RESEARCH ARTICLE OPEN ACCESS

Enhanced Swarm Based Mac Layer Protocol For Lazy Receiving Process In Manets

G. Nazia sulthana*, Dr.Virendra kumar sharma**
*(Dept. of Computer Science & Engineering, Bhagwant University, Ajmer, India
Email: naziasulthana83@gmail.com)
** (Dept. of Electrical and Electronics Engineering, Bhagwant University, Ajmer, India
Email:viren_krec@yahoo.com)

Abstract:

Lazy Receiver Processing is new network subsystem architecture, which provides stable overload behaviour, fair resource allocation, and increased throughput under heavy load from the network. Enhancements in the MAC layer protocol need increases the efficiency of scheduled process. Another major concern in LRP is security. The LRP network is always highly vulnerable to attackers due to wireless communication mediums. If any such attack occur in the network degrades the network performance and increases the overhead in the network. In this paper, our focus is to improve the network life time by enhancing scheduling process in MAC layer & enhancing detecting and diffusing attacks capabilities by improvements in AODV. Enhanced ant colony based AODV protocol for the analysis of gray and black hole attack effects. A comparative analysis is shown among EAACO (Energy aware ant colony optimization) and EAODV (Enhanced AODV) protocols. We compared the performance of these protocols based on various QoS parameters delay, control overhead, throughput and packet delivery ratio & alive nodes. The simulation results show that our protocol performance is better than others.

Keywords — **MANET, LRP, Black Hole, Gray Hole Attack, malicious node.**

I. INTRODUCTION

The uses of wireless devices have been growing tremendously in the past decade [1]. The Mobile Ad hoc Networks is somewhat remote system, where remote gadgets, for example, convenient or handheld PCs, PDAs, and PDAs are communicating among themselves through wireless medium. MANET's have some unique characteristics like higher interference rate, Low bandwidth, limited transmission rates, dynamic network conditions, higher data loss rates due to interference, Limited computing power, limited energy resources, limited service coverage and less secure network [1]. Due to dynamic nature of movements, nodes may join and leave the system very frequently.

Lazy receiving process [11] is primarily focused on main memory allocation and swapping designed to ensure graceful behaviour of a timeshared system under various load conditions. Resources consumed during the processing of network traffic, on the other hand, are generally not controlled and accounted for in the same manner. This poses a problem for network servers that face a large volume of network traffic, and potentially spend considerable amounts of resources on processing that traffic. Under this system, resources spent in processing network traffic are associated with and charged to the application process that causes the traffic. Incoming network traffic is scheduled at the priority of the process that receives the traffic, and excess traffic is discarded early. This allows the system to maintain fair allocation of resources while handling high volumes of network traffic, and achieves system stability under overload.

The architecture of MANETs:

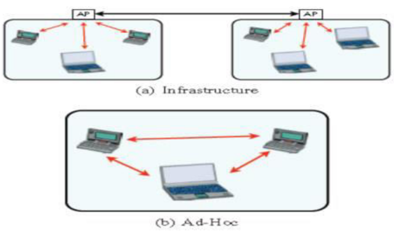

Fig . 1 Wireless Networks

The wireless networks can be categorized based on their system architecture into two basically versions [1]. The one is Infrastructure (Fig 1a) and second is ad-hoc network (Fig 1b). The biggest difference in them is infrastructure networks consist of access point and nodes, meanwhile the ad hoc networks are independent from access point. In the infrastructure version, a terminal can't communicate directly with other terminals in the same cell and other cell. An access point here performs control messages. Messages are sent to the access point and then the access point distributes the messages to the desired terminal.

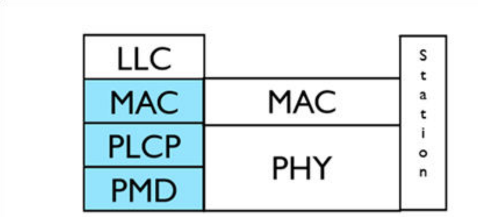

Fig. 2 Standard IEEE 802.11 Architecture

Figure 2 shows architecture arrangement of layers in wireless communications. IEEE 802.11 used for Ad Hoc Networks: The IEEE Standard 802.11 (IEEE, 1999) describes common family of wireless LANs[1]. The standard specifies physical layer (PHY) and medium access control (MAC) of wireless transmission. The main purpose of this standard was the specification of simple and robust wireless LANs. The standard is expected to support the energy conservation of the mobile terminal, consideration of hidden terminal, and possibility of a global license-free service. The basic MAC layer's services are supported asynchronous data service and optional time-bounded service. The IEEE-Standard 802.11 for ad hoc provide only asynchronous data service.

In this paper, we are focusing on improving network lifetime by optimizing scheduling features and increasing security by detection of gray and black attacks in AODV routing protocol. MANET's provide a secure channel for communication is a very challenging issue. The network is very susceptible to the radio interface and accessible to everyone and attackers are easily able to enter into the network [1]. The purpose of the method to maintain good level of the following QoS parameters like throughput, packet delivery ratio, delay, Packet drop & network lifetime. We have considered other routing protocol such EAODV [2] and EAACO [3] for the evaluating performance of our routing protocol.

II. RELATED WORK

The mobile ad hoc network (MANET) is always very energy consuming and network life time needs to improved to save battery life and it is vulnerable to various security attacks due to its characteristics like limited bandwidth, wireless connectivity, easy deployment etc. There are lot of works has been carried out and ongoing on increasing network lifetime and detection of malicious node [5]. Here, we have discussed various works exist on improving scheduling process & detection of black and gray hole attacks and solutions to overcome from such attacks.

Wenkai Wang et al [19] has proposed cross layer attacks and defending the cross layer attacks in cognitive radios. The existing research on security issues in cognitive radio networks mainly focuses on attack and defense in individual network layers. However, the attackers do not necessarily restrict themselves within the boundaries of network layers. In this paper, they design cross-layer attack strategies that can largely increase the attackers' power or reducing their risk of being detected.

A. Rajaram et al [18] have developed a trust based security protocol based on a MAC-layer approach which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, we design a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. In the next phase of the protocol, they provide link-layer security using the CBC-X mode of authentication and encryption

In [6] observed the effect of black hole and gray hole attack on Wireless Sensor Networks (WSN). The analysis is done on LEACH protocol, how this protocol is affected by these attacks are shown clearly. The simulation result proven that the Black Hole attack is severely affected the network performance than Gray Hole attack, both attack reduces the packet delivery. In [7] authors have discussed the issue related to black hole attack in MANET. The AODV steering protocol performance is degraded in terms of packet delivery ratio and throughput, if black hole attack occurs in the network. The proposed system for distinguishing a black hole assault with less correspondence cost. The secure protocol proposed is compared with standard AODV routing protocol. The simulation outcomes show that the proposed algorithm achieves improved results as compared to AODV. In [8] authors address the issue of finding malicious node in MANETs by sending a control arrangement to the neighbor nodes and analyzing its response. In this paper, authors developed a numerical model for the analysis and establish a secure and short route to the destination. In [9] wormhole attack is analyzed for wireless sensor network. A model for detection and prevention of wormhole attack is proposed. The AOMDV (Ad hoc On demand Multipath Distance Vector) convention chosen for the analysis. The convention determined the round trip time (RTT) of each course to ascertain edge RTT. The proposed protocol performance is better than AOMDV. In [10] AODV routing protocol is highly susceptible to black hole attack, where malicious nodes get the data packets and drop them without forwarding to the intended destination node. The existing methods for black hole detection only very few techniques able to identify single and community oriented assaults. The major drawbacks of existing methods incur higher storage and excess computational overhead. The objective of the proposed two different schemes of detecting single and community oriented black hole attacks is minimum directing and less computational overhead.

In [11], there are various types of attacks when malicious nodes manage to enter in the network are gray hole attack, black hole attack, routing attack, message altering attack etc. These attacks have very bad effect on the throughput, packet delivery ratio and normalized routing load etc. In this survey, shows various analysis on the existing attacks along with their detection and prevention mechanisms. In [12] authors discuss the black hole and gray hole attack in DTN system This network is vulnerable to attack due to the limited connectivity. The malicious nodes gain access to the network drop all or part of the received messages. In [13] review on Black hole and Grey hole attack is analyzed based on their types and their functioning for mesh network. The OLSR routing protocol is used and shows how to minimize the effect of these attacks. Analysis shows that black hole attack detection is easier than gray hole attack detection. In [14] authors focused on detection and mitigate the bogus node which is acting as a typical node of the proposed algorithm for detecting the malicious node. The main goal of this proposed method is to identify and prevent gray hole attack and black hole attack. The results show improvement in the security and just as the performance of the network.

In [15] authors planned solutions for black and gray hole attack in various adversary scenarios like single, cooperative, and multiple. The reproduction results accomplish better execution notwithstanding thinking about different instances of black and gray opening assaults when contrasted with existing arrangement Bulwark-AODV. In [16] authors discussed some conservative protocols such as AODV, DSDV and DSR protocols. There are various types of malicious assaults exist in MANET are Black hole, Gray hole, Jellyfish and Wormhole Attack are studied. Here, how trust based scheme is introduced to overcome the adverse effects of such attacks in the network. Each node is assigned a trust value in order to avoid addition of a malicious node during data transmission. In [17] authors discuss various conceivable conduct of node due to attacks drops packets in the network. When number of black hole nodes increase in the network suddenly reduces Packet delivery rate. To improve the security in the network proposed strategy is based on dynamic destination sequence number threshold value. This method helps in detecting the malevolent node and also prevents it from further participation during the route discovery process. The proposed method is to perform better as compared to existing methods in term of packet delivery rate and average throughput under black hole attack. The limitation of the proposed protocol is unable to detect smart gray hole attack due to its participation in route discovery process.

III. PROPOSED METHOD

Methodology has been divided into three major parts

Phase 1: Formation of clusters

Phase 2: Enhancement in MAC layer scheduling

Phase 3: Enhancement in Routing Protocol

Phase 1 : Formation of clusters

MANETs change the topology vigorously without a centralized control, to adopt the topology change; Adaptable K-level hierarchical cluster is used [1]. In fig.1, an example hierarchical clustering is shown. A k-level clustering chain of command is mainly useful in decreasing the power consumption of the network compared to Low-energy Localized Clustering (LLC).This clustering is particularly possible in diminishing the vitality utilization of the system contrasted with (LLC). Since it takes into consideration short-run transmission. Besides, it guarantees flexibility to changes that influence both the system and environment are independent in the routing choice. It naturally gives snappy responses to topological changes in the system by training new clusters setup and does not include routing calculation and nodes perform neighbourhood choice to choose the ideal route. So the X-LLC cluster is utilized because X-LLC allows decreasing the cluster size by considering the radius via the use of different levels of power. This offers a notable benefit in terms of transmission energy consumption minimization with respect to conventional hierarchical algorithms for forming clusters [1].

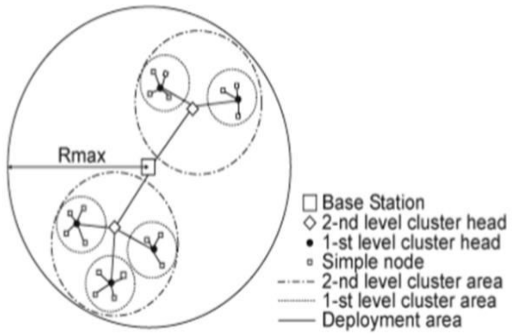

Fig.3 .Example of a hierarchical structure

The formation of cluster consists of election and organization stages.

Step-I: Election stage

In this stage, we have consider k ≥1 levels of cluster heads and k unique election and association phases, LLC derives by choosing k =1. Fig.3 depicts an example of a progressive structure.

The symbols used in the algorithm are shown in Table 1.

TABLE I
SYMBOLS USED

Symbols	Explanation
N_0	Total number of nodes
S_i	The group of node swallowed to involved to the i^{th} level election
N_{ji}	The j^{th} node € S_i
E_{ji}	The residual energy of Nji power level
P_{ji}	Probability that Nji participate to election phase
R_w	The transmission sweep at the w-th transmission control level
τa , τb	The timer value of the node

Process:

Step 1: every node initializes the number of selection messages obtained by a candidate node.

Step 2: m at 0 and creates a uniformly distributed random values u between 0 and 1.

Step 3: compared with threshold Pji defined in (2).

Step 4: when Pji is previously mentioned u, the node turns into a candidate cluster head and participates towards election phase; else, it continue to be silent until the election process terminates .

Step 5: The node is empowered in a commencement m old beginning from the esteem τa.

Step 6: every candidate node transmits an advertising message with transmission power Pw that covers a spatial vicinity of radius Rw.

Step 7: every applicant hub gathers the promoting messages originating from the different competitor hubs in the region and additionally tallies the gained messages by expanding m.

Step 8: when time τa expires, the candidate sets the promotion timer to τb, where τb is function of the number of acquired messages m and the node residual energy.

Step 9: lastly, when τb expires, the candidate timer node turns into a cluster head at i^{th} level, and it transmits an advertising message with Pw transmission power.

Step 10: alternatively, when the timer remains counting down as well as the node obtains an advertising message, it interrupts the promotion timer and wait for the election process termination.

Step 11: Cluster heads at i^{th} level take an interest to the (i +1)th level cluster head selection if not elected, otherwise just remain cluster heads at i^{th} level [1].

Stage II: Organization stage

The organization stage begins following the culmination of the election procedure and involves k-specific affiliation sub stages that are completed in a best down manner beginning from the Base Station to straightforward hubs. At this stage, first kth-level cluster heads relate themselves to the BS, which returns them back the TDMA table. At that point, the (k− 1)th-level cluster makes a beeline for the closest kth-level cluster head, that replies by giving the TDMA table; the procedure repeats down to the ordinary ad hoc node level.

In addition, the accompanying likewise remains constant.

i) Each cluster head controls over few hubs.

ii) Simple hubs finds closest cluster head with separation of single jump.

iii) The transmission scope of straightforward hubs can be diminished regarding the one required by LLC. Therefore, transmission needs less power and the inter cluster obstruction diminishes.

Assurance of the ideal amount of levels for a specified application relies upon the attributes of the sending, the presented hierarchy overhead, the type of hubs, the total degree, the accessible transfer speed and residual vitality.

Phase 2: Enhancement in MAC layer:

Let us assume for simplicity that all packets are of equal length; it is straightforward to extend the algorithm to consider variable length packets. Define the transmission energy ω(τ) of a packet with transmission duration τ as the amount of energy necessary to send the packet over timeτ. Recall that we assume the energy function is strictly convex in transmission duration, so ω(τ) decreases with increasing τ; we will examine the factors governing the convexity of ω(τ) in Section 6. Suppose that the inter-arrival times d1,d2,...,dM for the M packets that arrive in the interval [0,T) are known in advance, i.e., before t=0. (We can assume, without loss of generality, that packet 0 arrives at time 0.) The offline scheduling problem is then to determine the transmission duration

Let K_0=0. Define

$$m_1 = \max_{k\in 1,\ldots,M} \left\{ \frac{1}{k} \sum_{i=1}^{k} d_i \right\}$$

And

$$k_1 = \max \left\{ k : \frac{1}{k} \sum_{i=1}^{k} d_i = m_1 \right\}.$$

For j ≥ 1, let

$$m_{j+1} = \max_{k\in\{1,\ldots,M\}} \left\{ \frac{1}{k} \sum_{i=1}^{k} d_{k_j+i} \right\} \qquad (1)$$

And

$$k_{j+1} = k_j + \max \left\{ k : \frac{\sum_{i=1}^{k} d_{k_j+i}}{k} = m_{j+1} \right\}. \qquad (2)$$

where k varies between 1 and M − kj. These pairs (mj, kj) are used to obtain the schedule ∼ τ defined as

τi = mj if kj−1 < i ≤ kj.

∼ τ has been shown to be optimal; we do not repeat the proof here. Therefore, ∼ τ gives us a lower bound on the energy consumption for all our later comparisons and calculations.

PseudoCode:

```
Initialize : currentTime = 0;
count = packet arrivals till lookahead time T;
availableTime = T;
nextIterationStartTime = T;
repeat { while (currentTime <= nextIterationStartTime)
{        if (channel is Idle)
{
                 send Packet;
wait for ack;
 if (no_ack)
{ // collision
 wait randomTime in (0, 2 * Last CW Value);
availableTime −= randomTime;   }
 else { // no collision    count −−;    availableTime −= curnetPacketDuration;   } }
else
{   wait till Channel is free;
 if (transmitter of the last packet is transmitting
 for the first time in this iteration)
 {    if ( myself transmitted atleast one packet in         this iteration )
 {     // my load is already factored in
 count = availableTime / tranmsissionDuration;    }
 else  {      // my load is not factored in
```

```
count = availableTime / transmissionDuration            + myNumberofPackets;    }   }
else {     count −−;    }
 availableTime −= last packet transmission duration;  } }
nextIterationStartTime += T;
update count with new arrivals; }
END
```

Phase 3: Enhancement in Routing protocol

Enhanced ant colony based AODV (EAAODV) Protocol is a routing protocol works on real time communications. This is achieved by maintaining a fixed delivery speed by means of feedback control and geographic forwarding. Following steps indicate process of routing and eliminating malicious nodes. Fig.4 shows the forwarding mechanism of EAAODV protocol.

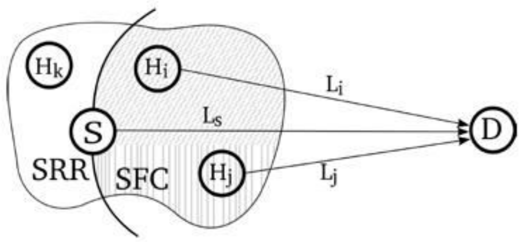

Fig.4 Forwarding mechanism of EAAODV

Step1: Beacon messages are sent with node ID, Position & delay estimation by all nodes.
Step2: Cluster head sends Msg with fake destination id
Step3: If node replies to Msg
  Node = suspected malicious node
  Sends alert msg to all cluster node
 Else
  Node = Non-malicious
 End
Step 4: S uses Sender Radio Range (SRR) finds Hk, Hi & Hj as next hop candidates.
Since Hi & Hj are in direction of D destination they are considered to be positive speed. Where, Hk is in other direction so Negative Speed and discarded & Maximum transmission speed of Hj (since it is farther than Hi and nearer to D) so Hj is selected as Next hop.
Step 5: Backpressure Beacon Message is used in case of congestion to reroute.

IV. SIMULATION AND RESULTS

The simulation work has been carried out in NS-2 simulator, which is widely used for simulation of wireless networks. The simulation parameters considered is shown in table -2.

TABLE II
Simulation parameters

Name	Value
Network Area	850 x 670
Reproduction time	10 sec
Number of nodes	20-100
MAC type	802.11
Antenna Model	Omni directional
Node speed	Uniform (10m/s)
Transmission Range	250 m
Traffic Source	CBR
Protocol	EAAODV

The performance of EAAODV protocol is compared with existing EAODV [2] and EAACO [3] protocols. The following QoS parameters are considered for result analysis.

Control Overhead: The control overhead is a very important factor. When network encounter any attack on the ongoing routing path. Then to mitigate the effect of gray and black of attack new routes are established for proper delivery of data. Here, in fig.5 clearly shows that proposed EAAODV(Enhanced ant colony based AODV) is performed better than EAACO(Energy aware ant colony optimization) and EAODV(Enhanced AODV). The overhead occur during route discovery , route maintenance is minimum as compared to other protocols.

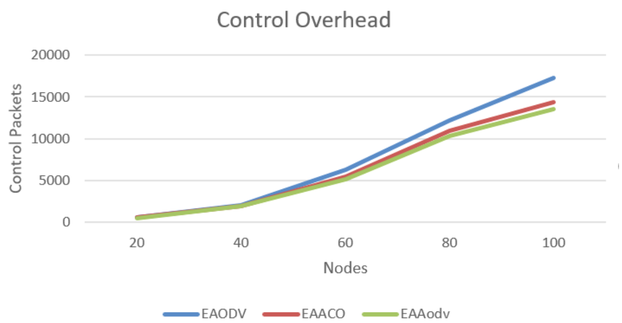

Fig. 5 Number of Nodes versus Control Overhead

Throughput: This is the amount of data packets passed on from a source node to a goal node for each unit of time. The fig.6 shows the throughput achieved by various routing protocol EAODV, EAACO, EAAODV. The throughput is improved as compared to other protocols. The result clearly shows that throughput achieved in our proposed protocol is better as compared to others. With increasing number of nodes the value of throughput is also increasing.

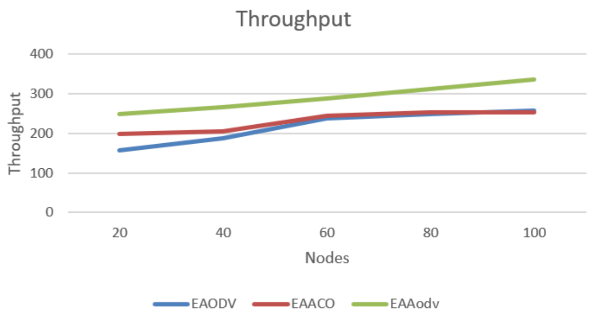

Fig. 6 Number of Nodes versus Throughput

Delay: The variation between accepting time and sending time of packets is considered as delay. The fig.7 shows the delay comparison among protocol EAODV, EAACO, and EAAODV routing protocols. The transmission delay is highest in EAACO protocol for 80 nodes. With gradual number of nodes the delay obtained in our protocol is better than others. The delay is marginally expanded with expanding number of nodes 60 onwards in our convention.

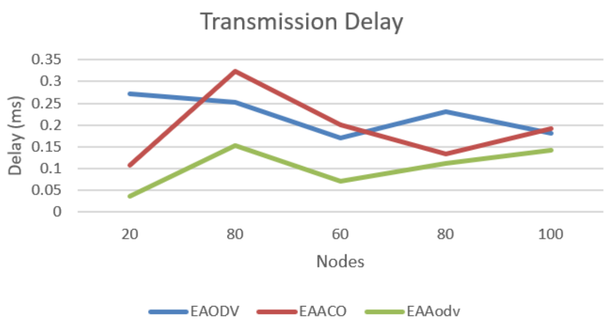

Fig. 7. Number of Nodes versus Delay

Packet Delivery Ratio (PDR): This is the proportion of data on packet received by the destination and data packets sent by the sources. It is clear from Fig.8 that the PDR value achieved by our protocol is acceptable. The numbers of nodes are increased and PDR value is also gradually decreased for all protocols namely EAODV, EAACO, and EAAODV. Overall, throughput with various number of nodes our protocol achieve higher PDR.

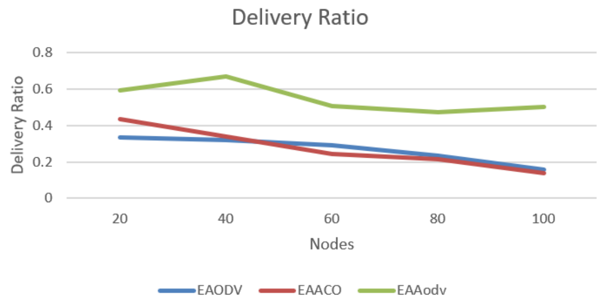

Fig. 8. Number of Nodes versus Packet Delivery Ratio

V. CONCLUSIONS

In this paper, we have discussed an advanced version of AODV protocol namely EAAODV & novel MAC layer protocol to increased network lifetime. The results obtained in term of alive nodes, control overhead, delay, throughput and packet delivery ratio is analyzed for evaluation the performances of these protocols. The proposed protocol shows significant performance as compared to others. In future, we will investigate for maximum value of PDR and also devise mechanism to improve in presence of gray and black hole attack.

REFERENCES

[1] Mobile Ad Hoc Networking. Edited by Basagni, Conti Giordano, and Stojmenovic. Chapter-1, A JOHN WILEY & SONS, INC., PUBLICATION, 2004, pp.1-47.

[2] Taher Delkesh & Mohammad Ali Jabraeil Jamali, "EAODV: detection and removal of multiple black hole attacks through sending forged packets in MANETs", Journal of Ambient Intelligence and Humanized Computing, Springer, · March 2018.

[3] M. Syed Khaja Mohideen and P. Calduwel Newton, "Energy Aware Ant Colony Optimization (ENAANT) to Enhance Throughput in Mobile Ad hoc Networks", International Journal on Future Revolution in Computer Science & Communication Engineering , Volume: 4 Issue: 3, 2018, pp. 343 – 347.

[4] Heena Rani, Jasvir Singh, "Analysis of Swarm Intelligence Optimization Techniques

used in MANETS: A Survey", International Journal of Advanced Research in Computer Science Volume 8, No. 5, May-June 2017.

[5] Shobha arya and Chandrakala arya, "Malicious nodes detection in Mobile ad hoc networks "Journal of Information and Operations Management, Volume 3, Issue 1, 2012, pp.210-212.

[6] Meenakshi Tripathi,M.S.Gaur,V.Laxmi "Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN", The 8th International Symposium on Intelligent Systems Techniques for Ad Hoc and Wireless Sensor Networks (IST-AWSN), Procedia Computer Science 19 (2013) 1101 – 1107.

[7] Vimal Kumar , Rakesh Kumar, "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network", International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014), Bhubaneswar, Odisha, India, Procedia Computer Science 48 (2015) 472 – 479.

[8] Arvind Dhakaa, Amita Nandal and Raghuveer S. Dhaka, "Gray and Black Hole Attack Identification using Control Packets in MANETs", Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015), Procedia Computer Science 54 (2015) 83 – 91.

[9] Parmar Amish ,V.B.Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol", 7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science 79 (2016) 700 – 707.

[10] Arathy K S, Sminesh C N, "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET", Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016), Procedia Technology 25 (2016) 264 – 271.

[11] Benzeer Kaur and Harleen Kaur, "Detection of Black and Gray Hole Attack in Manet: A Review", Advances in Computer Science and Information Technology (ACSIT)pp-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 5; July-September, 2016, pp. 396-400.

[12] T. Sasilatha, S. Vidhya and P. Suresh Mohan Kumar, "Detection and Elimination of Black Hole and Grey Hole Attack on MANET", International Journal of Pure and Applied Mathematics, Volume 116 No. 24 2017, 235-242.

[13] Rupinder Kaur and Parminder Singh, "REVIEW OF BLACK HOLE AND GREY HOLE ATTACK", The International Journal of Multimedia & Its Applications (IJMA) Vol.6, No.6, December 2014.

[14] Nisha, Simranjeet Kaur and Sandeep Arora, "Analysis Of Black Hole And Gray Hole Attack On RPAODV In MANET", International Journal of Engineering Research & Technology (IJERT)Vol.2 Issue 8, August – 2013, pp.192.196.

[15] Vasantha Sandhya Venu and Damodaram Avula, "Invincible AODV to detect black hole and gray hole attacks in mobile ad hoc networks", Int J Commun Syst. 2018;31, PP.1-19.

[16] Swapnil S. Bhalsagar et al. , "Performance Evaluation Of Routing Protocol Under Black hole Attack In Manet And Suggested Security Enhancement Mechanisms", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-5 March, 2019.

[17] Shashi Gurung and Siddhartha Chauhan, "A dynamic threshold based approach for mitigating black-hole attack in MANET", Wireless Networks, (2018) 24:2957–2971.

[18] A.Rajaram, Dr. S. Palaniswami, "The TrustBased MAC-Layer Security Protocol for Mobile Ad hoc Networks", International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010.

[19] Wenkai Wang and Yan (Lindsay) Sun, Husheng Li, Zhu Han, "Cross-Layer Attack and Defense in Cognitive Radio Networks", IEEE GlobeCOM, 2010