Life Time Improvement and Attack Resilience Against Gray and Black Hole Attacks in Dragon Fly Topology Based MANET

Premala*, Md.Bakhar**

Research Scholar, Dept. of E&CE, Guru Nanak Dev Engineering College, Bidar, Karnataka, India

Professor, Dept. of E&CE, Guru Nanak Dev Engineering College, Bidar, Karnataka, India

Corresponding Author; e-mail: kashipremala@gmail.com

ORCID ID: 0000-0003-3267-4731, 0000-0003-2624-6298

Research Paper Received: 19.08.2019 Revised: 07.09.2019 Accepted: 24.09.2019

Abstract-MANET is an autonomous network of nodes with capability of movement and without any necessity of infrastructure for connectivity. Due to mobility of nodes, network topology changes continuously characterized by network partitioning and routing disruptions. Dragon fly topology is used to improve the network throughput and reduce latency in internet. The hierarchical nature of Dragon fly reduces the network diameter, cost and latency. This work proposes Dragon fly clustered energy efficient ant colony based AODV (DC-EEAAODV) protocol extending the concepts of Dragon fly topology to MANET and ant colony based route selection with goal to improve network QOS and life time of the network. Due to hierarchical nature, the impact of attacks like gray, black hole on network is high and this work proposes efficient routing resilient against gray and black hole attacks for Dragon fly based MANET. The simulation of the proposed DC-EEAAODV is done in NS2 environment and performance of the proposed protocol is compared against AOMDV and Dragon fly based FFAOMDV to prove the efficiency of the proposed DC-EEAAODV protocol.

Key words: MANET, Black hole, Gray hole attacks, Dragonfly Topology.

1. Introduction

MANET is created by autonomous moving nodes which cooperatively engage in a continuously changing infrastructure. An Important characteristic of MANET is that there is no necessity of a backbone infrastructure for connectivity and communication of the nodes. Each node cooperatively manages the absence of

an infrastructure backbone. Due to node mobility and continuously changing infrastructure, multi hop routing becomes challenging. The life time of path is low and faults in routing are quite common. Optimum energy consumption and network life time improvement is also a critical requirement for MANET deployed in unattended environments like wild life monitoring. But for a network to be usable in many applications, it must deliver a certain level of quality of service. Capacity and quality at each link is different and hence QOS is very difficult.

Dragonfly topology is a most popular topology for internet. Being a low diameter network it is able to achieve high index routes. Due to high index in routes, there are multiple paths in the network and it ensures a fault tolerant routing. It is gaining popularity as the most promising network topology for internet. The network is of low diameter due to high radix routers. The network is of two level hierarchy with router groups are fully connected. These groups are then connected at second level assuring fully connected network.

Performance in dragonfly is highly dependent on communication patterns and routing method. Throughput and delay is best in dragonfly topology due to presence of shortest number of hops between the source and destination nodes for any traffic patterns. This work extends Dragon fly topology for MANET with goal of increased network throughput, minimal delay and energy consumption. Since MANET is an autonomous network, presence of attackers must be detected and prevented to maintain the quality of service. Impact of attacks, especially gray and black hole attacks is higher in case of Dragon fly adopted MANET's due to its hierarchical nature. This work proposes an energy efficient attack resilient routing in Dragonfly adopted MANET. The contributions in this paper are

- Extension of Dragon fly onto MANET with a solution to higher contention in intergroup links and poor use of path diversity in typical Dragon fly topology.
- Ability to detect black and gray hole attacks in Dragonfly topology and preventing the network from those attacks.
- Routing adaptations for Network life time enhancement in Dragonfly topology.

2. Literature Survey

In [1] author analyzed bio inspired and evolutionary approaches for routing. The method works for wireless ad hoc sensor networks. Two methods of swarm optimization and colony optimization for routing are surveyed in this work. The work inferred that evolutionary approaches are effective in improving routing performance. Authors in [2] developed an efficient encoding scheme using particle swarm and formed a multi-objective fitness function for clustering and routing decisions. Failure of cluster head is tolerated effectively using the proposed solution. The work did not consider the mobility and transient failure of nodes, also the work is centralized. A differential evolution based

algorithm is proposed in [3]. It solves the problem of routing in two tier sensor networks. Using a novel mix of search and differential evolution it is able to find optimal routes. Experimentally differential evolution is found to be better than genetic based algorithms. Algorithm for black hole detection and prevention working over the backbone of AODV is proposed in [4]. Each nodes trust is calculated in the network using data control packets and nodes with trust lower than threshold are dropped in routing paths. The communication overhead is higher due to frequent exchange of data control packets in the network.

Authors in [5] propose two novel routing mechanisms in aim to avoid deadlock in Dragonfly networks. Routing freedom and deadlock free paths are the salient features in this solution. Black hole detection and prevention using the concept of dynamic threshold is proposed [6]. The advantage in this approach is that black-hole nodes are detected during finding of routing paths rather than during data transmission stage. The limitation in this work is that, routing overhead is high in this approach, also it is not secure against gray hole attacks. Authors in [7] proposed a multi path routing protocol with consideration for energy optimization. Particle swarm optimization is used in this work. Optimal loop free paths are found using neural networks and this solved the problem of link disjoints. Particle swarm optimization trains the parameters of neural network and this neural network finds the best path from source to destination. The PSO parameters used for training neural network are transmission cost, energy factor and optimal traffic ratio. Due to control packet flooding, the routing overhead is high in this approach. To detect gray hole nodes in MANET, a heuristic solution is proposed in [8]. This approach is done extending the AODV protocol with bait detection based on destination sequence number. This approach has low overhead as the attackers are detected using route discovery stage. Detection of black hole using cooperative sensing and assistance is proposed in [9].

Every node watches if neighbor is forwarding packet and if it detects a misbehavior, broadcasts the misbehaving nodes identified to other nodes in the network, so that routing via those misbehaving nodes are skipped. This approach is dependent on cooperative assistance and fail, in case of node fails to send OERR cooperatively. Optimization of energy consumption in MANET using AODV routing backbone is proposed in [10]. It is referred as Fitness function based AOMDV. Energy Optimal path form source to destination is found using the fitness function. A multipath routing protocol using the concept of Hopfield network is proposed in [11]. This method solves node disjoint and link disjoint problem in routing paths. This approach considers only reliability in construction of multi path routes with consideration for delay and energy consumption. Life time is proposed using PSO and based on it route recovery is done in [12]. Life time is predicted using the parameters of nodal mobility and drain in energy .Fuzzy rules are created to make the nodal decision as strong or weak. Weak nodes are replaced with strong nodes

in the route, thereby routing performance is stabilized. Dual attack detection method is used to detect black and gray hole attack is proposed in [13]. It used Intrusion Detection System to analyze the behavioral information and based on it malicious nodes are detected. The malicious nodes are black listed. The approach is not secure against cooperative attacks.

Authors in [14] proposed a novel method for clustering. It was inspired by PSO based multi agent stochastic parallel search technique. The cluster heads are selected in such a way to take care of mobility and remaining energy. The fitness function used in this work improved the lifetime of Cluster heads and Cluster members. Authors in [15] extended the geographic routing with PSO based optimization for energy efficiency. This method increased the life time by minimizing the energy utilization. The fitness function is modeled in terms of distance between nodes and nodal power. Authors in [16] secured the MANET topology against routing attacks. Cooperative black hole attacks are detected using this solution. Certain designated nodes called Security Monitoring Nodes (SMNs) are deployed in the network. They monitor the behavior of node during routing. The malicious nodes are detected by SMN and the information is periodically exchanged to other nodes, so as to prevent the nodes from black hole attacks. This approach does not consider the case of SMN being compromised. The well known TORA routing protocol was extended with PSO based energy optimization in [17]. This work considers hop count of route and energy of route in its route search process .The routing is formulated as optimization problem and BPSO is used to choose a route so as to maximize the energy level of route. The approach is able to ensure fairness in energy consumption by distributing the load among routes based on energy of routes. MANET with fitness function for routing based on optimization of energy consumption is proposed in [18].

3. Proposed DC- EEAAODV Solution

The proposed Dragon fly clustered energy efficient ant colony based AODV (DC-EEAAODV) solution consist of three stage

- Dragon fly topology adaptation.
- Energy Efficient Routing using ACO.
- Attack resilient Routing.

3.1 Dragon Fly topology Adaptation

Dragon fly topology creates a hierarchical clustered network with the goal creating a network with higher reliability and increased packet delivery ratio. The entire MANET network is split to three layers of node, group and system as shown in Figure 1. A two level of clustering is done. Nodes with cluster heads in one level called as node group and second level cluster heads in next level called as system group. There is one connection between every pair of groups. Balanced paths are created as result of Dragon fly topology with at least two local channels for packet traversal. Since there are redundant paths, the reliability of the network is increased. Among the multiple paths available for routing, the shortest paths are selected using ant colony optimization and packet delay is reduced in these

shortest paths. The pseudo code for partition of the MANET using Dragon fly algorithm is given in Table 1.

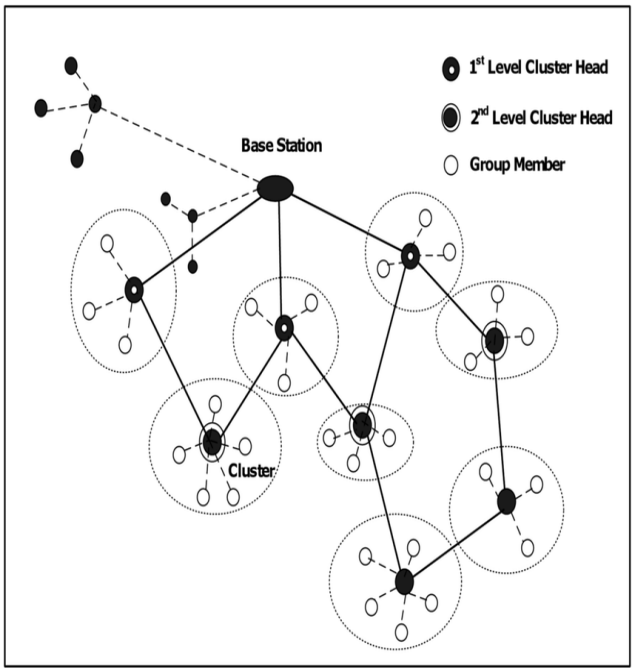

Fig.1.Dragon fly adopted for MANET

Table. 1.Pseudo code for Dragonfly topology creation

Step 1: position of the node recorded

Step 2: random direction for nodes is given

Step 3: random velocity assigned to each nodes

Step 4: Mesh topology is initialized to all nodes

Step 5: each nodes assigned with equal radius for dragonflies

Step 6: calculate distance between each nodes and normalizing values

Step 7: For (Iter = 1 to Iter ==10)

Clustering nodes = All

While (Nodes for cluster = None)

End While

FOR (Dragonfly(i) = 1 to All

a) Fand E_s = empty, F_s Cost = ∞, and E_s cost= -∞)

b) Calculate objectives for Dragonflies

c) Update radius& F_s , E_s

d) Update weights

e) Neighboring radius

END FOR

Calculate

a) Separation distance
b) Alignment value
c) Enemy weight
d) Food Weight

IF neighbor! =0

a) Update velocity
b) Update new position

Else

a) Levy flight

END IF

END FOR

Optimal cost == fitness in food

END FOR

Step8: IF (Non clustered nodes > 15%)

Repeat Step 1

Else

Quit

End IF

Abbreviations:

Iter : Iteration

Fs: food source (Shortest path)

E_s : Enemy source (Malicious node, Black/Gray hole)

3.2 Energy Efficient Routing using ACO

The proposed solution used Optimization based on Ant Colony (ACO) to find the energy optimized routing path from source node to sink on Dragon fly topology realized using above procedure. For use of ACO on the Dragon fly network G, each of the links are associated with an artificial pheromone value τ. The value of τ modifies due to two conditions of ant moving it or

time period. Modification due to transition of ant over link ij is expressed as

$$\tau_{ij} = \tau_{ij} + \Delta\tau \qquad (1)$$

And the modification due to time is expressed as

$$\tau_{ij} = (1 - \sigma)\tau_{i\,j} \qquad (2)$$

Where the σ is the evaporation constant for the pheromone. Source node becomes starting point of travel for a configured number of nodes and these ants travel in all possible paths to destination and converges in a shortest path. At each hop, each ant stochastically makes a probabilistic decision to move to next hop. The probability is expressed as

$$p_{ij}^{d} = \begin{cases} \frac{\tau_{ij}}{\sum_{j \in N_i} \tau_{ij}}, & j \in N_i \\ 0, \text{otherwise} \end{cases} \qquad (3)$$

Ni being the number of neighbors. Due to availability of multiple paths in Dragon fly topology more number of paths are explored in the search process and the ant arriving soon to source, gives the path with shortest number of hops from source to destination.

3.3 Attack Resilient Routing

The proposed routing on the Dragon fly adopted MANET considers resilience from following cases of selective forwarding (SF) attacks.

Gray hole	Packets dropped by some selective nodes
Black hole	Packets from all nodes are dropped

The proposed SF resilient routing adapts the AODV and consists of two phases

1. Detection phase
2. Diffusion of detected nodes from routing table

The requests (RREQ) and reply (RREP) used in current format by AODV is modified to detect malicious nodes. The modification is done by inducing some of the proactive routing behaviors into reactive nature of AODV. The logic of original AODV's sequence numbering scheme is used in this work. Any wireless node having packet to base station sends RREQ and waits for the route in reply RREP. From all the RREP, the router with shortest hop is used for data transmission. When a Selective forwarding (SF) attacks occurs, the source node is not aware of it. To solve it, sink assistance is added. By examining the sequence numbers in packets arriving from source, sink can detect the presence of SF attack. There will be gap in the sequence number in case of SF attack which sink can detect. Sometimes packet loss may be due to channel quality, so sink can detect SF attack with a probability.

The proposed solution used SPEED based forwarding mechanism. The packet is sent with fixed speed in this protocol. The speed s guarantees that packet traverses each hop in bounded time (Ad/s). Due to this packets traverse in shortest path to destination. Packet transmission in opposite direction is not allowed as it will make speed to go in negative value. During packet transmission from source S to destination D, from perspective of source S, two space regions are identified.

- Sender Radio Range (SRR)
- Sender Feasible Candidate(SFC)

SRR contains all nodes reachable from source. SFC is the next hop nodes to neighbor of source S. In the Figure 2 below, A and B are in the SFC region with positive speed, while 1 is not a possible solution due to negative speed. The next available node with capability to reach transmission speed above threshold is selected between A and B.

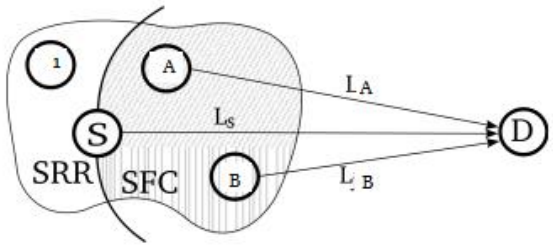

Fig.2. SRR/SFC

Following are the features of the proposed forwarding protocol.

Stateless architecture	The protocol does not need to store and decision is made without any state. Due to this it requires less memory.
Real time	It is possible to configure fixed speed. Thus guaranteeing soft real-time speed
Minimum Mac layer support	The protocol only requires best effort delivery from the MAC layer.
QOS management	In case of congestion the protocol can use back pressure to reroute by which it can control congestion and improve QOS.

The procedure for suspicious node detection has two phases

- Detection of Suspicious node
- Forwarding time detection

In first phase, each node proactively detecting the presence of attacker with steps below

Step 1: Each node sends a message with random non-existent dummy destination.

Step 2: Grey hole and Black hole nodes replies with the RREP for those destination.

Step 3: The source node can identify the suspected gray and black hole node from the RREP.

Step 4: Source node sets deadline time to reach to the destination which is called expected latency.

Step 5: Source compares the latency of each route leading to the destination by expected latency and takes up next hop decision.

Step 6: If latency is more than expected such nodes or routes are identified to paths of attackers.

Step 7: Every node repeats this activity after every periodic interval. Proposed protocol avoids suspected nodes while routing.

The second phase consists of detection of suspicious nodes are normal or malicious (gray or black hole) during the packet forwarding process with steps given below.

Step1: Source node search for the next forwarding node in the routing path.

S is the source node; D is the destination node; and A is a black hole in the below scenario. The routing path is S, A, B, D. Node S becomes watcher for only Node A, and not Node 1 and Node 2 in our scheme.

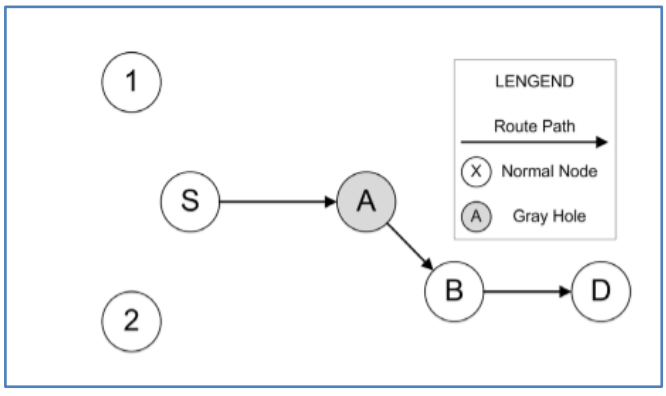

Fig.3. Detection during forwarding

Step2: If next hop is suspected node then follow step 3 else forward the packets

Step3: In each node, a forward packet buffer (FBP) is present. It is used for packet signature verification. The algorithm has following steps:

1) During packet forwarding, its signature is added into the FPB and this is overheard by the detecting node.

2) When next hop data forward is overheard, signature is released from the FPB.

3) Forwarding rate is calculated by the detecting node for every fixed interval of time and compared to the threshold.

The next hop node is detected as black or gray hole attacker if the forwarding rate is less than threshold. Once this is detected, next hop node is added into blacklist and the detecting node never forwards to that next hop node. So our proposed protocol avoids the malicious nodes in the form of black and gray hole attacks while packet forwarding.

4. Simulation Results and Discussion

The proposed solution was simulated in NS2. Simulation was conducted with following parameters.

Table. 2.Simulation Configuration

Parameters	Values
Nodes in the Network	100
Communication range	250m
Simulation area size	1200m*1200m
Priority distribution	Uniform distribution with 20% distribution for each priority
Node Deployment Topology	Random
Simulation time	30 minutes
Interface Queue Length	50
MAC	802.11
Number of Base station	1
Location of Base station	Upper right
Initial energy of nodes	8 joules
Data traffic	CBR with each packet of size 512 bytes
Percentage of attackers	10% of total node
Routing Protocol	DC-EEAAODV

The proposed solution is compared with AOMDV and Dragon fly based FFAOMDV [10]. We measured following parameters

- Throughput
- Delay
- Packet Delivery Ratio
- Network Lifetime
- Energy Consumption
- Energy Consumption in presence of black and gray holes

Throughput: The throughput at sink (kbps) is measured for different number of nodes and result is given below Figure 4.

The proposed solution has higher throughput than FFAOMDV and AOMDV. The throughput increased by a factor of 7kbps on compared to FFAOMDV and factor of 10kbps compared to AOMDV in the proposed solution. The higher throughput is attributed to shorter hop for the travel of packet from node to sink and the availability of multiple paths in dragon fly topology.

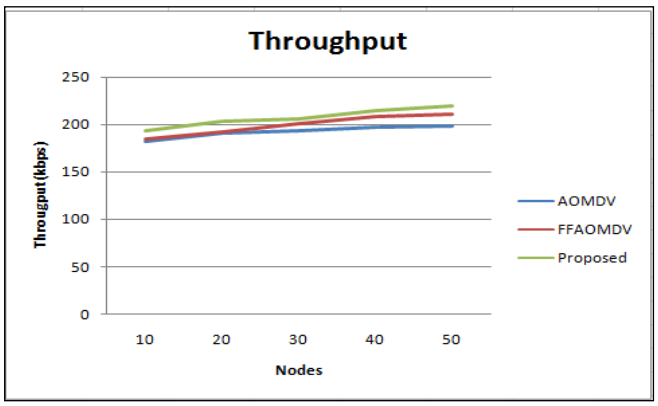

Fig.4.Number of Nodes vs. throughput

Delay: The average delay (sec) is measured for different number of nodes, as shown in Figure 5.The proposed solution has lower delay than FFAOMDV and AOMDV. The delay reduced by 33% compared to AOMDV and 19% compared to FFAOMDV in the proposed solution. The reduction in delay is mainly due to identification of shortest path by ant colony guided AODV on the dragon fly topology.

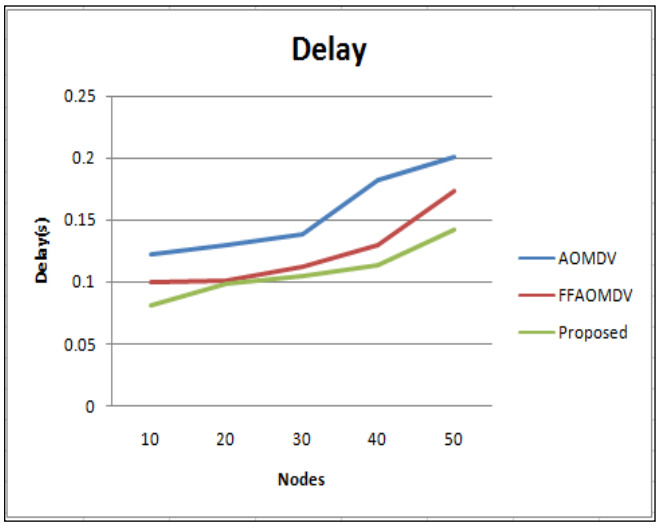

Fig.5.Number of Nodes vs. Delay

Packet Delivery Ratio: The ratio of packet delivered successfully at sink is measured for varied nodal number in network and result is given below Figure 6.The packet delivery has increased on average 5-6% in the proposed solution compared to AOMDV and FFAOMDV. The packet delivery ratio is higher in the proposed solution due to use of redundant path support inbuilt into Dragon fly topology adopted in this work.

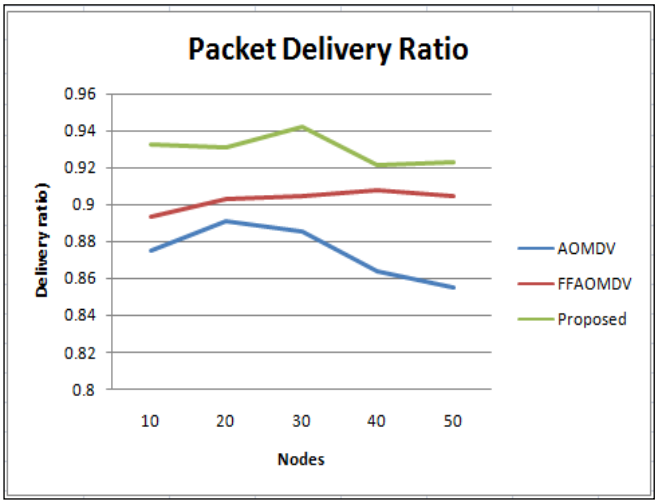

Fig.6.Number of Nodes vs. Packet Delivery Ratio

Dead Nodes: Network life time is measured in number of dead nodes over the time of simulation and the result is shown in Figure 7. The dead node count is reduced by a factor of 30% in the proposed solution compared to FFAOMDV and 18% compared to AOMDV. The reason for reduction in dead node count is due to reduction in energy consumption in the paths found using ACO.

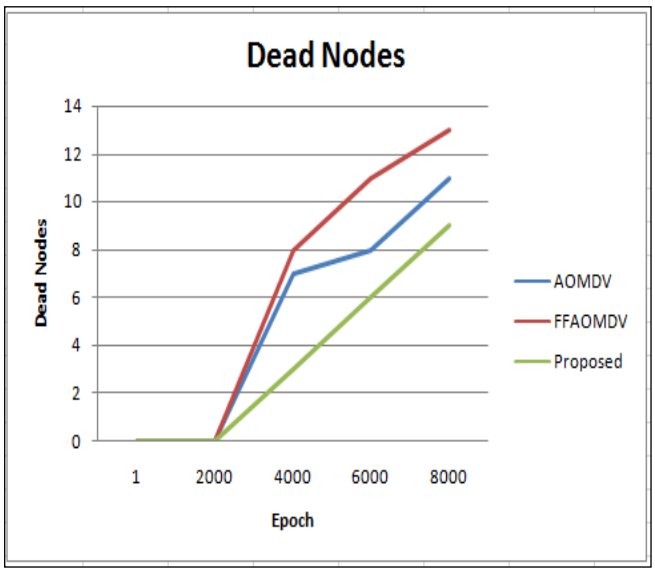

Fig.7. Number of Nodes vs. Dead Nodes

Energy Consumption: The energy consumption in the path is measured and plotted as shown in Figure 8.The energy consumption for routing is reduced by a factor of 15% in case of proposed compared AOMDV and 49% compared to FFAOMDV. The reason for energy consumption is mainly due to reduction in path hop count and selection of less interference paths.

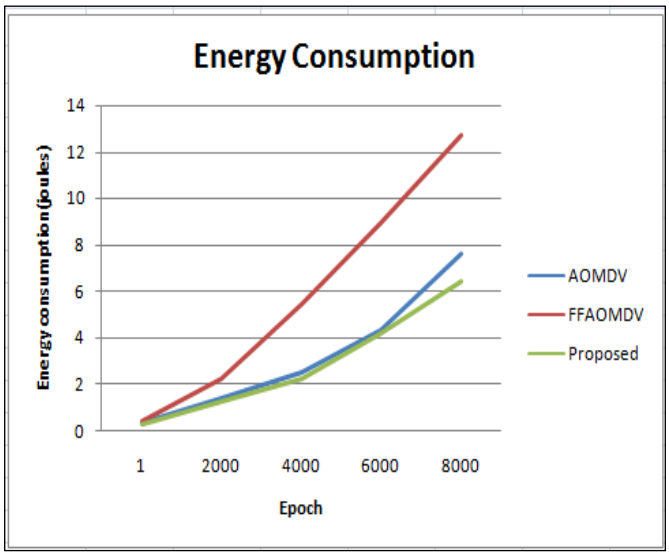

Fig. 8.Number of Nodes vs. Energy Consumption

The effect of attackers on energy consumption in paths is measured and plotted. Even in presence of attackers, the energy consumption is comparatively lower in the proposed solution as demonstrated in Figure 9.

The results are more similar to case of black hole attackers and even in presence of attack; the energy consumption is low, resulting in better life time than existing solutions.

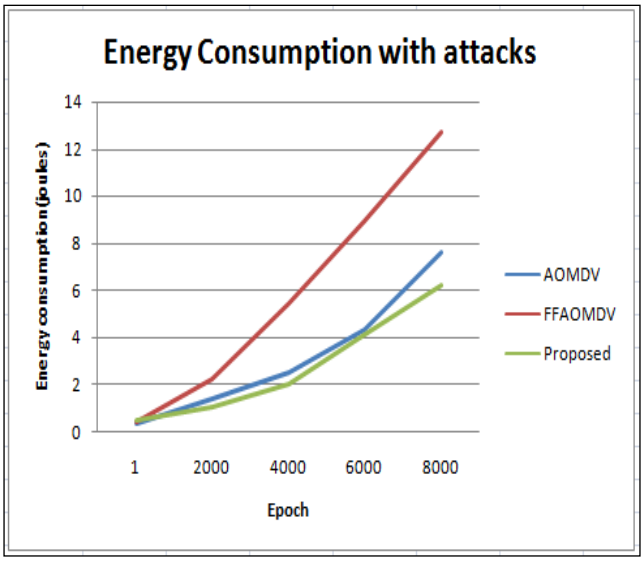

Fig.9. Number of Nodes vs. Energy Consumption with attacks

5. Conclusion & Future Work

Dragon fly cluster based energy efficient ant colony based AODV is proposed in this work. Due to Dragon fly topology, path redundancy is provided and use of ant colony based AODV for path selection ensures higher packet delivery ratio. Due to proposed detection method black hole and gray hole attackers are detected and dropped in the routing path. Due to this, the proposed solution is resilient against attacks. The proposed solution was simulated in NS2 and performance is compared against AOMDV and FFAOMDV. The proposed solution is found to have better

performance in terms of ratio of packet delivered successfully, delay and network life time. The packet delivery ratio improved by factor of 6% compared to exiting solutions. The throughput increased by a factor of 10kbps and the delay dropped by average 20%. The number of dead nodes dropped by 30% compared to existing solution proving the life time efficiency of the proposed DC-EEAAODV protocol.

The work can be extended by adding defensive mechanisms for other type of attacks like denial of service, wormhole attacks. The work can also be extended for delay tolerance in routing selection.

References

[1] Z. Ali and W. Shahzad, "Critical Analysis of Swarm Intelligence based Routing Protocols in Ad hoc and Sensor Wireless Networks", IEEE International Conference on Computer Networks and Information Technology, 2011.

[2] M. Azharuddin and P. K. Jana, "PSO-based approach for energy-efficient and energy-balanced routing and clustering in wireless sensor networks", Soft Comput. Springer, 2017, Vol.21, Issue 22, pp.6825-6839.

[3] U. K. Chakraborty and S. K. Das, "Energy-Efficient Routing in Hierarchical Wireless Sensor Networks Using Differential-Evolution-Based Memetic Algorithm", WCCI 2012 IEEE World Congress on Computational Intelligence.

[4] A. Dorri, S. Vaseghi, "DEBH: Detecting and Eliminating black holes in Mobile Ad Hoc Network", Springer, 2018, Vol.24, Issue 8, pp.2943-2955.

[5] M. Garcia and E. Vallejo, "Efficient Routing Mechanisms for Dragonfly Networks", 2013, 42nd International Conference on Parallel Processing.

[6] S. Gurung, S. Chauhan, "A dynamic threshold based approach for mitigating black-hole attack in MANET", Wireless Networks, Springer, 2018, Vol.24, Issue 8, pp.2957-2971.

[7] Y. H. Robinson, M. Rajaram, "Energy-Aware Multipath Routing Scheme Based on Particle Swarm Optimization in Mobile Ad Hoc Networks", The Scientific World Journal, Vol. 2015.

[8] R. H. Jhaveri , N. M. Patel, "A sequence number based bait detection scheme to thwart gray hole attack in mobile ad hoc networks", Wireless Network, Springer, 2015, Vol.21, Issue 8, pp.2781-2798.

[9] Y. M. Khamayseh and S. A. Aljawarneh, and A. E. Asaad, "Ensuring Survivability against Black Hole Attacks in MANETS for Preserving Energy Efficiency", Sustainable Computing: Informatics and Systems. Vol.18, pp.90-100, suscom.2017.07.001 http://dx.doi.org/ 10.1016/j.

[10] S. Jaiswal, "Energy efficient and improved network life time multipath routing using FF-AOMDV and Dragon Fly topology", Communications on Applied Electronics, Vol. 7, April 2018.

[11] M. Sheikhan, E. Hemmati, "PSO-Optimized Hopfield Neural Network-Based Multipath Routing for Mobile Ad-hoc Networks", International Journal of Computational Intelligence Systems, Year 2012, Vol. 5, No.3, pp. 568-581.

[12] D. Manickavelu, R. U. Vaidyanathan, "Particle Swam Optimization based node and link time prediction algorithm for route recovery in MANET", EURASIP Journal of Wireless communication and Networking, 2014.

[13] Z. Ali Zardari, J. He, N. Zhu and K. H. Mohammadani, "A Dual Attack Detection Technique to Identify Black and Gray Hole Attacks Using an Intrusion Detection System and a Connected Dominating Set in MANETs", Future Internet 2019, 11, 61; doi:10.3390/fi11030061.

[14] N. Khatoon, Amritanjali, "Mobility Aware Energy Efficient Clustering for MANET: A Bio-Inspired Approach with Particle Swarm Optimization", Wireless Communications and Mobile Computing, Vol.2017, Article ID 1903190.

[15] C. Nallusamy, A. Sabari, "Particle Swarm Based Resource Optimized Geographic Routing for Improved Network Lifetime in MANET", Mobile Networks and Application, Springer 2019,Vol.24,Issue 2, pp .375-385.

[16] T. Poongodi, M. Karthikeyan, "Localized Secure Routing Architecture Against Cooperative Black Hole Attack in Mobile Ad Hoc Networks", Wireless Personal Com., Springer,2016.Vol.90, Issue 2, pp.1039-1050.

[17] C. Rajan, K. Geetha, "Investigation on Novel Based Naturally-Inspired Swarm Intelligence Algorithms for Optimization Problems in Mobile Ad Hoc Networks", World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering, Vol.9, No. 3, 2015.

[18] S. Jamali, L. Rezaei, "An Energy-efficient Routing Protocol for MANETs: a Particle Swarm Optimization Approach", Journal of Applied Research and Technology, 2013, Vol.11, Issue 6, pp. 803-812.