles towards it. A malevolent hub sends counterfeit directing data, asserting that it has an ideal course and makes another great hubs course information passes through the noxious one.

- **Sinkhole Attack**

In a sinkhole assault, a traded off hub attempts to draw on the information to itself from every neighboring hub. In this way, for all intents and purposes, the hub listens in on every one of the information that is being imparted between its neighboring hubs. Sinkhole assaults can likewise be actualized on Adhoc systems, for example, AODV by utilizing blemishes, for example, boosting the arrangement number or limiting the jump check, so the way exhibited through the vindictive hub has all the earmarks of being the best accessible course for the hubs to impart.

- **Gray hole Attack**

This assault is otherwise called steering bad conduct, assault which prompts dropping of messages. Gray hole has two stages. On the main stage the hub promotes itself as having a legitimate course to the goal while in the second stage, hubs drops captured bundles.

- **Denial of Service Attack**

Denial of administration assaults is gone for finish interruption of storing data and in this manner the entire task of the specially appointed system.

- **Sybil Attack**

The Sybil assault, particularly goes for circulating framework conditions. The assailant endeavors to go about as a few distinct personalities/hubs instead of one. This permits him to produce the consequence of a voting utilized for limit security techniques. Since specially appointed systems rely upon the correspondence between hubs, numerous frameworks apply repetitive calculations to guarantee that the information gets

from source to goal. An outcome of this is aggressors have a harder time to decimate the uprightness of data [15].

**Table no: 2 Comparative Study of Attacks**

| Attacks | Packed Loose | Battery Power | Delay |
|---|---|---|---|
| Worm Hole | 50 percent | Extremely high | 20 percent |
| Sybil Attack | 30 percent | Normal | 20 percent |

## V. PROPOSED WORK

In this section , defined that the proposed work in MANET. The objectives are mentioned below:

1. To study the various routing protocols, and attacks in Mobile ad-hoc network.
2. To implement a hybrid approach to detect the wormhole attack in the Mobile Networks.
3. To design evolutionary algorithms to perform the prevention phase in the NETWORK.
4. To evaluate the performance parameters with Hybrid and Evolutions techniques using throughput, E2E delay, Jitter, Packet Delivery Rate and Compared with the Existing technique (Routing Protocols).

The hybrid approach has implemented in DSDV and DSR routing protocol.

DSDV extends variation Bellman Ford Routing framework. Every contraption spares the table involving information about existing centers. It requires every contraption in framework to propel its own particular guiding table to neighboring center points [14]. DSDV is adjusted from the standard Routing Information Protocol (RIP) to extraordinarily delegated framework directing. It joins another trademark, gathering numbers, to each course table area of the standard RIP. Utilizing the starting late included assembling number; the flexible focus focuses can see stale course data from the new and along these lines keep the progression of organizing circles. It requires each adaptable station to announce, to its each present neighbors, its own specific directing table (for instance, by conveying its passageways).

DSR tradition was made for multi hop remote uncommonly delegated framework [16] contains "Course Maintenance" and "Course Discovery" for self-made nature. Data package saves data of widely appealing center points in the header for a specific objective. Utilizing DSR, the system is completely self-managing and self-engineering, requiring no present structure foundation or affiliation. The system focuses guides collaborate toward forward packs for each other to permit correspondence over different "skips" between focus focuses not immediate inside remote transmission degree of each other.

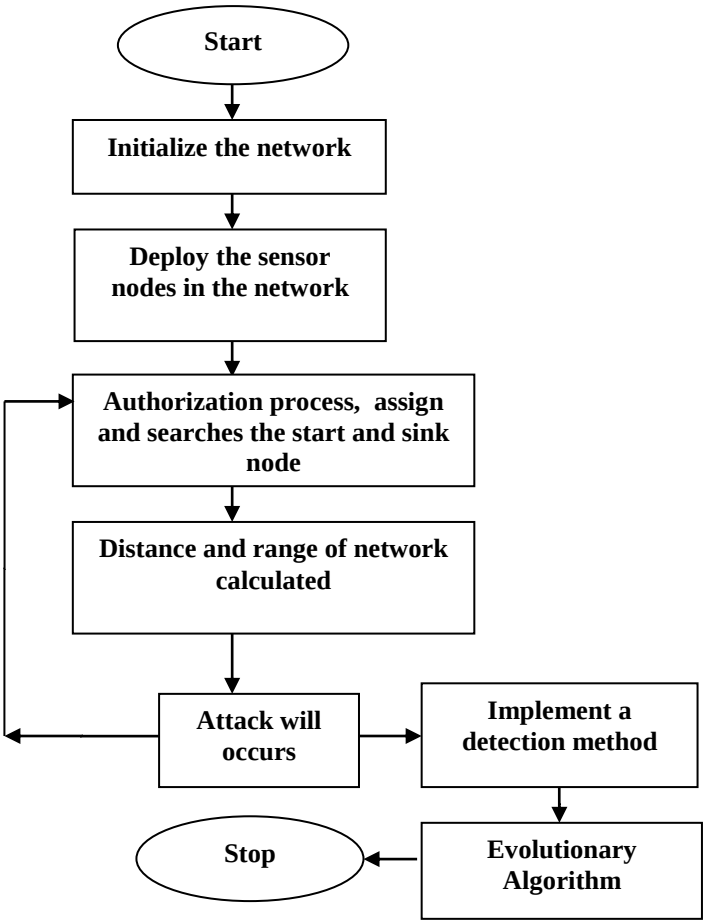


Fig 1. Proposed Work Flow Chart

GA is important when:

- Need of searching in extreme complex areas.
- Calculation free examination.
- Complex and approximately coupled issues that work with claim rules.
- The existing pursuit methods fizzle.
- Revealing of Domain Knowledge to encode decreased space.

Genetic calculation is the techniques of common advancement in organizing to measure the multilayered nature and to demonstrate developmental frameworks.

## VI. SIMULATION RESULT AND DISCUSSIONS

The above figure shows the deployment of the nodes in the network. The area considered in 1000*1000 meters. The deployment of the nodes deals with the x locations and y location of the nodes. The message box defined that the cluster head assign according to the number of mobile nodes in the network. The calculate the source node and sink node in the mobile area networks. Coverage set means information travelling source to sink node in the network and calculate the coverage distance and range of data transmission.

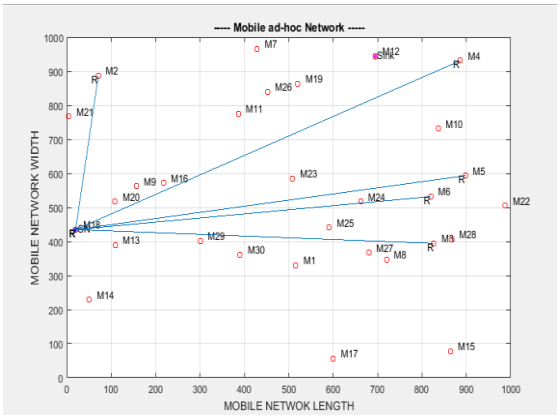


Fig 2. Mobile ad ho network (req sent)

The above graph defined that the source node sent the request and signal broadcasting. Source sent the request to the nearest and reply node which is free in the network. It defined that the route in the network which is present and received the request in the Mobile Adhoc Networks.

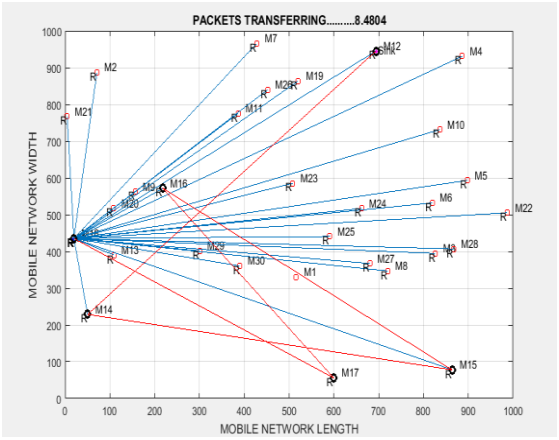


Fig 3 Final route, creating and Packet Transferring

The figure shows that the route searching in the various root cause of the best route calculated to less energy consumed and time consumed at the network. The highest data transmission and improve the performance in the network. The message box defines that the tunnel nodes to attack, according to the nodes that are consuming the high energy and time which means packet has been loosed in the network.

In this section, comparison described in the various routing schemes AODV, DSR, ZRP and Evolutionary (Proposed Methods).

**Table 1: Comparison – Throughput (%)**

| Number of Attackers | Evolutionary Algorithm | Existing Algorithms | | |
|---|---|---|---|---|
| | | AODV | DSR | ZRP |
| 1 | 80% | 40% | 60% | 70% |
| 2 | 79% | 42% | 62% | 72% |
| 3 | 81% | 43.4% | 63% | 74% |

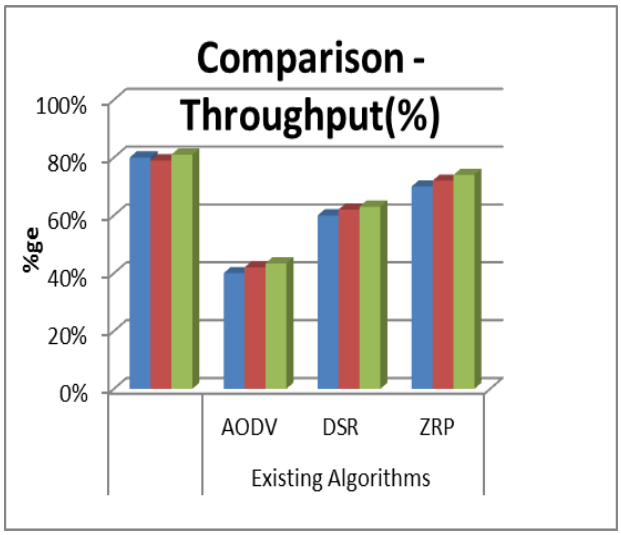


Fig 4. Comparison between Proposed and Existing Work (Throughput)

The above figure defined that the packet delivery rate Hybrid and Evolutionary Algorithm, and Existing work. We represent the performance of the network, accurate according to nodes. We improve the performance according to the routing protocol DSR and DSDV with Evolutionary Algorithm approach. Hence, we improve the performance parameters w.r.t Existing ones.

**Table 2: Comparison – PDR (Packet Delivery Rate) (%)**

| Number of Attackers | Evolutionary Algorithm | Existing Algorithms | | |
|---|---|---|---|---|
| | | AODV | DSR | ZRP |
| 1 | 3000 | 440 | 450 | 600 |
| 2 | 3400 | 432 | 445 | 657 |
| 3 | 3567 | 546 | 567 | 765 |

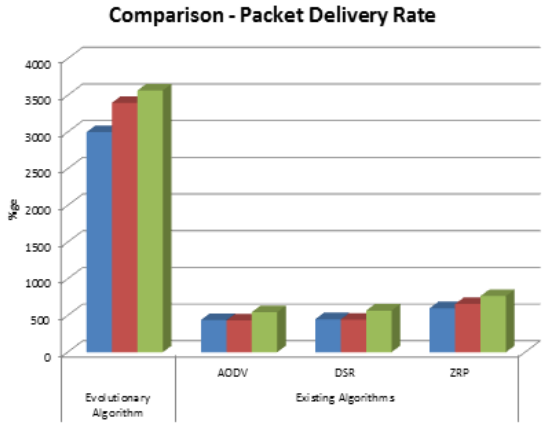


Fig 5. Comparison between proposed and existing work (PDR)

The above figure defined that the packet delivery rate, Hybrid and Evolutionary Algorithm and Existing work. We represent the performance of the packet delivery according to nodes. We improve the performance according to the routing protocol DSR and DSDV with Evolutionary approach. Hence, we improve the performance parameters w.r.t Existing ones.

**Table 3: Comparison – PL (Packet Loss) (%)**

| Number of Attackers | Evolutionary Algorithm | Existing Algorithms | | |
|---|---|---|---|---|
| | | AODV | DSR | ZRP |
| 1 | 30 | 49 | 48 | 40 |
| 2 | 29 | 50 | 52 | 39 |
| 3 | 27 | 53 | 54 | 35 |

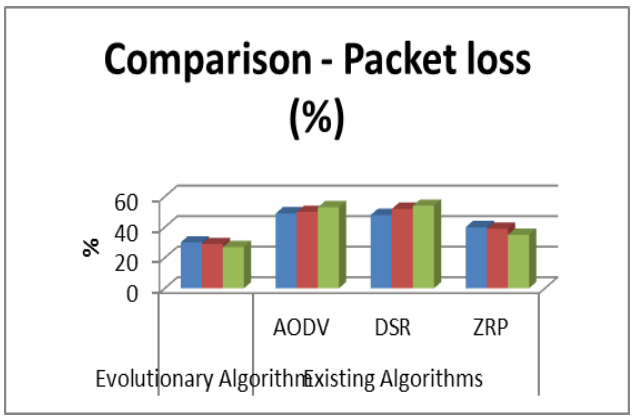


Fig 6. Comparison between proposed and existing work (PL)

The above figure defined that the comparison between the packet Losses performance parameters with existing and proposed work. We improve the performance of the packet Losses with decreasing the losses in the packer with Hybrid and Evolutionary Algorithm.

**Table 4: Comparison – PL (E2E delay ) (ms)**

| Number of Attackers | Evolutionary Algorithm | Existing Algorithms | | |
|---|---|---|---|---|
| | | AODV | DSR | ZRP |
| 1 | 0.05 | 0.09 | 0.02 | 0.34 |
| 2 | 0.02 | 0.1 | 0.01 | 0.4 |
| 3 | 0.01 | 0.4 | 0.4 | 0.56 |

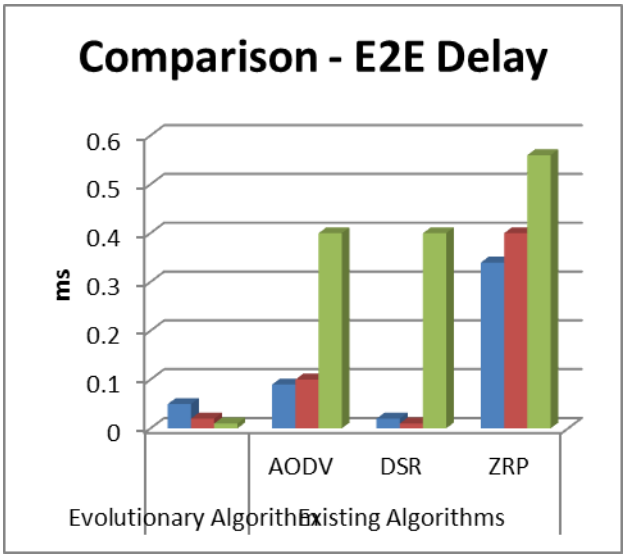


Fig 7. Comparison between Proposed and existing work (E2E delay)

The below figure defined that the performance according to the time. We improve the delay performance parameters w.r.t Existing Work. We use Hybrid (DSR and DSDV) protocol approach.

## VII. CONCLUSION AND FUTURE SCOPE

The performance of various routing schemes depends up-on numerous factors such as a number of senders, receivers and attacker nodes. MATLAB simulation Tool uses accurate and correct values which could be utilized for comparison various routing schemes. After that the reviewing all the above graphs, it could be accurately calculated that the performance of HYBRID and EVOLUTIONARY algorithm is more efficient by the wormhole in terms of PDR, E2E delay, PL and Throughput etc. In this attack, a malicious node advertises that it has the best path to the destination node during the route discovery process. Whenever it receives the RREQ message, it immediately sends out a fake RREP to the source node. The

source node first receives the RREP from the malicious node ahead of other RREPs. However, when the source node starts sending the data packet to the destination by using this route, the malicious node drops all packets instead of forwarding. The routing method studied, selective use of arbitrary waypoint versatility display for regressions in spite of a few specialists distinguishing confinements with this way to deal with testing. The accumulations of measurements from reproductions are another region which was featured in a few of the surveyed papers, scientists center upon unmistakable metric gathering yet avoid accumulation of center measurements, for example, organize throughput or defer which are fundamental for understanding the execution of a convention. This is additionally valid on account of reproductions which perform testing of conventions in disengagement; this lessens the appropriate estimation of the outcomes since they can't be specifically contrasted with accessible options. Whereas the proposed optimization algorithm exhibits more average E2E delay and AODV and DSR routing schemes demonstrates more Delay. The results of this research work, clarify that if various attacker nodes are present in the mobile network then the performance of the routing protocols de-grades.

In the future work, they will reproduce and correlation of various steering conventions can be performed under various kinds of wormhole assaults. In view of the above recreation brings about a protected wormhole identification and anticipation system can be produced which will enhance the execution AODV as far as Bundle Conveyance Proportion, Throughput, and Losses in the packet forms.

## REFERENCES

[1] Kumar, M., & Mishra, R. (2012). An overview of MANET: history, challenges and applications. Indian Journal of Computer Science and Engineering (IJCSE), 3(1), 121-125.

[2] Yang, Bo, Ryo Yamamoto, and Yoshiaki Tanaka. "Historical evidence based trust management strategy against black hole attacks in MANET." Advanced Communication Technology (ICACT), 2012 14th International Conference on. IEEE, 2012.

[3] Tan, Seryvuth, and Keecheon Kim. "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs." ICT Convergence (ICTC), 2013 International Conference on. IEEE, 2013.

[4] Dave, Dhaval, and Pranav Dave. "An effective Black hole attack detection mechanism using Permutation Based Acknowledgement in MANET."Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE, 2014.

[5] Sarkar, Manasi, and Debdutta Barman Roy. "Prevention of sleep deprivation attacks using clustering." Electronics Computer Technology (ICECT), 2011 3rd International Conference on. Vol. 5. IEEE, 2011.

[6] Alikhany, Meysam, and Mahdi Abadi. "A dynamic clustering-based approach for anomaly detection in AODV-based MANETs." Computer Networks and Distributed Systems (CNDS), 2011 International Symposium on. IEEE, 2011.

[7] Pandey, M. A. (2015). Introduction to Mobile Ad Hoc Network. International Journal of Scientific and Research Publications, 5(5).

[8] Kumar, S., & Kumar, J. (2012). Comparative analysis of proactive and reactive routing protocols in mobile ad-hoc networks (Manet). Journal of Information and Operations Management, 3(1), 92.

[9] Kaur, P., Kaur, D., &Mahajan, R. (2017). Simulation Based Comparative Study of Routing Protocols Under Wormhole Attack in Manet. Wireless Personal Communications, 96(1), 47-63.

[10] Liu, X., Li, Z., Yang, P., & Dong, Y. (2017). Information-centric mobile ad hoc networks and content routing: a survey. Ad Hoc Networks, 58, 255-268.

[11] Conti, M., & Giordano, S. (2014). Mobile ad hoc networking: milestones, challenges, and new research directions. IEEE Communications Magazine, 52(1), 85-96.

[12] Lo, N. W., & Liu, F. L. (2013). A secure routing protocol to prevent cooperative black hole attack in MANET. In Intelligent technologies and engineering systems (pp. 59-65). Springer, New York, NY.

[13] Haque, M. M., Shohag, M. S. A., Yasin, A. S. M., & Anwar, S. B. Mobile Ad-Hoc Network Security: An Overview.

[14] Dhenakaran, D. S., & Parvathavarthini, A. (2013). An overview of routing protocols in mobile ad-hoc network. International Journal of Advanced Research in Computer Science and Software Engineering, 3(2).

[15] Tan, Seryvuth, and Keecheon Kim. "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs." ICT Convergence (ICTC), 2013 International Conference on. IEEE, 2013.

[16] Datey, S. G., & Ansari, T. (2015). Mobile Ad Hoc networks its advantages and challenges. International Journal of Electrical and Electronics Research, 3(2), 491-496.