International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Collaborative Black Hole Attack Detection in MANET

Shivani Gogia[1], Dr. Rashmi Popli[2]

[1]Research Scholar, J.C. Bose University of Science & Technology, YMCA Faridabad
[2]Assistant Professor, J.C. Bose University of Science & Technology, YMCA Faridabad

---

Abstract - *MANET is an association of connectionless mobile nodes which transmit data through wireless channels in the absence of stable infrastructure. Both genuine and malicious nodes can ingress the network. So MANET is predominantly liable to different attacks. The dropping of data packet while transmitting from source node towards destination node is one of the critical problems in MANET. There are many factors by which dropping of data packet is caused. The principal cause for data loss is black hole attack. In black hole attack, during process of route discovery malicious node publicizes itself as having the shortest way from source node towards destination node and then switches the information of data towards it and afterwards drops that data instead of sending it towards destination node. We have studied different algorithms for detection of attack. Now for overcoming limitations of previous detection strategies, we are proposing a new approach for detection of malicious nodes in any order and at any position in network. The work is carried on MATLAB. Our main aim is to ensure security against Black hole attack.*

Keywords: **MANET; AODV; Black Hole Attack; Firefly; Fuzzy SVM.**

1. INTRODUCTION

MANET is a type of multi-hop networks in which each node has a non-wired transceiver device. MANETs are utilized in the zone of military, disaster relief management, sensor networks, commercial sector, medical service, personal area network. Basically technology of Adhoc network is originated in communication of battlefield network and the technology is mainly applied in commands of military operations, communication network of tactical battlefield. Due to the flexibility of network, it is widely used and developed. In MANET, the routing protocols that are used for supporting the nodes connectivity are DSR (Dynamic Source Routing), DSDV (Destination Sequence Distance Vector) and AODV (Adhoc On-demand Distance Vector). AODV is also known as source initiated on-demand routing protocol. MANETs are helpless against different types of layer attacks. For the mechanism of the AODV routing protocol, most significant layers are Physical, MAC, and Network layer. Among these, the most important layer attack is network layer attack. Purposes of attack in network layer are: Not to forward the information of data packets, Changing & adding some parameters of routing messages. MANETs are mainly suitable for these areas. In these kinds of areas, communication between nodes with one another are open with no fixed foundation, so the network connectivity between the nodes are given by forwarding packets over themselves. Every node behaves itself as a router, and a correct and effective path is found to forward data packets towards the destination node. In AODV routing protocol, during the process of route discovery, intermediate nodes are dependable to discover a fresh and effective path towards the destination node. The process is not only used by fake nodes but apart from that, false information is immediately responded back towards the source node as though it has enough fresh paths towards destination node. Thus, data packets are sent towards destination node by source node via malicious node. Various sort of network layer attacks are – Black hole attack, worm hole attack, sink hole attack, gray hole attack etc. Black hole Attack is a significant attack.

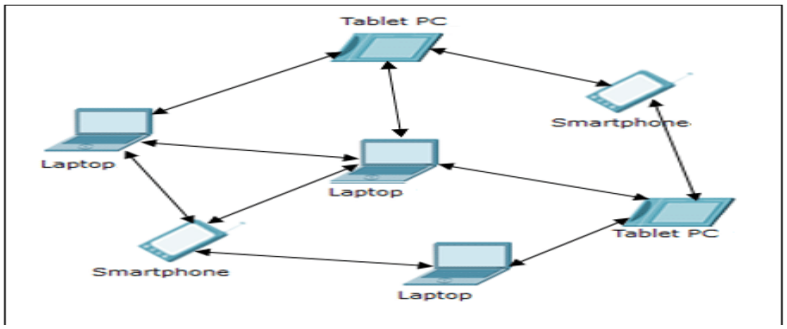


Fig-1: Communication phase of MANET.

At the point, when an attacker node receives Route Request message, it returns back Route Reply message to the source node with an extremely high destination sequence number to accept that the attacker node has the fresh path towards the

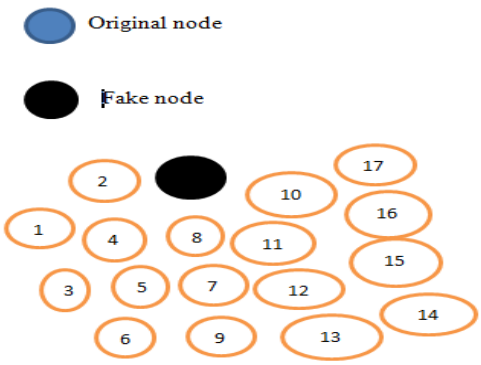
destination node. Among all of these, the source node will choose this malicious route towards the attacker node and eliminate other legitimate RREPs.

Security Problems in MANET:
• Open media
• Routing protocol don't have any security component
• Inaccessibility of central organizer.

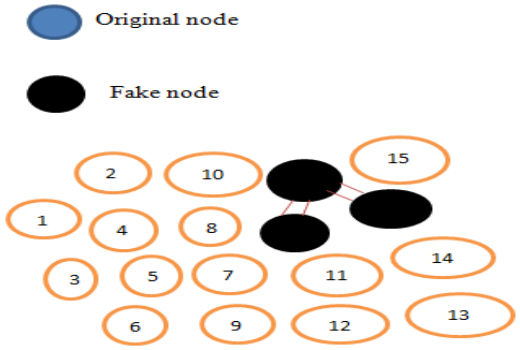
Security vulnerabilities of the routing protocols are most essential issue in MANET. Nodes in MANET might be compromised in such a way that it may not be conceivable to detect the malicious behaviour of nodes effectively. Now, to improve the performance of network in various manners, a mechanism is proposed which includes a procedure of choosing a subset in relevant features, known as subset selection and parameters optimization. The strategy works with AODV routing protocol. Now to optimize route that is to select best route among different routes, optimization algorithm named as firefly algorithm is used. After that, FSVM Fuzzy Support Vector Machine) is used to classify black hole attack in MANET.

2. BLACK HOLE ATTACK

On network's routing protocol, the manner in which each fake nodes utilizes the information of data so as to break the information into the network. In an AODV based network, RREP packets are created by malicious node a with a high sequence number in response to RREQ packets. Thus, the way with fake node is picked as the freshest way by the source node. With respect to the number of fake nodes taking an interest in network, black hole can be examined in three types which are: Single, Cooperative and Distributed black hole. In single black hole, as showed in Figure 2(a), there is just one fake node in network; while, in cooperative black hole, as showed in Figure 2(b) there are more than one fake nodes that cooperatively work with one another so as to cover their tracks. In single black hole attack, all malicious nodes are in the wireless range of each other. In addition to this, now we characterized another kind of black hole attack, which is known as distributed black hole attack. In this type of attack, malicious nodes are conveyed and can be located in different locations in network. Every single malicious node knows about different malicious node's position and ID and work helpfully to cover their tracks. The quantity of malicious nodes in every area can be unique. Figure 2(c) is an example of distributed black hole attack.



a) Single



b) Cooperative

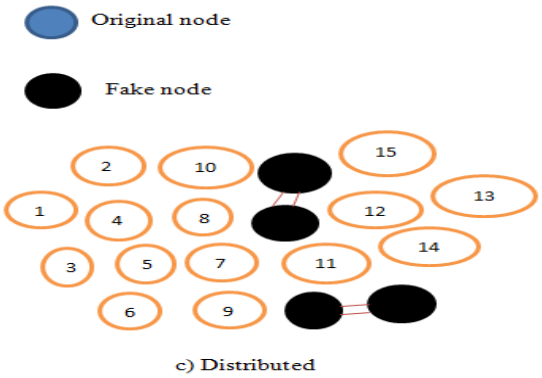


Fig-2: Black Hole Attack

ARCHITECTURE

The malicious node which participates in network management drops all the data of information packets which goes through it instead of sending them towards destination node. During route discovery process malicious node falsely publicizes great paths towards destination node such behaviour is known as black hole attack. The mitigation procedure is partitioned into following steps as shown in Fig 3.

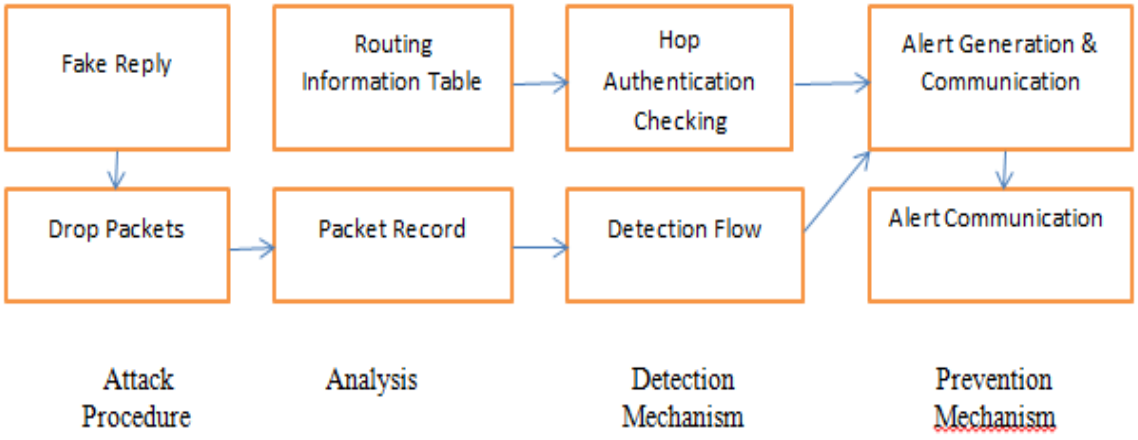


Fig-3: Mitigation Mechanism for Black Hole Attack

2.2 Detection Methods of Black Hole Attack

Black hole is nothing but the malicious node. This node acknowledges the data from source however doesn't forward it to the destination. This node is utilized for hacking purpose. There are two detection strategies involved in the detection of black hole:

- Depending upon how often that path is utilized for transmission.
- By updating the routing table and comparing unique sequence number at each time.

2.3 Solution for the Black Hole Attack on AODV Routing Protocol in MANET

By various ways, the Route reply (RREP) message that begins is checked first. Then without checking its routing table, RREP message is immediately send back by black hole node towards the source node. The first RREP consistently originates from black hole node. In this way, arrangement will dispose of the main Route Reply (RREP) packet utilizing the course that answers from malicious node and pick the second Route Reply (RREP) packet.

3. RELATED WORK

In this section, several solutions to black hole attacks are reviewed.

3.1 Sachin Malviya et al. proposed GA & SVM for protection of data security system from black hole attack. For optimization purpose Genetic Algorithm (GA) is utilized and for classification purpose Support Vector Machine (SVM) are utilized [1]. He suggested that the proposed strategy is utilized for detection of network attack more efficiently. In this paper, limitation was settled up for SVM Parameters and optimization by utilizing GA which gives optimal solution.

3.2 Houda Moudni et al. proposed PSO & ANFIS strategy is utilized for identification of attack.
ANFIS (Adaptive Neuro Fuzzy Inference System) – It is a methodology which incorporates fuzzy logic to neural network. ANFIS forecasts make it conceivable to reconstitute the future behaviour of attacker and in this manner to recognize it [9].
PSO (Particle Swarm Optimization) – PSO utilizes candidate solutions population to develop optimal solutions of given problem. PSO is also applied to improve the performance of ANFIS, by changing membership function and after that minimizing the error.
ANFIS – PSO Algorithm work together to detect Black Hole Attack – By creating a neighbour table, database is extracted from network. FPR & ADSN parameters are calculated from database. Mapping process is done by identifying normal & abnormal activities. I/O dataset is utilized for training of ANFIS. N*M matrix is created (include membership function parameters & consequent parameters). Now, Membership Function parameters & consequent parameters are optimized using PSO algorithm. Now, fitness function is defined as mean square error between measured & experimental data.

3.3 Kirandeep Kaur published a review paper for detection of black hole attack in MANET using techniques fuzzy logic and firefly algorithm [4]. Fuzzy Logic- It is based on three core concepts, namely, fuzzy sets, linguistic variables, and possibility distributions. The importance of fuzzy logic derives from the fact that most modes of human thinking and especially common sense reasoning are approximate in nature. Firefly Algorithm- The Firefly algorithm is encouraged by the social presentation of fireflies. Fireflies may also be called as lightning bugs. There are around 2000 firefly species in the globe. A large portion of firefly species build short and musical flashes. The model of flashes is one of a kind for specific species. A firefly's twinkle principally acts as a sign to attract mate partners and potential prey. Flashes likewise serve as a cautious warning instrument.

3.4 Amanpreet Kaur et al. proposed Firefly and ANN techniques to prevent network from black hole attack. He uses the concept of firefly to optimize best route and ANN for classification purpose [3]. The main focus of their study is to acquire proper routing and packet transmission functions since it is the reason for multi-hop connections between different nodes that are away from one another.

3.5 Ramanpreet Kaur et al proposed ANN modelling feedforward back propogation learning algorithm & Graphical user interface for detection of black hole attack in network. ANNs are one of the artificial intelligence techniques that can give a solid instrument to identifying malicious nodes in MANET [7]. High calculation rate, learning capacity through pattern introduction, expectation of unknown patterns and adaptability attacks the noisy patterns are the primary focal points of ANNs.

3.6 Meenashu Gupta et al. proposed a methodology for QOS Parameters improvisation by Detecting and Preventing attack utilizing Artificial Intelligent. In this paper, Cuckoo Search & ANN Algorithm has been proposed for elimination of Black Hole Attack [11].

Cuckoo search – It is a numerous nature-inspired algorithm utilized to take care of optimization problems in various fields of engineering. It is an extremely powerful in understanding worldwide enhancement since it can keep up balance among local and global random walks utilizing exchanging parameter.
Artificial Neuron Network (ANN) –ANN relies upon the structure and component parts of biological networks. The information of data impacts on the structure of ANN & additionally the neural network changes, it could be said in view of input and output.

The steps that are followed using the research work are described as – Create a simulation environment for MANET using height & width of 1000 * 1000m. Now, initialize N number of nodes within the network. Define coverage area of each node & define source and destination node. Route is discovered using AODV to find route between source and destination. Check network performance, if performance of network is degraded then initialize cuckoo search algorithm using objective function otherwise evaluate parameters and Optimize properties of nodes according to objective function. If properties of nodes are satisfactory then train them using ANN otherwise reject that property. Classify attacks present in

route. If node is real then create a new route and evaluate performance parameters like throughput, delay, BER. Otherwise consider an attack and remove from route.

3.7 Saurabh Kumar proposed a technique for Detection & Mitigation of Black Hole Attack in MANET using Artificial Intelligent Technique. In this paper, ABC (Artificial Bee Colony) & ANN (Artificial Neural Network) techniques have been proposed for detection of Black Hole Attack [12].

ABC –It relies upon the foraging behaviour of swarm of honey bee. It is utilized as an optimization algorithm. In this, primary portion of swarm of honey bee comprises of employed bees, and the onlooker bees are established by subsequent halves. The quantity of arrangements in the swarm is equivalent of the number of employed bees or the onlooker bees. This technique creates a randomly dispersed beginning population of SN arrangements (nourishment sources), where swarm size are indicated by SN. ABC works in four phases: - initialization phase, employed bee phase, onlooker bee phase, scout phase.
ANN –This model depends on the structure and elements of biological networks. It is utilized as a computational model for classification purpose. Information that moves through the system influences the structure of the ANN on the grounds that a neural network changes - or learns, it could be said - in view of input and output.

3.8 G.Vennila, Dr. D.Arivazhagan, N.Manickasankari, proposed a methodology for Prevention of attack in network on DSR protocol utilizing Cryptographic Algorithm. In this paper, one cryptographic algorithm RSA & sequence number calculation has been proposed to eliminate Black Hole Attack [13]. RSA is an algorithm utilized by modern PCs to encode and decode messages. It is an asymmetric cryptographic algorithm. Public key and private key are included by RSA. Public key could be known to everyone; it is utilized for encoding messages. Utilizing the public key messages are encoded, it then must be decoded with the private key. After getting the RREP in source, it figures out that the threshold_diff value in which the RREP originate from legitimate node or fake node. Based on the threshold_diff, it sends the packet from source to destination/goal. If the distinction of sequence value is below the threshold_value, then the node is considered as legitimate node Assume the difference of Sequence number is more prominent than the threshold_value, at that point the node is considered as fake node.

3.9 Ramanpreet Kaur et al. proposed a methodology for detection of attack in network utilizing Artificial Neural Network [7]. By utilizing a simulated MANET environment Artificial Neural Network methodology has been proposed for elimination of Black Hole Attack. For detection of attack demonstrating of ANN are examined and it is demonstrated that model can recognize nodes under attack effectively. ANNs are one of the artificial intelligence techniques that can give a solid instrument to identifying malicious nodes in MANETs. High calculation rate, learning capacity through pattern introduction, expectation of unknown patterns and adaptability attacks the noisy patterns are the primary focal points of ANNs.

To design the mechanism, following steps are taken:

- Black hole attack definition and parameters selection.
- MATLAB simulation
- Data Extraction
- ANNs Modelling
- Result Analysis

3.10 A Sharma, P.K. Johari et al. proposed a fuzzy Logic for elimination of attack in network [16]. Rather than fixed reasoning fuzzy logic manages with approximate strategy. Fuzzy factors may have a truth value that reaches in degree somewhere in the range of 0 and 1; stretched out to deal with the idea of incomplete truth where the truth value may extend between totally true or totally false. An immense number of complex issues might be tackle utilizing Fuzzy logic explicitly fuzzy modelling and optimization technique. Fuzzy modelling is the comprehension of the issue and investigation of the Fuzzy data where the Fuzzy enhancement understands Fuzzy model ideally utilizing optimization techniques by means of membership functions.

4. PROBLEM IDENTIFICATION OF THE EXISTING WORK

Due to attack, the main problem of the network is that the throughput and efficiency decreases and bandwidth of the network also decreases. And by this, the network efficiency decreases. No one single algorithm presents the maximum throughput and less wastage of bandwidth.

Paper No. Author & Year	Techniques used	Algorithm used	Function of Algorithm	Simulator used	Parameter Compared	Direction of Future Work
1.Houda Moudni Et al. [2019]	Fuzzy Based IDS	ANFIS & PSO	For detection & prevention of attack in Mobile Adhoc Network (MANET).	NS-2 & MATLAB.	Rate of detection & Rate of false alarm.	IDS are contracted and other IDS are proposed for attack detection and also plan for recognition of attacks that occur in MANET.
2.Meenashu Gupta et al.[2018]	Artificial Intelligent Techniques	Cuckoo Search is utilized for optimization purpose & ANN is utilized for classification purpose.	For detection& prevention of Black Hole Attack in network.	MATLAB	Throughput Delay, BER, Energy Consumption	1. Utilized for recognition and prevention of various attacks like gray-hole, warm hole. 2. Performance of network could be expanded by utilizing other optimization strategies like GA, ABC and classification strategies like fuzzy logic, SVM.
3.Saurabh Kumar et al.[2017]	Artificial Intelligent Techniques	ABC is utilized for optimization purpose & ANN is utilized for classification purpose.	For detection & mitigation of black hole attack.	MATLAB	Energy consumption, Throughput Delay , Packet Delivery Rate (PDR).	To Identify and prevent network from black hole attack and to expand accuracy of system the Classification of neural network can be utilized along with fuzzy logic, and ABC can be utilized for optimization purpose in hybridization with GA.
4.A. Sharma et al.[2017]	Utilize Fuzzy Logic Technique for elimination of attack from network.	Fuzzy Logic	1. Attacker node distinguishes during path discovery period of AODV protocol. 2.For Removal of black hole nodes from network.	NS-2	Packet delivery ratio (PDR), routing overhead & Throughput.	In future, extend to upgrade performance of network under gray-hole attack.

5.Rama-npreet Kaur et al[2014]	Artificial Neural Network	ANN modelling feedforward back propogation learning algorithm & Graphical user interface	For detection of black hole attack.	MATLAB	Throughput, Packet delivery ratio & end to end delay.	The classification algorithm i.e. ANN could be worked together with different methodologies like fuzzy logic & GA, for developing of mechanisms which can detect the attack with more ease , more speed & more efficiency,
6.G.Vennile et al.[2014]	Cryptographic Algorithm	RSA	Performance of MANET can be improved by utilizing secure DSR protocols.	MATLAB	Delay, Throughput	Proposed algorithm apply to other types of attacks such as worm hole, gray hole etc.
7. Sachin Malviya et al. [2016]	Intrusion Detection, Denial Of Service & Data Mining Techniques	G.A. & SVM	G.A for optimization & SVM for classification purpose.	MATLAB.	Packet Drop Rate (PDR).	These techniques can be utilized to detect more intrusive activity & also for making some action against intrusion.
8.Aman-preet Kaur et al. [2019]	Artificial Intelligent Techniques.	Firefly & ANN	Firefly for optimization & ANN for classification purposes.	MATLAB	Energy consumption, PDR & Delay	1. In future, these techniques are utilized for detection of other attacks such as worm hole, sybil attack. 2. Other techniques can be utilized for enhancing the proposed work. The techniques can be Ant Colony Optimization & G.A.
9. Kona-gala Pavani et al. [2014]	Intrusion detection system, Multi-layer perceptron	SVM & Decision tree	Decision tree & SVM is utilized for classification purpose.	NS2	Error Rate, Accuracy.	In future, these methodologies are utilized for detection of other network layer attacks such as worm hole, gray attack.

Table-1: Comparison of Different Techniques.

The impact of black hole nodes on literature review basis can be concluded as:

- The estimations of hop count and path optimality tend to decline linearly. As the level of nodes ranges to 100 percent the quality approaches zero.
- The estimations of reachability does not arrive at zero level even at 100% grouping of black hole nodes since at this fixation the communication still wins between neighbouring nodes. While designing any protocol for ad hoc network, all these results can be very useful for the protocol designers.

From the outcomes acquired it is seen that when the malicious node is present in the network:

- It definitely reduces the packet delivery to destination.
- The throughput of network diminishes definitely.
- There is decrement in end to end delay.

After the overcoming of black hole attack and proceeding of course is done [7], it is observed that:

- Than black hole attack, now the Packet delivery proportion is obviously better.
- Throughput of system increments and reaches to acceptable level.
- When contrasted to Normal system.

5. FLOW OF WORK

The complete execution of this project is given in the following steps:

Phase 1: Literature Review: All the previously proposed algorithms have been reviewed before the writing of this paper such that the authors get a good insight of the problems in the algorithms to get the work started.
Phase 2: Problem Identification: After reading the literature and making a review, the problem identification part can be carried out.
Phase 3: Design of the new technique: After this, the designing or the developing of new technique is done.
Phase 4: Implementation and Analysis: The implementation of the proposed technique is started and it can be analysed on grounds of certain parameters.

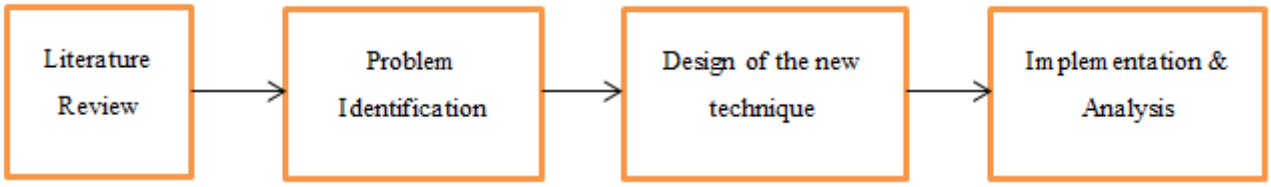


Fig-4: Flow of Work

6. PROBLEM STATEMENT

For security of network, it is essential to prevent the harm that could be caused by various sorts of attacks. The most common attack is known as black hole attack. This attack harms the network and its aim is to prevent network's connection [23]. Whenever the path is required by source node, utilize routing protocol i.e. AODV. This protocol is utilized to find out the shortest path from source node to destination node for data communication purpose in the network [6]. For detecting the network from black-hole attack, AODV routing protocol is not provided with an algorithm. For detection of attack and for prevention of its harm in the network efficiency, main aim is to upgrade the AODV routing protocol with a lightweight methodology. On the basis of restrictions of existing technique, proposed a new method for detection of attack adequately.

7. PROPOSED METHODOLOGY

On the basis of previous study it is claimed that no such schemes are available to strongly prevent the network from black hole attack. We introduce a strategy in which fuzzy SVM & Firefly strategies are utilized for detection of attack.

7.1 Proposed Solution

First source node sends a route request message to the adjoining nodes to locate the exact goal node. On receiving the reply from those nodes, source node extracts that data and checks the outcome which is obtained from them. If the outcome is correct, then it begins a path towards the destination node and sends the data. If the outcome is not correct, then an additional route towards all the neighbouring nodes is sent out just to examine whether a route from the intermediate node towards the destination node exists or not. At that time, an alarm message is sent out throughout the network. Thus, we evade this problem.

7.2 The proposed work model is divided in following areas: Route Discovery, Enhancement of route &Detection of attack.

A. Route Discovery

First we create node enviornment with various mobile nodes. Now source node needs to establish connection for transmitting data towards destination node. A source node sends the data packets towards the destination node by intermediate nodes. These intermediate nodes are called routers. If route is found out by source node towards destination node then source sends the data packets otherwise it sends the RREQ (Route Request) towards destination node for finding the path. If route is discovered then destination node sends back RREP (Route Reply) message to the source node which contains the node ID, Sequence number and other details. If these details are matched with the source node details then connection is established otherwise connection is lost.
In Fig 5, various routes are available from source to destination and we have to choose best route for the data transfer.

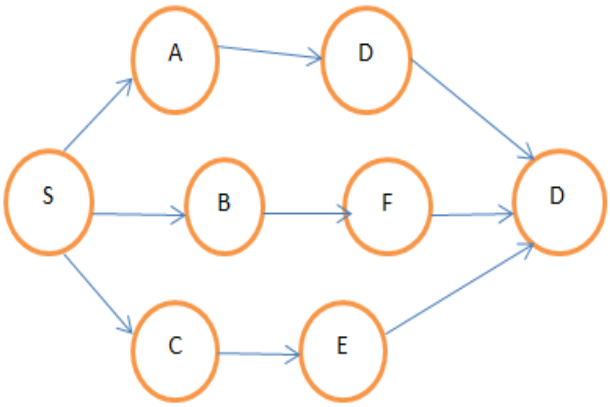


Fig-5: Route Discovery

The procedure of route discovery follows the AODV architecture and furthermore optimizes the route using Firefly algorithm.

B. Route Optimization

This section optimizes the route which has been previously discovered. The proposed architecture utilizes Firefly algorithm for route optimization [4].

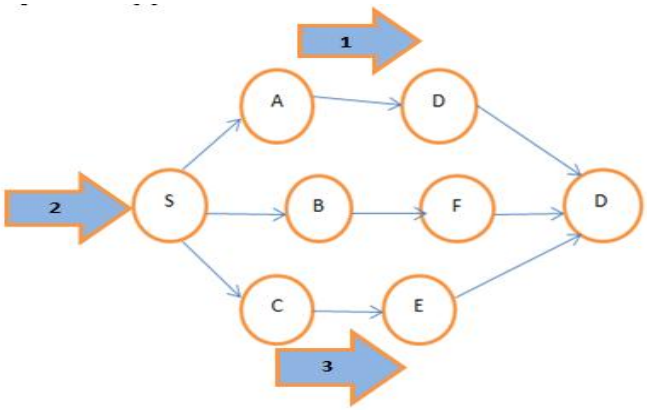


Fig-6: There are 3 routes from source to destination.

Considering above fig 6, there are 3 routes from source to destination. We have to select Best and Optimized route. Firefly helps in examining the behaviour of intermediate nodes utilizing their fitness function. By behaviour of nodes if fitness criteria of firefly are fulfilled, then it would be considered as black hole attack.

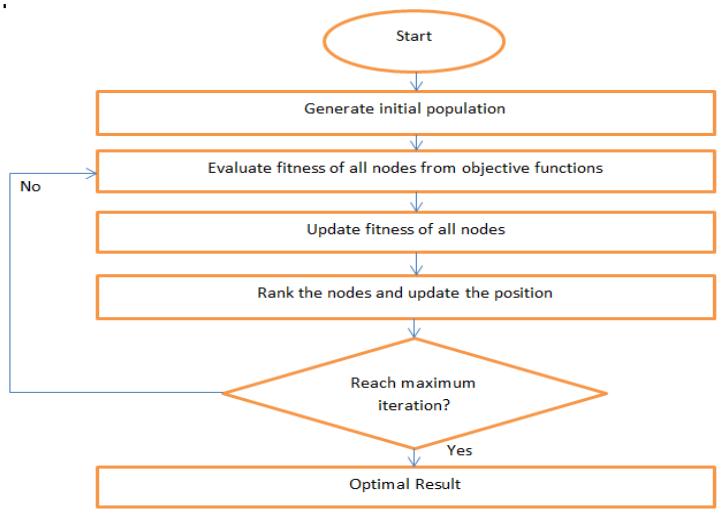


Fig-7: Flow Chart of Firefly Algorithm

Advantages of firefly Algorithm:

1. Firefly Algorithm can efficiently manage multi-modular and non-linear problems of optimization.
2. Firefly Algorithm does not utilize velocities and also there is no issue as that related with PSO (Particle Swarm Optimization).

Now the route is optimized using firefly algorithm, as the malicious node wants to make the maximum damage in the network, so the node may fall under some security threats. After the formation of network, the process will attract malicious nodes, as data starts to transfer from source node to destination node.

C. Detection of Attack

An adaptive learning mechanism strategy is utilized by the proposed model i.e. Fuzzy Support Vector Machine (FSVM). From decision surface two input classes are discovered in Support Vector Machine and besides to any of these input classes, information focuses may not be circulated totally [2]. In proposed method, for each information point a fuzzy membership is applied and furthermore there is reformulation of SVM for learning of decision surface as various contributions are made by various information points. So, we call this proposed strategy a fuzzy SVM (FSVM). It is a multi-classification algorithm; which gives result according to fuzzy logic. It is a new classification algorithm with good interoperability, high generalization power and robustness.

7.3 Malicious Node Detection Algorithm:

Step1. Select Source and Destination
Step2. Broadcast RREQ packet from source node
Step3. Search intermediate node and shortest path
Step4. If reply the RREP packet
It is destination
Else
Broadcast packet to other intermediate node
Step5. If packet drop
Malicious node
Else
Intermediate node, Go to Step 3
Step6. End

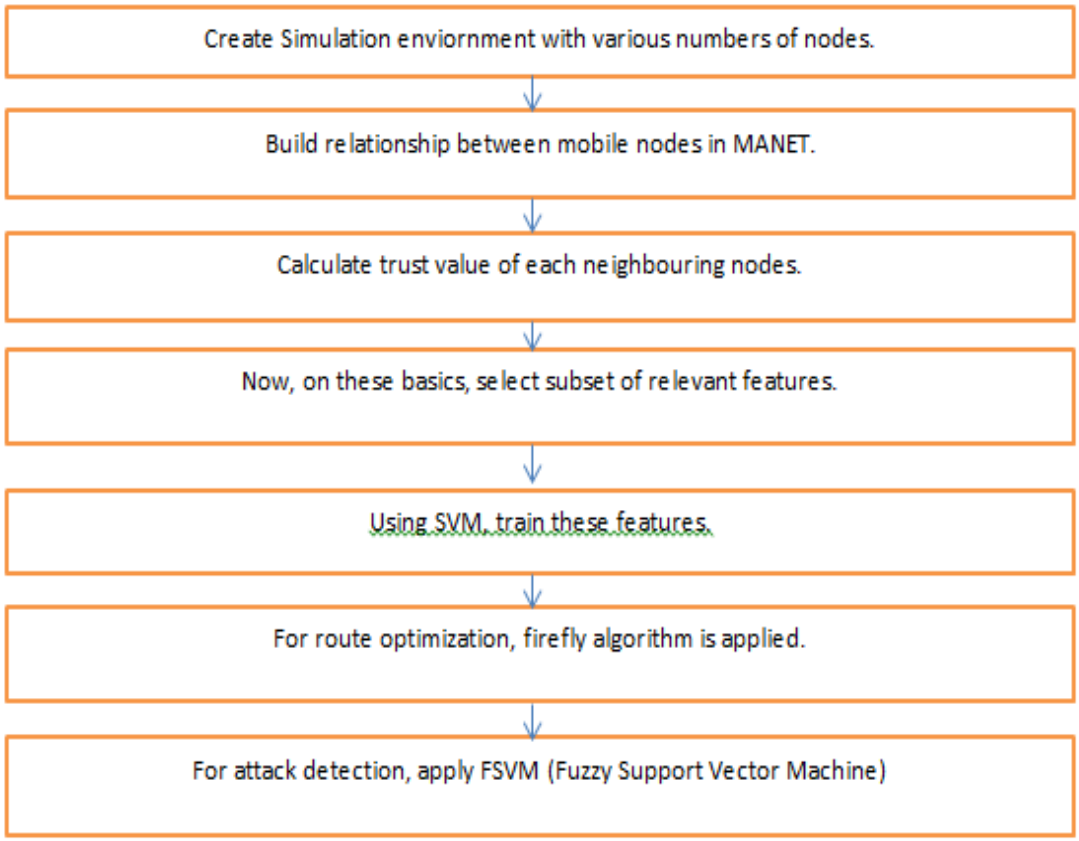


Fig-8: Flow Chart of proposed work

8. SIMULATED RESULTS

Simulation has been done in MATLAB R2018A environment and then network performance will be examined with and without optimization and classification techniques.

8.1. Simulation profile

The simulation profile is listed in table below:

PROPERTY	VALUE
Number of nodes	100
Simulation Time	10 sec
Coverage Area	1000m * 1000m

Table-2: Simulation profile

8.2 Performance matrix:

There are two areas in performance matrix. One is source port and other one is destination port. In which source port has contained generation of information packets and destination port has contained receiving of information packets. Now evaluate the performance of network by utilizing Firefly & Fuzzy SVM by observing changes that occurred in the value of various performance metrics such as Packet delivery ratio, Throughput as well obtained simulation results by varying number of nodes in the network from 10 to 100.

a) Throughput

In total simulation time, the ratio of amount of data transferred from one end towards another end is known as throughput.
In Fig 9: Blue line indicates the obtained throughput value with optimization algorithm i.e. proposed output whereas Red line indicates the throughput values without optimization algorithm i.e. the existing output. With and without optimization, the maximum throughput value is 15000 & 10000 respectively. Now it is concluded that when firefly algorithm and Fuzzy SVM are applied to the network throughput of the network increased.

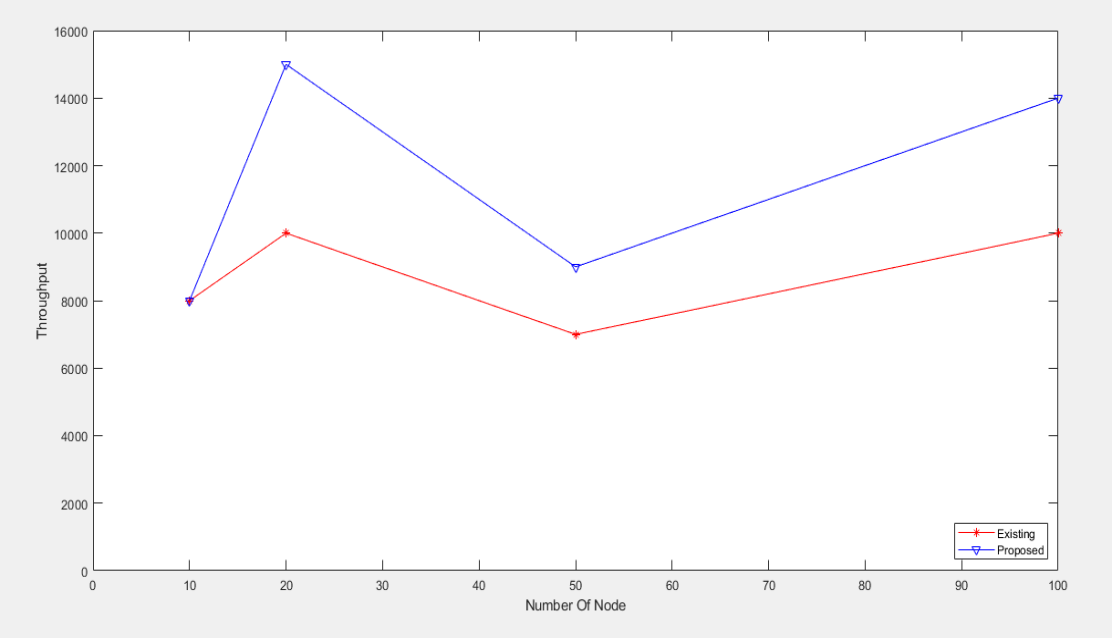


Fig-9: Values of throughput with and without optimization of the network

b) Packet Delivery Ratio (PDR)

The number of information packets that has been sent out by source node contrasted with successfully delivered information packets towards the destination node is known as Packet Delivery Ratio (PDR).
In Fig 10: Red line indicates the obtained value of packet delivery ratio with optimization algorithm i.e. proposed output, whereas Green line indicates the values of packet delivery ratio without optimization algorithm i.e. the existing output. With and without optimization, the maximum value of packet delivery ratio is 1809 & 1591 respectively. Now it is concluded that when firefly algorithm and Fuzzy SVM are applied to the network, packet delivery ratio increased.

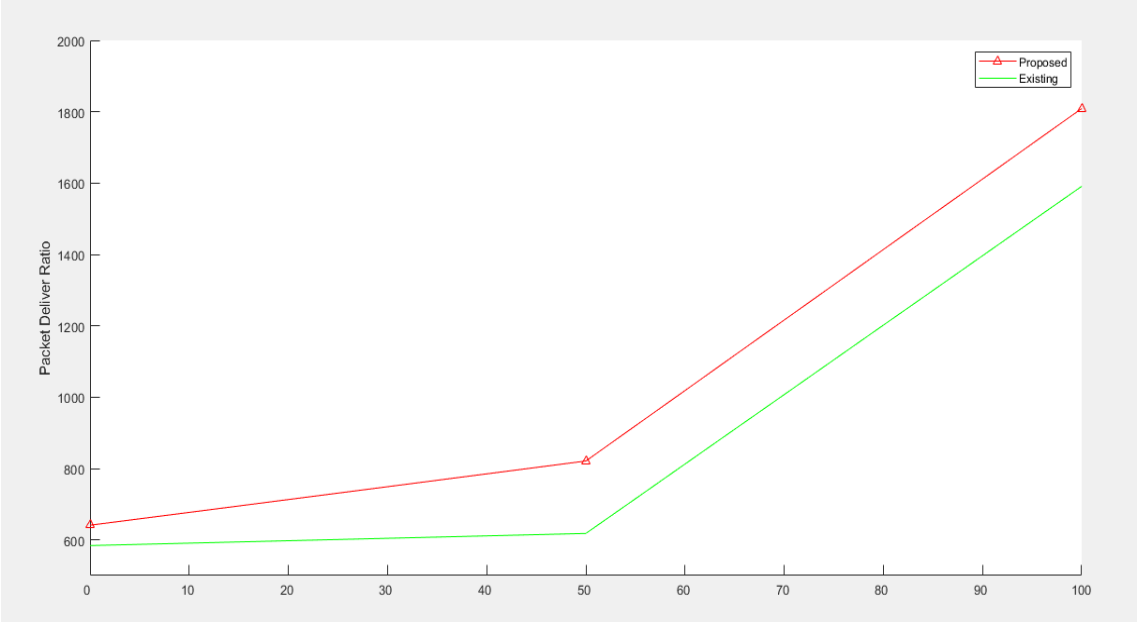


Fig-10: Values of packet drop ratio with and without optimization of the network

8.3 Simulation Analysis

The simulation analysis that throughput increases, Packet drop ratio increases. Security being the major concern of the dissertation, it focuses on how to enhance the security in the network against black hole attacks.

9. CONCLUSION & FUTURE WORK

9.1 Conclusion

The proposed model deals effectively for the detection and prevention of black hole attack in Mobile Adhoc network. The system out to be made secure from different attacks for maintaining data integrity that are noticeable. It was concluded that performance of system are improved by the applied strategy which gives better outcomes. The proposed work is superior to the existing work. In this proposed work, the tool utilized for simulation is MATLAB, which gives a better analysis of the work. It can be concluded that by the use of proposed algorithm the throughput and packet drop ratio increased. The algorithm prioritises security as one of the main concern to be looked upon. When compared with the circumstance, loss ratio is diminished where algorithm was not applied. How the work has been done to overcome the performance of attack is the proof of simulation results. First the analysis is summarized and then it can be utilized for attack mitigation. The simulation results show that the proposed method has high accuracy in classifying and predicting harmful nodes in the network. The precision of the proposed method is about 85%, which is comparable with previous methods in predicting malicious nodes and network infiltration.

9.2 Future Work

In future work, these methodologies can also be utilized for detecting & preventing the network from other network layer attacks like Gray hole attack, sink hole attack. By utilizing other optimization techniques and classification techniques, the performance of network can also be increased. Like Genetic algorithm, Cuckoo Search algorithm for optimization of routes and Fuzzy logic, Support Vector Machine, Artificial Neural Network for classification of attack.

In the proposed work, within the network, first black hole node is recognized and afterward removes the forged route from network. Now by utilizing SVM which is a machine learning technique, route is find out from source node to destination node. If network suffers from malicious node, at that point the performance of the network like delay, throughput, Bit Error Rate (BER), Energy Consumption have been degraded. Now for improving the network performance and reducing the packet drop ratio, by using optimization algorithm named as firefly algorithm, route has been optimized. Firefly algorithm finds the nodes on the basis of fitness function and after that classifies the network using Fuzzy SVM. Now, the route has been removed from the network, if it suffers from Black Hole attack and after that parameters are

evaluated. By using these optimization & classification techniques, a secure and an efficient network have been designed. Comparison graph are discussed with and without optimization algorithms and it is discovered that performance of network is preferred with optimization over that of without optimization. The proposed algorithm is utilized only for AODV protocol but in future it tends to be utilized for other routing protocols like DSDV, DSR.

REFERENCES

[1] Sachin Malviya, "An optimized approach for Black Hole Attack Detection in MANET", in: International journal of S/w & H/w Research in Engineering, ISSN – 2347- 4890. Vol. 4, Issue-2, February 2016.
[2] Vishal Wlia, "Trust Management Based Improved Mechanism to prevent MANET from Security threats using Optimized SVM", in: International Journal of innovative Technology & Exploring Engineering (IJITEE), ISSN – 2278-3075, Vol. 8, Issue-9, July 2019.
[3] Amanpreet Kaur, "Prevention & Detection of Black Hole Attack in MANET", International Journal of Advanced Computeronics & Management Studies", in: Vol.3, Issue-6, May-2019,pp-1-10,ISSN: 2456 – 1835.
[4] Kirandeep Kaur, "Comparison Analysis of Fuzzy Logic & Firefly Algorithm for Co-operative Attack Detection in MANET: A REVIEW", International Journal of Innovative Research in Computer & Communication Engineering, in: Vol. 4, Issue-4, April 2016.
[5] Kongala Pavani, "Anomaly Detection System for routing attacks in Mobile Adhoc network", in: ACEEE, International Journal of N/w Security, Vol.6, April 2014.
[6] C. K. Nagpal, Chirag Kumar, Bharat Bhushan, Shailender Gupta, "A Study of Black Hole Attack on MANET Performance", in: I.J.Modern Education and Computer Science, 8, 47-53,2012.
[7] Ramanpreet Kaur, Anantdeep kaur,"Black Hole Attack Detection in MANETs using Artificial Neural Networks", in: International Journal For Technological Research In Engineering, Volume I, Issue 9,May-2014.
[8] Vishnu Balan E, Priyan M K. GokulNath C, Prof.Usha Devi G, "Fuzzy Based intrusion detection system in mobile ad hoc networks", in: Science Direct, Procedia Computer Science 50(2015), pp.109-11,2015.
[9] Houda Moudni ,Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, "BlackHole Attack Detection Using Fuzzy Based Intrusion Detection System In Manets", in: International Workshop of web search and data mining,ScienceDirect,pp.1176-1181,2019.
[10] Sarika S, Pravin A, Vijaykumar A, Selvamani K, "Security Issues In Mobile Ad Hoc Network", in: Science Direct, Procedia Computer Science 92,pp.329-335,2016.
[11] Meenashu Gupta , Mr. Varun Juseja, "Improvisation of QOS Parameters by Detecting and Preventing Black Hole Attack using Artificial Intelligent Techniques", in: International Journal For Research In Applied Science In Journal & Engineering Technology(IJRASET), Volume 6, Issue II, February 2018.
[12] Saurabh Kumar, Anjani Garg, "Detection & Mitigation of Black Hole Attack in MANET using Artificial Intelligent Technique", in: International Journal Of Engineering Research in Computer Science and Engineering(IJERCSE), Volume 4, Issue II, November 2017.
[13] G.Vennila, Dr. D.Arivazhagan, N.Manickasankari,"Prevention of Cooperative Black Hole Attack in MANET on DSR protocol using Cryptographic Algorithm", in: International Jorunal of Engineering and Technology(IJET), Volume 6, November 2014.
[14] A. Sharma, P.K. Johari, "Eliminating Collaborative Black Hole Attack by using Fuzzy Logic in MANET", in: International Journal Of Computer Science and Engineering(IJCSE), Volume 5, Issue 5,May 2.
[15] Jaydip Sen, Sripad Koilakonda, Arijit Ukil, "A Mechanism of Detection of Cooperative Black Hole Attack in Mobile Adhoc Network", in: 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, 2011 IEEE, DOI 10.1109/ISMS.2011.58.
[16] Vaishali Gaikwad, Lata Ragha, "Security Agents for Detecting and Avoiding Cooperative Blackhole Attacks in MANET", in: 978-1-4673-9223-5/15/$31.00_c 2015 IEEE.
[17] Dr. G. Krishna Kishore, K. Jahnavi, D. Suresh Babu, "Tracing down Black hole attack in MANETS", in: IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 5, Ver. III (Sep.- Oct. 2017), PP 06-10.