An Improve Energy Consumption in O-AODV Protocol for MANETs using MATLAB Simulator

Nirmaljit Kaur[1], Parveen Sharma[2]
[1]M.Tech (Scholar), [2]Associate Professor
Department of computer Science Engineering, CGC, Landran (Mohali)

***Abstract* -** Wireless Sensor Network type is a Mobile ad-hoc network which is a self-organizing network of movable nodes associated with wireless links that initialize a topology. The movable nodes are run time free to move randomly and to organize themselves in a random method. The Mobile ad-hoc network topology might extend speedily and unpredictable. In this field, the routing protocol plays a significant role of enhancing quality of service. There are various types of routing protocols such as hybrid, re-active and proactive routing protocol. In a MANET, there is progress in resolving the security issues, which has directed to the proliferation of threats given the vulnerabilities of network. In this paper, we implemented a novel routing protocol called Optimized on-demand Distance Vector routing, which lower the energy and failure route path correction messages and provides better performance than the original On-demand distance vector routing protocol w.r.t set of evaluation metrics such as throughput, end to end delay, packet loss and packet delivery etc. we designed the Optimized-AODV routing protocol and implemented with assured simulation evaluation parameters using MATLAB 2013a. The Performance analysis of routing protocol designed for WSN has been very challenging. Later, imitations are continuously used to get the preferred performance consequences.

***Keywords* -** Wireless Sensor Network, Mobile Ad-hoc Network, O-AODV, MATLAB simulation Tool.

I. INTRODUCTION

Classified the Wireless Sensor Networks are two types i.e infrastructure and infra-structure-less networks. In this network, every node ismanaged by a main center access point and base station since in infra-structure-less networks the each other without any main head. MANET is an illustration of infra-structure-less network has been designed anywhere, any site at any time interval any pre-described structure [1]. The mobile nodes are associated with each other without any center access point. The self-determining ability of each mobile node makes each mobile node to search the nest-hop nearest to send the mobile node to reach at the sink in the absence of a central co-ordinator. In MANET is described as infra-structure-less, multi-hop and rapidly growing dynamic topology. The main challenge in mobile ad-hoc network is how to make reliable and connected for efficient transport of data. The dynamic topology, error advantage WC(Wireless Channel) and self-organizing capacity of this network makes routing more challenging compared to newest cellular network[2].

The aim of routing protocol is to describe some set of rules that each mobile node has to follow to connect with other mobile nodes. Routing protocol describes the choice of the route path to issue the data and to select a route path between any binary moveable nodes available in the network [3]. Every moveable node describes the network topology in advance and maintains its own routing-table. Routers pick information about the network topology by disturbing information among proximate nearest node. In MANET working, when the node moves from person, place with other network speed, locations of mobile nodes very w.r.t time. The dissimilar moveable models are used to verify these moveable designs and there is a need to study various mobility structures [4]. The purpose is that the moveable structure has great effect on the performance measure of MANET might not be correct and misinform the application [5]. Left of the research paper is described as follows: Section II discussed the prior work and routing protocols available in the survey. Section III presents that the issues in MANET, Section IV described the Proposed Work with the algorithm and Section V discussed the simulation consequences followed by a conclusion n Section

II. RELATED WORK

K.Sumathia(et.al),2015 presented the achievement of Adaptive HELLO messaging proposal to decide the local link connectivity information to check the link status between nodes along with the incorporation of Dynamic on Demand Routing Protocol to decrease the energy consumption of mobile nodes to certain extent [6]. **Ahmed, Marian, (et.al) , 2014** they are suggesting changes in conventional AODV protocol to prevent black hole attack . The essential idea to detect and isolate spiteful nodes is which the use of false messages [7]. **Jhaveri, Rutvij(et.al) 2012** proposed a scheme for Ad-hoc On-demand Distance Vector protocol, where a middle node detects the spiteful node sending false routing in sequence; routing packets are used not only to pass routing in sequence, but also to pass information about spiteful nodes [8]. **V. Kamatchi(et.al), 2012** deals with prevention of both types of black hole attacks and secure data communication using secret sharing and Random ultimate Routing Techniques [9]. MANETs defined few intruders that could be easily attacked MANET. Normally, there are binary kinds of attack define in an Ad-hoc network are Passive and Active Attacks [16]. In Passive attack never destroyed / manipulate the methods of a routing protocol, but it only tries to get the reasonable information by just looking and studying the network traffic, which varieties user issue to detect it. Inactive attack is a challenge to unauthorized access and manipulates data, gain confirmation or acquireaccessibility by adding incorrect packets into the system. Active attack could also be divided into binary types: external and internal attacks [17]. An external attack is an individual that is produced by the movable nodes,i.e. not from the similar network. An internal attack is completed by the movable nodes that belong to the same network [18,19]. The comparatively external attack, internal attack is more complex to identify, since the intruder nodes already defined to the similar network as security parties [20].

III. SECURITY ISSUES and GAP IN MANET NETWORK

During the study of the literature survey we have found out some ways MANET like open intermediate, high dynamic nature of the network lead to several attacks which partition or ends entire network. A black hole attack can be working in obstruction to routing in mobile ad-hoc networks [10]. A black hole node is a malicious node which sends the fake reply to route requests and drops the packets. In this paper, an original approach is proposed to detect black hole nodes in the MANET. Our explanations find out the benign route between sending node and receiving node [11] . The simulations show that the planned approach is more efficient than normal AODV when the black hole attack is current with high packet delivery and less packet drop. From the survey we have found the problem or proposed work in which we are going to continue our work of Energy optimization in MANET using AODV protocol / find Black hole attack.

Research gaps/ Problem:

• Mobile ad-hoc framework is the type of framework where communication takes place in a distant medium by developing an access point. Conversely, several dissimilar models such as Wireless Sensor Networks are the models/systems in which transfer of data packages takes place by using physical medium [12].

• The network layer in Mobile Ad-hoc Networks is vulnerable to several attacks as a result of snooping by way of using a malevolent intent, spoofing some specific control and data packages handled malicious alteration of the package matters as well as the Denial-of-service attacks, Wormhole attacks, Sinkhole attacks, Black hole attacks [13].

• The routing protocols of MANET are unprotected and after this... takes effect come around into the system with the noxious malicious nodes in the system, e.g. DSR, OLSR, AODV, etc. Amongst these, we tried to check and improving the safety of the AODV routing protocol [14,15].

IV. PROPOSED METHODOLOGY

In proposed work, we will focus on the AODV routing protocol to find a black hole attack. In this routing protocol the route discovery mechanism is used to send packets from one mobile node to other that will help to find malicious nodes in the black hole attack. In order to avoid such route detection mechanism each time when the package is transmitted, the routing technique is used. Then black hole nodes will be optimized using artificial be a colony algorithm in AODV environment using parameters like end to end delay, energy consumption, and throughput and error rate.

Step 1: Initialization a network in mobile ad hoc network. We defined the number of moveable nodes in MANET network. First, we varied to the number of nodes from 0 to n nodes in the given area of 1000*1000m.

Step 2: To find the source and destination. In source node, sent the request to the intermediate node and search the sink node to transfer the information. Destination sends the acknowledgment signal to the source node.

Step 3: Design the coverage area, to transfer the information one node to another node. Calculate the coverage area, coverage matrix and distance etc.

Step 4: Initialize AODV Protocol means ad hoc on demand distance vector routing protocol is a reactive routing protocol,which create a route when a node necessitates sending data packets. It has the ability of unicast and multicast defeating. It uses a terminus sequence number which makes it dissimilar from other on demand routing protocols.

Step 5: Nearest path search to transfer the information. Data travels one node to another node, then attacker node occurs to loss the information and time consumption increases. This attack can be easily decreased by setting the unrestrained mode of each node and to see if the next node on the path forward the data traffic as expected. Evaluate the performance parameters i.e energy consumption, error rate, throughput and delay etc.

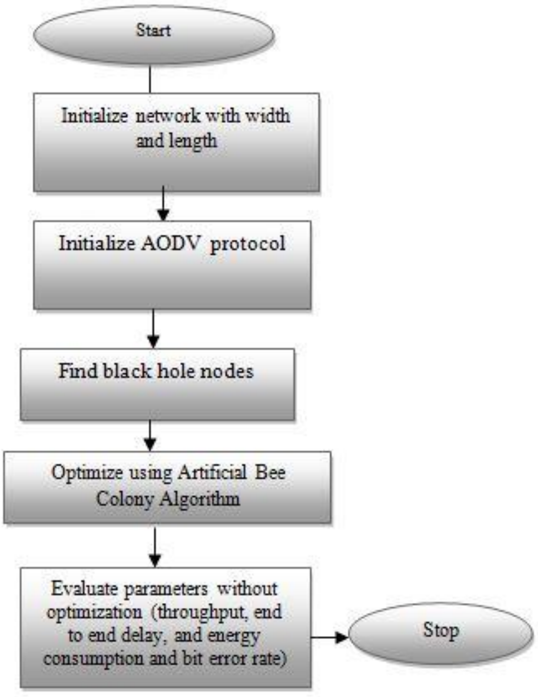
Start
Initialize network with width and length
Initialize AODV protocol
Find black hole nodes
Optimize using Artificial Bee Colony Algorithm
Evaluate parameters without optimization (throughput, end to end delay, and energy consumption and bit error rate)
Stop

Fig.1 Proposed Flow Chart

- RREQ
- RREP

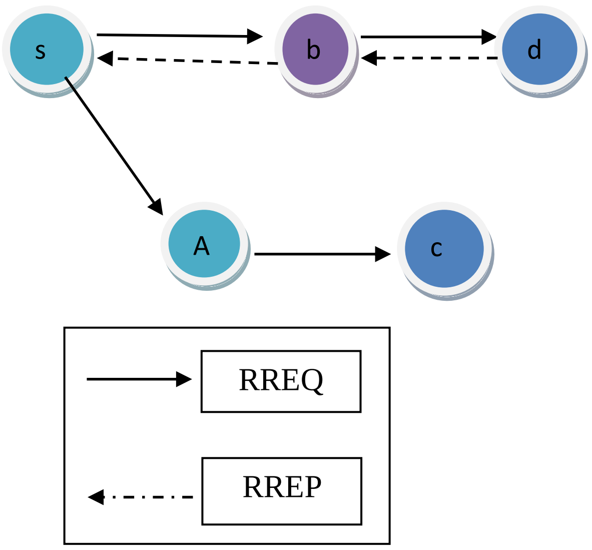

Fig.2 AODV Protocol

In this figure 2 described that the nodes 2 and 4 verify that this is a novel request and that the start_sequence _@ is not stated with respect to the reverse route to node 1. Nodes 2 and 4 forward the request. Update start_seq for node 1 and Increment hop_connect the request packet.

Step 6: Apply Artificial Bee Colony optimization algorithm using a fitness function to optimize the effect on the attacker node. In ABC algorithm, an artificial bee colony consists of working bees, onlookers and scouts. A bee coming up on the dance area to obtain the information about food sources is called a bystander, a bee going to the food source is named as an employed bee, and a bee carrying out an accidental search is called a guide. The location of a food source denotes a possible solution to the optimization problem, and the nectar amounts of a food source represent the quality of the connected solution. Initially, a randomly distributed population is generating. For every food source, there is only one working bee. So the number of working bees is equal to the numeral of food sources. Afterward, the positions will be updated repeatedly with the subsequent cycles until the maximum repetition is reached or stop conditions are satisfied.Evaluate parameters like end delay, throughput, energy consumption, bit error rate.

Step 7: Optimized –On demand distance Vector Routing Protocol: In this proposed work, we implement the optimize-AODV protocol to increase the packet delivery, throughput and reduce the energy consumption. Evaluate the performance parameters and compare with previous one.

V. SIMULATION RESULTS

These experiments are used, performance parameters shown as Table 1. We calculate condense mobile ad hoc network with 30 nodes within an area size of network 1000*1000m using MATLAB (2013a). We analyses optimizethe delivery packets value for the time Seconds under numerous speed and mobility rush models.

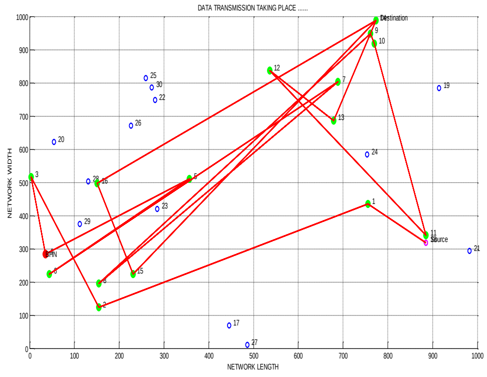

Fig.3 Network Architecture in MANET

In this figure no. 3 described that the network architecture in MANET.We calculate a mobile node in the network is 30 nodes within area size is 1000*1000. The Data is travelling the source to destination through the neighbor node from the destination node. We implement the AODV protocol, we initialize the nearest nodes and node sent the request to another, one node is free then packet transfers the intermediate node from the destination node. Attack nodes occur in the secure route and generate the issues i.e delay increases and packet loss.

Table no.1 Comparison between Packet Loss in AODV and O-AODV Protocol

Number of Nodes	Packet Loss (AODV)	Packet Loss (O-AODV)
5	14.6	6.1
10	14.8	10.19
15	15.1	11.7
20	15.3	11.87
25	15.5	11.96
30	15.7	13.27

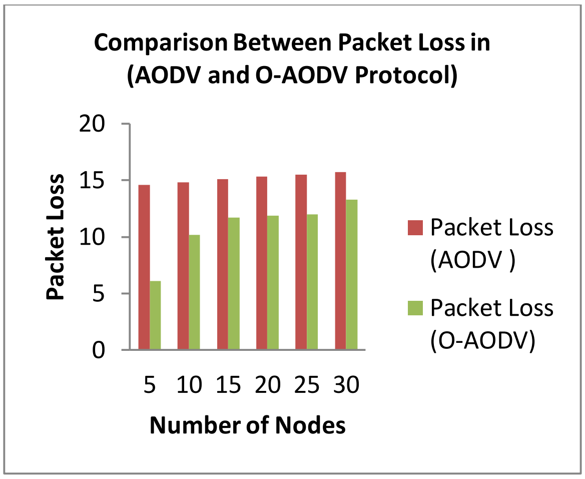

Fig.4 Comparison between AODV and O-AODV protocol in Packet loss

The above figure defined that the packet loss with AODV+O-AODV Protocol. Packet Loss is the disposal of packets in a network when a router or other network device is loaded and cannot accept added packets at a given instant.

Table no.2 Comparison between Delay in AODV and O-AODV Protocol

Number of Nodes	Delay (AODV)	Delay (O-AODV)
5	4.36	3.2
10	4.38	4.7
15	5.5	5.2
20	5.6	5.23
25	5.8	5.24
30	6.0	5.26

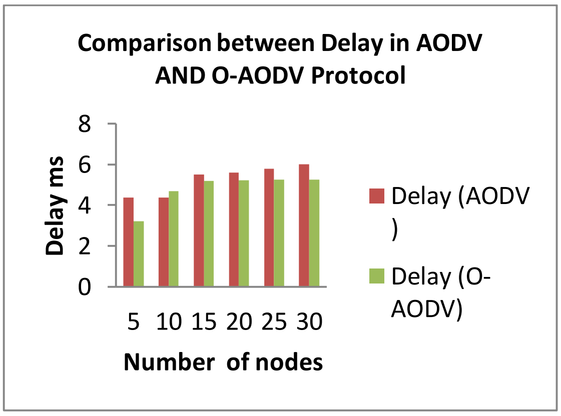

Fig.5 Comparison between AODV and O-AODV protocol in Delay

The above figure defined that, for the time taken for a packet to be transmitted across a network from source to destination.The end to end delay which is less,as compared to the end delay with Black hole attack. This measure should be low to successful delivery of packets at a particular time from source to the destination.

Table no.3 Comparison between Delivery in AODV and O-AODV Protocol

Number of Nodes	Delivery (AODV)	Delivery (O-AODV)
5	61	95.1
10	66	95.3
15	74	95.5
20	77	95.7
25	81	95.9
30	82	96

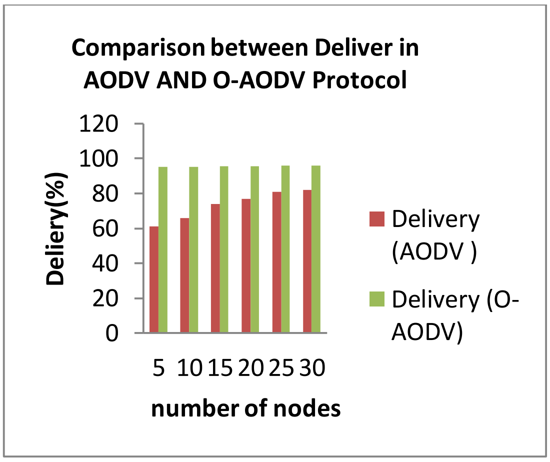

Fig.6 Comparison between AODV and O-AODV protocol in Delivery

The above figure described that the Packet delivery rate using AODV+O-AODV Protocol withBlack Hole attack. It means attacking will come to less deliver the packets.

Table no.4 Comparison between Throughput in AODV and O-AODV Protocol

Number of Nodes	Throughput (AODV)	Throughput (O-AODV)
5	5	10
10	9	20
15	20	50
20	30	58
25	39	70
30	48	95

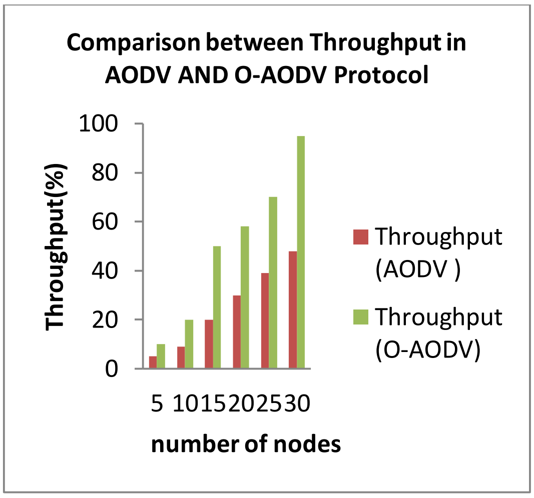

Fig.7 Comparison between AODV and O-AODV protocol in Throughput

The above figure described that the Energy consumption using AODV+O-AODV Protocol and Black Hole attack. The attack has performed the ad-hoc network, then decreases the performance of the throughput.

Table no.5 Comparison between Energy in AODV and O-AODV Protocol

Number of Nodes	Energy (AODV)	Energy (O-AODV)
5	51	46
10	145	134
15	159	149
20	247	250
25	300	279
30	359	300

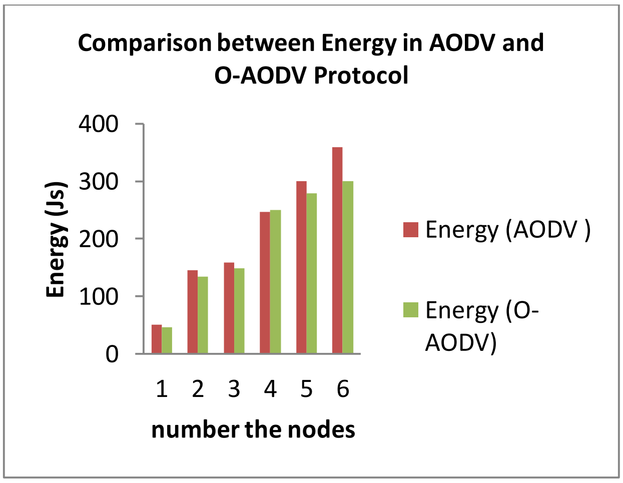

Fig.8: Comparison between AODV and O-AODV protocol in Energy

The above figure described that the Energy consumption,according to the AODV+O-AODV and Smartest Hole attack. The attack will come from the ad-hoc network increase the energy consumption. The behavior of sensor nodes when they are close to their end of a lifetime is defined and analyzed. An assessment with other models for energy consumption is made and propositions for upcoming work are obtainable.

VI.CONCLUSION

This paper presents in deep study of AODV and O-AODV reactive routing protocols for securing the information, packet loss recovery and route discovery. MATLAB Simulator has been used as the simulation tool to test the performance metrics of these protocols. Some parameters such as end-to end delay, throughput, packet delivery ratio; packet loss network lifetime has been measured as the performance metrics to check the applicability of these protocols.Simulation results designate that (between O-AODV and AODV) DSR is better than AODV in terms of packet delivery ratio and throughput, whereas O-AODV has less average end to end delay than AODV.

Again, surprisingly with increasing no. of nodes O-AODV and AODV produce almost constant delivery. But, the routing delay supports O-AODV and delay is more in AODV in case of normal mobility model and nearly equal in the case of random model. Further, our simulation study achieves that network continues for a longer period of time using AODV protocol than O-AODV protocol.O-AODV route discovery succeeds in fewer tries than AODV routing protocol. We have carried out an a extensive simulation study to analysis the performance of proposed O-AODV and compared it with that of an existing AODV routing protocol using theMATLAB simulator tool. The simulation results show that the performance of O-AODV routing protocol is better than AODV routing protocol in most of the metrics, such as the energy consumption.

VII. REFERENCES

[1]. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., Nemoto, Y.: Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. International Journal of Network Security 5(3), 338–346 (2007).

[2]. Jaisankar, N., R. Saravanan, and K. DuraiSwamy. "A novel security approach for detecting black hole attack in MANET." Information Processing and Management. Springer Berlin Heidelberg, 2010. 217-223.

[3]. Mahmood, RA Raja, M. Hussin, N. Manshor, and A. I. Khan. "Impact of node inter-domain movement on MANETs performance." In Communications (MICC), 2015 IEEE 12th Malaysia International Conference on, pp. 107-112. IEEE, 2015.

[4]. Nayak, Padmalaya, and Pallavishree Sinha. "Analysis of Random Way Point and Random Walk Mobility Model for Reactive Routing Protocols for MANET Using NetSim Simulator." In Artificial Intelligence, Modelling and Simulation (AIMS), 2015 3rd International Conference on, pp. 427-432. IEEE, 2015.

[5]. Biradar, Siddlingappagouda, and Prahlad Kulkarni. "An Improved Quality of Service Using R-AODV Protocol in MANETs." In Artificial Intelligence, Modelling and Simulation (AIMS), 2015 3rd International Conference on, pp. 402-407. IEEE, 2015.

[6]. Sumathi, K., and A. Priyadharshini. "Energy Optimization in Manets Using On-demand Routing Protocol." Procedia Computer Science 47 (2015): 460-470,elsvier.

[7]. Ahmed, Mariwan, and Muhammad AwaisHussain. "Performance of an IDS in an Adhoc Network under Black Hole and Gray Hole attacks." Electronics, Communication and Instrumentation (ICECI), 2014 International Conference on. IEEE, 2014.

[8]. Jhaveri, Rutvij H., Sankita J. Patel, and Devesh C. Jinwala. "A novel approach for grayhole and blackhole attacks in mobile ad hoc networks."Advanced Computing &Communication Technologies (ACCT), 2012 Second International Conference on. IEEE, 2012.

[9]. Kamatchi, V., and RajeswariMukesh. "Securing Data from Black Hole Attack Using AODV Routing for Mobile Ad Hoc Networks." Advances in Computing and Information Technology. Springer Berlin Heidelberg, 2013. 365-373.

[10]. Luo, Zhe, Xiaoying Gan, Xinbing Wang, and Hanwen Luo. "Optimal Throughput–Delay Tradeoff in MANETs With Supportive Infrastructure Using Random Linear Coding." IEEE Transactions on Vehicular Technology 65, no. 9 (2016): 7543-7558.

[11]. Sinha, Vishal, and Tilak Raj. "Implementation of message passing interface in MANETs in processing of big data." In Computers, Communications, and Systems (ICCCS), International Conference on, pp. 113-117. IEEE, 2015.

[12]. Jathe, Shreyas S., and Vidya Dhamdhere. "Hybrid Cryptography for Malicious Behavior Detection and Prevention System for MANETs." In Computational Intelligence and Communication Networks (CICN), 2015 International Conference on, pp. 1108-1114. IEEE, 2015.

[13]. Nikam, Pranjali Deepak, and Vanita Raut. "Improoved MANET Security Using Elliptic Curve Cryptography and EAACK." In Computational Intelligence and Communication Networks (CICN), 2015 International Conference on, pp. 1125-1129. IEEE, 2015.

[14]. Gupta, Subodh Kumar, Kapil Govil, and Alok Agarwal. "Routing Algorithm for Energy Conservation in MANET." In Computational Intelligence and Communication Networks (CICN), 2015 International Conference on, pp. 165-167. IEEE, 2015.

[15]. Thomas, Ashish, Vijay Kr Sharma, and Gaurav Singhal. "Secure Link Establishment Method to Prevent Jelly Fish Attack in MANET." In Computational Intelligence and Communication Networks (CICN), 2015 International Conference on, pp. 1153-1158. IEEE, 2015.

[16]. Soni, Mohit, Manish Ahirwa, and Shikha Agrawal. "A Survey on Intrusion Detection Techniques in MANET." In Computational Intelligence and Communication Networks (CICN), 2015 International Conference on, pp. 1027-1032. IEEE, 2015.

[17]. Kumar, M. Senthil. "A Survey on Intrusion Detection Techniques in MANETs." International Journal 3, no. 10 (2015).

[18]. Hartaman, Aris, and Basuki Rahmat. "Performance and fairness analysis (using Jain's index) of AODV and DSDV based on ACO in MANETs." In Interactive Digital Media (ICIDM), 2015 4th International Conference on, pp. 1-7. IEEE, 2015.

[19]. Mohanapriya, T., S. Raja Ranganathan, and S. Karthik. "A survey on top-k query processing in MANETs." In Intelligent Systems and Control (ISCO), 2017 11th International Conference on, pp. 480-484. IEEE, 2017.

[20]. Wu, Chuchu, Mario Gerla, and Mihaela van der Schaar. "Social Norm Incentives for Network Coding in MANETs." IEEE/ACM Transactions on Networking (2017).