Detection and Prevention of Sybil attack In DSDV Based MANET Using BFO Algorithm

Mrs. S. Swathi[1], Dr. R. Vadivel[2]
[1,2] *Department of Information Technology Bharathiar University, Coimbatore, Tamil Nadu, India*

Abstract **- MANET could be a sort of remote ad-hoc organization. It may be a self-designing framework of portable switches related to remote associations with no access point. Each portable device in a framework is self-sufficient. The portable devices are permitted to move heedlessly and sort out themselves self-assertively. Ad-hoc systems do not depend on any fixed system. Each node is liable for directing the message from one node to the following like a switch, which causes organize more defenseless against the different attacks. One of the hurtful attacks is the Sybil attack in which a node misguidedly states different characters. In this circumstance, the real node offers data to the malicious node, and the data is lost. With the objective that it gets imperative to create beyond any doubt almost the framework from this kind of attack. The Bacteria Foraging is a developmental calculation that estimates fetched work after each iterative development of the program as the program execution proceeds and prompts consistently way better wellness (less fetched work). The boundaries to be improved talk to encourages (position) of the bacteria. This paper proposed recognizes and avoids Sybil attack and comparison of AODV and DSDV directing protocols and the results are simulated in ns2.**

Index Terms **- BFO, DSDV, MANET, Sybil Attack.**

I.INTRODUCTION

A Mobile ad-hoc network may be a collection of remote portable that should shape a transitory organization without the assistance of any setup foundation or centralized organization. In such an environment, it may be basic for one convenient have to select the help of other has in sending a packet to its goal, due to the limited run of each convenient host's farther transmissions. Much exertion has gone into a versatile ad-hoc network (MANET) ask almost over the past decade. Be that as it may, in fact, these days, portable ad-hoc organizing is seen as a for the most part modern zone or ask approximately. The reason for this will be taken after the reality that the improvement in truly understanding these frameworks is still alarmingly low and the genuine sending of these frameworks unprecedented [1]. An ad-hoc or short-lived organize is the network of two or more versatile gadgets related to each other without the help of setting up a system that separates to a settled inaccessible organize, an ad-hoc arrangement can be passed on in inaccessible geological regions and requires the slightest setup time and organization costs. In expansion, the integration of an ad-hoc organization with a more prominent organization-such as the Web or a farther system organize increases the scope extend, and application space of the ad-hoc organization. Portable ad-hoc sensor systems are uncommonly valuable in totally diverse scenarios. These frameworks advance operational MANETs are a kind of inaccessible ad-hoc framework that as a run the show contains a routable organizing environment on the beat of an Interface Layer advertisement to organize [2]. The enhancement of tablets and 802.11/Wi-Fi further organizing has made MANETs a well-known inquire about point since the mid-1990s.

Numerous scholarly papers evaluate conventions and their capacities, tolerating changing degrees of portability interior a bounded space, more frequently than not with all hubs interior numerous bounces of each other. Diverse traditions are at that point evaluated based on degree such as the allocated drop rate [3], the overhead displayed by the coordinating tradition, end-to-end allocate delays, organize throughput, etc. Inaccessible Frameworks are being anticipated utilized for watching and controlling the physical environment. They have been broadly utilized in region checking, normal checking, smart household building, and military applications among various others. Distinctive sensitive computing

methods are utilized, by and by days to unwind the issue of optimization in a given specialized circumstance. In remote and ad-hoc arrange situations prepared to additionally utilize the optimization methodologies like Particle Swarm Optimization (PSO), Genetic Calculation (G.A.), and Artificial Bee Colony Optimization (ABCO), etc can be utilized to optimize the course [4], sensor as well as hub zone, through-put & Transmission capacity as well as control utilization. Characteristic assurance tends to arrange of animals with dejected "foraging strategies" (strategies for finding, managing with, and ingesting nourishment) and bolster the engendering of qualities of those animals that have fruitful scrounging strategies are more likely to appreciate regenerative triumph (they get sufficient nourishment to enable them to duplicate.

II.RELATED WORK

Vasudeva, Amol, et al An exchange of messages over a wireless communication channel is the only available method for each node in a WANET to identify its neighbors A malevolent node can misuse this property by sending messages with different fake characters to control a considerable parcel of such a network. This type of attack is known as a Sybil attack [5]; it can occur in distributed systems operating without a central authority Sybil attack in which malicious node M joins the network and then introduces four virtual identities that force the legitimate nodes to incorrectly perceive that four new nodes have joined the network. These numerous personalities of a malicious node are called Sybil nodes or Sybil identities.

Khanna, Nitin et al Black hole attack is a very destructive packet drop attack in which the malicious node on receiving an RREQ packet replies with a fake RREP packet that contains a small hop count and a destination sequence number, making the source believes that the RREP packet sent by attacking node is genuine and that node really has the most optimal path to that particular destination indeed in spite of the fact that attacking node [6] has no route to that goal. When the source node actually transmits a data packet through that black hole node, the black hole node drops that packet and does not forward it further.

Khan, Khalid, et al. interruption location and its procedures in ad hoc networks. All of these surveys gave greater detail about intrusion detection and its techniques. Be that as it may, they failed to deliver all in one information. Comparing the survey with the considered ad hoc networks (both MANETs and WSN), while the survey only considered WSN. In overview a brief description of almost remote ad hoc systems, their sorts, and challenges confronted. Ad-hoc organize security challenges, security necessities, and conceivable attacks at the side of their sorts. Within the same study, high-lighted the attacks at different layers of the ad hoc organization with a brief presentation. After that interruption location framework.

III.SYBIL ATTACK

Sybil attack was, to begin with, presented by J. R. Douceur. Concurring to Douceur, the Sybil attack is an attack by which a single substance can control a significant division of the framework by showing numerous characters. The Sybil attack can happen in a distributed framework [7] that works without a central specialist to verify the identities of each communicating substance. In a Mobile Ad hoc Organize, as it were way for a substance to identify the presence of other entities is by sending and getting the messages over a shared broadcast communication channel. By taking advantage of this include, a malicious node can send messages with different fake personalities. The node spoofing the characters of the center points is called malicious node/Sybil attacker, and the centers whose characters are spoofed are called Sybil nodes [8]. Fig.1 represents a malicious node S at the side of its four Sybil nodes (S1, S2, S3, and S4). In case this malicious hub communicates with any legitimate node by displaying all its characters [9], the legitimate node will have an illusion that it has communicated with five diverse nodes. But in reality, there exists only one physical hub with different diverse IDs. In case a single malicious hub can convince its neighbors by showing different characters, it'll have control over the substantial parcel of the organization and can adversely influence the working of the network. According to Newsome, the instruments that are influenced by the Sybil attack are Information Aggregation, Reasonable Resource Allocation, Voting and Misbehavior Detection, etc. Karlof and Wagner have appeared in that Sybil attack

can moreover disrupt the working of certain directing conventions in MANETs such as multi-path routing protocols [10] and geographic-based steering conventions.

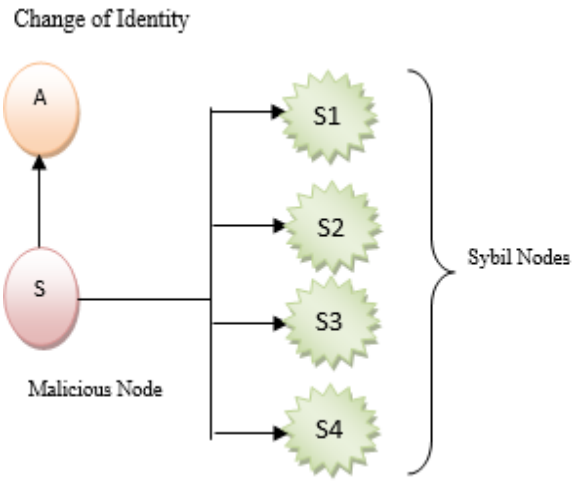

Fig.1 A Sybil Attacker with Multiple IDs

IV.PROTOCOLS OF MANET

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

Ad hoc On-demand Distance Vector Routing (AODV) protocol is an on-request directing convention because it determines a course to the goal as it were when a node needs to send data to that destination. The source broadcasts a course request (RREQ) packet when it needs to discover a way to the destination [11]. The neighbors, in turn, broadcast the packet to their neighbors until it comes to a middle node that has later route information approximately the destination or until it comes to the destination. An already gotten route ask packet is discarded by the nodes. The route request packet uses sequence numbers to guarantee that the courses are circle-free and that the middle node answers to course demands are the most later. A node records the node from which the request packet received, to begin with, to develop the inverted way for route reply to the source node [12]. As the course answer parcel navigates back to the source, the hubs along the way enter the forward route into their tables. Due to the portable nature of nodes, route maintenance is required. In case the source moves at that point it can reinitiate course revelation to the goal. If one of the intermediate nodes moves at that point the moved hub's neighbor realizes the connect disappointment and sends a connect disappointment notice to its upstream neighbors and so on until it comes to the source upon which the source can reinitiate course revelation if needed. AODV has incredibly diminished the number of routing messages within the organization [13]. AODV, as it were, underpins one course for each goal. This causes a node to reinitiate a route request inquiry when it's as it were course breaks. But in the case of mobility increases course demands moreover increments.

B. Destination Sequenced Distance Vector (DSDV)

This protocol is based on the classical Bellman-Ford routing algorithm planned for MANETS. Each node keeps up a list of all destinations and the number of hops to each destination. Each section is checked with an arrangement number [14]. It employments full dump or incremental upgrade to diminish arrange traffic generated by route upgrades. The broadcast of route upgrades is delayed by settling time. The only advancement made here is an avoidance of directing circles in a portable arrangement of routers. With this advancement, steering data is always available, in any case, whether the source node requires the information or not. With the expansion of arrangement numbers, routes for the same destination are chosen based on the following rules:

a. A route with a newer grouping number is preferred.
b. Within the case that two routes have the same sequence number, the one with distant better; a much better; a higher; a stronger; an improve stronger taken a toll metric is preferred.

Table.1 Routing Table

Destination	Next Hop	No. of Hops	Sequence no	Install Time

The above table.1 shows the list which is kept up is called the routing table. The routing table contains the following: The arrangement number is utilized to recognize stale courses from new ones and in this way it maintains a strategic distance from the arrangement of circles. The stations occasionally transmit their steering tables to their immediate neighbors [15]. A station in addition transmits its controlling table in the event that a basic change has happened in its table from the final overhaul sent. So, the upgrade is both time-driven and event-driven. Each push of the upgrade send is of the taking after form: grouping

number, Jump count. After accepting an update neighboring node utilizes it to compute the directing table sections.

V.PROPOSED WORK

Bacteria foraging optimization algorithms can be a well-known computational procedure that is base on the think almost of the bacterial foraging behaviors. the complex but organized exercises shown in bacterial foraging designs could inspire an unused arrangement for optimization issues. The underlying component of the surviving bacteria, particularly Escherichia coli (E. coli) is a microscopic organism that is normally found in the lower digestive tract of warm-blooded life forms. Most E.coli strains are innocuous, however, some can cause genuine food poisoning .in a complex environment has been detailed by researchers within the region of natural sciences. Inspired by these phenomena, BFOA was created as an optimization algorithm by K.M. Passino in which the self – the flexibility of individuals within the bunches looking exercises has pulled in a great bargain of the interface. The classical bacterial foraging optimization systems include three-run rule components specifically chemotaxis, generation, and elimination and dispersal.

A. Steps of bacterial Foraging Optimization Algorithm

There are following three steps in the Bacterial Foraging Algorithm after the look procedures like swimming and tumbling. They are:

1. Chemotaxis
2. Reproduction
3. Elimination and Dispersal

1) Chemotaxis

This preparation simulates the movement of an E. n.coli (Escherichia coli) cell through swimming and tumbling utilizing flagella. Actually, an E. coli bacterium shifts in two different ways. It can swim for a while within the same course or it may tumble, and interchange between these two modes of operation for a complete lifetime. Assume (b, c, r,) speaks to bth bacterium at cth chemotactic, rth reproductive, and lth elimination–dispersal step. C(i) is the estimate of the step taken within the irregular heading indicated by the tumble (run-length unit).

2) Reproduction

In this stage measure of the populace will stay the same by the method: each of the more beneficial bacteria (those yielding higher esteem of the objective work) sexually part into two microscopic organisms and the slightest solid microbes inevitably pass on, which are at that point put within the same area.

3) Elimination and Dispersal

Impulsive changes within the neighborhood environment where a bacterium populace lives may happen due to different reasons e.g. a critical rise in temperature may kill a bunch of microscopic organisms that are as of now in a locale with a tall center of supplement angles. Occasions can take put in such a way that all the microbes in a locale are slaughtered or a bunch is scattered into an unused area. To recreate this wonder in BFOA a few microscopic organisms are liquidated at subjective with a little likelihood whereas the unused substitutions are arbitrarily initialized over the look space.

This procedure comprises of three-phase to identify and prevent Sybil attack in MANET.

Phase 1: Network Construction phase

1. Create a network consisting of 50 nodes.
2. Select the source and the destination node.
3. The transmission will begin from source to destination by multi-hop.

Phase 2: Detection of attack

1. The Sybil attack is detected in the network by the chemotactic movement of data in the network.
2. The node that is not transmitting the data forward is the Sybil node.

Phase 3: Recovery

1. In the elimination mode of BFOA, eliminate the Sybil node.
2. Within the dispersion and propagation phase, a node is created that's the replacement of the Sybil node.
3. Analyze the P.D.R, throughput, and routing overhead.

Below Fig.2 shows the flowchart of the BFO process.

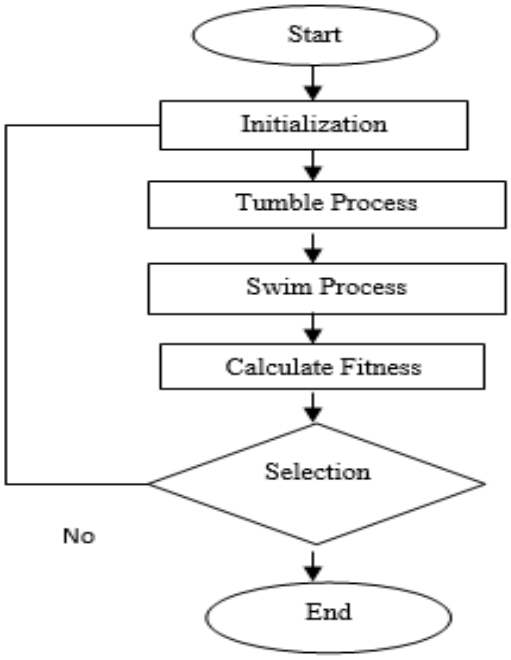

Fig.2 .Flowchart of BFO

VI.PERFORMANCE METRICS

This paper worked on Packet Delivery Ratio, overhead, and throughput as the performance metric to evaluate and analyze the performance of AODV and DSDV routing protocol. Below table.2 and fig.2 showing the performance metrics of routing protocols.

Table 2: Comparisons of Performance Metrics

Protocol	Generated Packet is (Seconds)	Received Packets (Seconds)	Packet Delivery Ratio	Routing Overhead
Aodv	11463	11346	98.984	0.10011
Dsdv	10265	9578	94.295	0.0884306

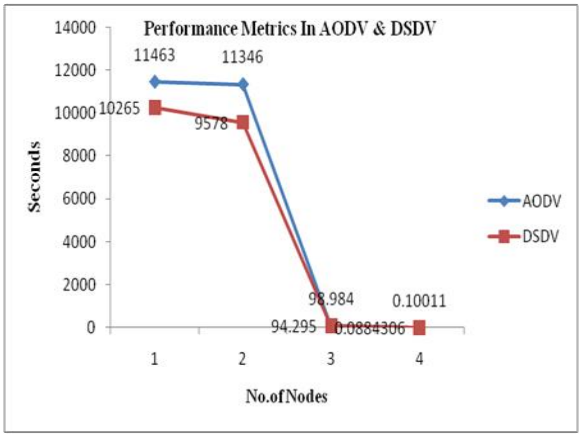

Fig .3 Performance Metrics in AODV & DSDV

VII.PERFORMANCE EVALUATIONS

The proposed BFO technique is implemented in NS2.35. The proposed work was compared with DSDV in different performance metrics. The simulation network consists of 50 nodes that are randomly deployed in 800m*600m. The simulation time is 100 seconds. The random waypoint mobility model was adapted, and the nodes move randomly in the deployment area at a speed between 40m/s to 20m/s. After moving to an arbitrary target position, there's a delay time sometime recently the hub begins an unused development. In case the stop time is set to 10, the hubs move ceaselessly; and in the event that the delay time is break even with the simulation time, meaning the hubs will stay at rest. The main parameters of the simulation are below shown in table 3.

Table 3. Simulation Parameter

PARAMETERS	VALUES
Area of Simulation	800m*600m
Mobile Nodes	50
Transferring Mode	Unicast through unipath
Maximum Speed	40ms
Minimum Speed	20ms
Routing Protocol	DSDV
Transport Layer	TCP, UDP
Traffic Type	CBR
Application Layer	FTP
Packet size	512 byte
Number of Sybil Identities	20
Start time	1.0s
Pause time	10s
MAC	MAC 802.11
Simulation Time (sec)	100

VIII.RESULTS AND IMPLEMENTATION

A. Packet Delivery Ratio

The ratio of the number of data packets delivered data to the destination. This describes the level of delivered data to the destination. A Number of packets receive/number of packets sent. The value of the packet delivery ratio implies the superior execution of the protocol. The below figure. 4 shows the packet delivery ratio using BFO.

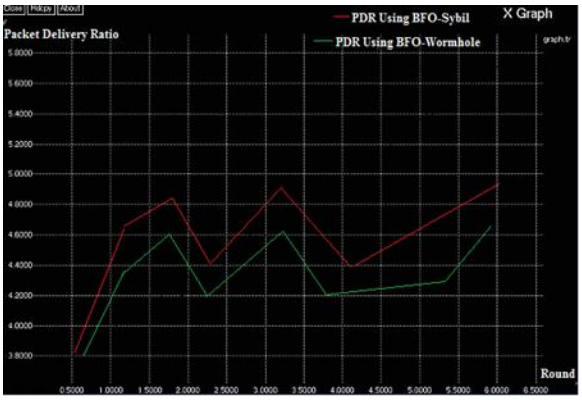

Fig 4: Packet Delivery Ratio Using BFO

B. Overhead

Another parameter of execution is overhead. The whole number of routing packets transmitted during the recreation tests. One transmission is number when a packet sent over different hops, of the organize, is characterized as the outside degree of adequacy, productivity is considered to be the inside degree to attain a given level of information directing execution, information routing execution may or may not be influenced by convention inside efficiency, In case the same channel is shared control activity and information activity and channel capacity is restricted, at that point excessive control activity frequently impacts information routing execution. Overhead of DSDV which is much less than AODV protocol overhead. The least overhead is appeared by DSDV protocol and the most extreme is appeared by AODV protocol. In this chart, overhead among the two protocols appeared below the figure. 5 represents the routing overhead using BFO.

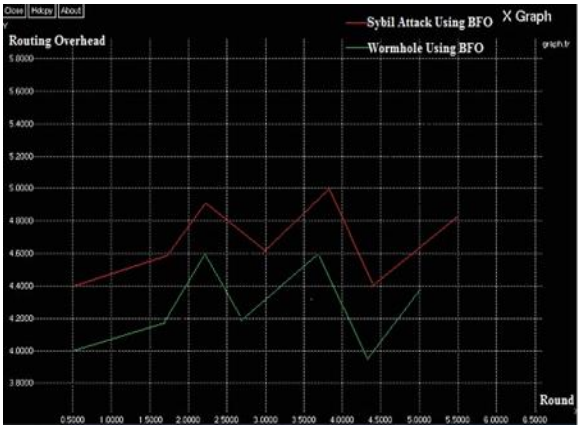

Fig.5 Routing Overhead Using BFO

C. Throughput

It is defined as the total number of packets over the total simulation time. The throughput comparison of AODV, DSDV. This Shows that which one is better than overhead is better for the performance of the protocol. Below figure. 6 showing the throughput after compensation using Sybil attack and BFO.

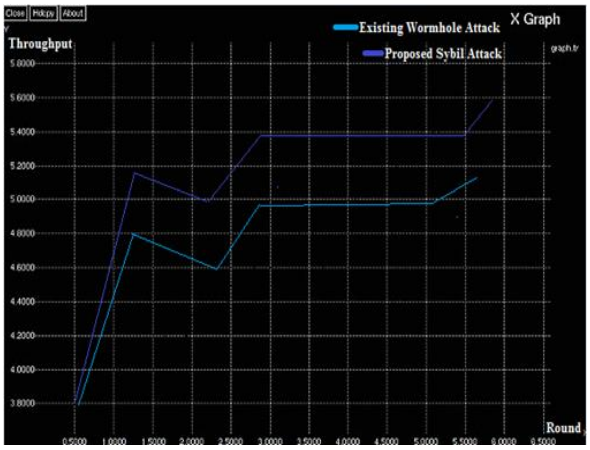

Fig .6 Throughput after Compensation Using Sybil attack and BFO

IX.CONCLUSION AND FUTURE SCOPE

This paper examines the execution of the BFOA procedure in MANETs The node's developments are like microscopic organisms development. The technique is applied for detection and prevention from the Sybil attack. By applying this technique to MANETs get better results than Existing MANETs attacks. The Sybil attack on different routing protocols such as proactive and reactive protocols in the MANETs, the attack becomes very difficult to detect and more destructive if the malicious node introduces its fake identities (Sybil nodes) by varying the transmission power, a malicious node may claim to have more number of neighbors by presenting multiple Sybil nodes. This improves performance in terms of packet delivery ratio, overhead, and throughput. In the future, BFOA will give medical information where a combination of microbes foraging and a case-based thinking framework can be utilized to analyze the patient's illnesses. This technique may also be applied in areas such as oceanographic astronomical observations and may also apply for solving a broad class of engineering design, software testing, and scientific problems and will prove to be a general-purpose powerful heuristic method for solving a wider

class of such problems. In the future, artificial intelligence methods will moreover propose security.

REFERENCES

[1] Muchtar Farkhana, Abdullah Abdul Hanan, Hassan Suhaidi, Khader Ahamad Tajudin and Zamli Kamal Zuhairi, "Energy conservation of content routing through wireless broadcast control in NDN based MANET: A review", Journal of Network and Computer Applications, Vol.131, No.109-132, Apr 2019.

[2] Ajay Kumar Yadav , Santosh Kumar Das and Sachin Tripathi, "EFMMRP: Design of efficient fuzzy based multi-constraint multicast routing protocol for wireless ad-hoc network" Computer Networks, Vol.118, No. 15-23, May 2017.

[3] Piyush yadav, Rajeev Agrawal and komal kashish, "Performance Evaluation of ad-hoc Wireless Local Area Network in Telemedicine Applications," 6th International Conference on Smart Computing and Communications, Vol. 125, No. 267-274, 2018.

[4] Dipika Sarkar, Swagata Choudhury and Abhishek Majumder, "Enhanced-Ant-AODV for Optimal Route Selection in Mobile Ad-Hoc Network," Journal of King Saud University-Computer and Information Science, Aug 2018.

[5] Vasudeva, Amol, and Manu Sood. "Survey on sybil attack defense mechanisms in wireless ad hoc networks." Journal of Network and Computer Applications, Vol. 120, No. 78-118, Oct 2018.

[6] Khanna N, and Sachdeva M. "A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs". Computer Science Review,Vol.32, No. 24-44, May 2019.

[7] Priya Jain and Rashmi Nigoti, "A Novel Technique for Sybil Attack Detection and Prevention in MANET," International Journal of Computer Applications, Vol. 150, No. 9, Nov 2015.

[8] Sonam Mahajan, Nidhi Dahiya and Devesh Kumar, "A Mechanism of preventing Sybil Attack in MANET using Bacterial Foraging Optimization", Thirteenth International Conference on Wireless and Optical Communications Networks", 2016.

[9] Nitin khanna and Monika Sachdeva, "A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs," Computer Science Review, Vol. 32, No. 24-44, May 2019.

[10] Sacha Trifunovic and Andreea Hossmann-Picu, "Stalk and lie—The cost of Sybil attacks in opportunistic networks," Computer Communications, Vol. 73, No. 66-79, Jan 2016.

[11] G. Jose Moses, D. Sunil Kumar, P. Suresh Varma and N. Supriya, "A Simulation Based Study of AODV, DSR, DSDV Routing Protocols in MANET Using NS-2," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Iss. 3, Mar 2012.

[12] Puneet Kaur and Navdeep Kaur, "A Survey of Black Hole Attack In AODV," International Journal of Advanced Computronics and Management Studies," Vol.1, Iss. 2, No. 11-15, Mar 2016.

[13] Chavan, D. S. Kurule and P. U. Dere, "7th International Conference on Communication, Computing and Virtualization," Vol. 79, No. 835-844, Jan 2016.

[14] Abeer Ghander and Eman Shaaban, "Power Aware Cooperation Enforcement MANET Routing Protocols," Procedia Computer Science, Vol. 73, No. 162-171, Jan 2015.

[15] Saba Farheen, N.S and Jain. A, "Improved Routing in MANET with Optimized Multi path routing fine-tuned with Hybrid modeling," Journal of King Saud University - Computer and Information Sciences, Jan 2020.