International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 9 Ver I || Sep 2018 || PP 01-09

Analysis of ExistingCosmic Dust and Black Hole Attack Avoidance Algorithms over AODV

D. Shanmugasundaram, Dr. A. R. Md. Shanavas
Assistant Professor, Department of Computer Science,Associate Professor, Department of Computer Science,Jamal MohammedCollege, Trichy.
Corresponding Author: D. Shanmugasundaram

Abstract.: *Mobile Ad Hoc Network (MANET) is one of the infrastructure less network. It is the mobile node's network. The mobility of the node causes the cosmic dust problem. It introduces lot of links break due to its mobility. So the network needs techniques to avoid the cosmic dust problem. The paper evaluates the existing techniques to avoid the above problem by the use of OmNetpp.*
Keywords: *MANET, Cosmic dust, OmNetpp.*

Date of Submission: 31-08-2018 Date of acceptance: 15-09-2018

I Introduction

Mobile ad hoc networks, named also MANETs, are formed by devices (nodes) that communicate with each other through wireless physical medium without having to resort to preexisting network infrastructure. Nodes consist of some ordinary devices such as mobile phone, laptop, PDA and personal computer that are participating in the network and are moveable. These nodes can operate as host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network. MANET have dynamic topology such that nodes can easily join or leave the network at any time. MANET have a large number of potential applications. Military uses such as connecting soldiers or other military units to each other on battlefields or establishing a new network in place of a network, which collapsed after a disaster like an earthquake. MANET is especially useful when conducting emergency and rescue operations. MANET have special features such as open communication medium, changing network topology dynamically, cooperative algorithm and lack of central monitoring and management while these features make MANET more flexible; they make it vulnerable to various types of attacks.

In mobile ad hoc network (MANET), mobile nodes are continuously moving from one location to another with a pause-time. Thus, MANET topology can change often and unpredictably. Excessive node mobility may lead to topology changes before network updates can propagate. Many protocols have been proposed for multihop[7] MANET routing to maintain best effort routes. Route stability mainly relies on route lifetime which, in turn, is related to the route length and the lifetime of each link. In large-scale MANETs, the route stability is very important . The hop count of a route may be large. If a route fails, the procedure of route rediscovery results in an increase in control overhead and end-to-end delay. In high-mobility MANETs, the fast changes in topology increase the complexity of routing. Hence, there is a need to construct a route in which each link has long lifetimes.

AODV is an efficient reactive routing protocol used in MANET, which may be influenced by black hole attack, in which a malicious node sends a fake RREP message as it has a fresh and shortest route to destination node. It is an excellent routing protocol for avoiding cosmic dust and black hole attack [5].

II AODV Routing Protocol

Ad hoc On-Demand Distance Vector AODV [8] is one of the best and popular routing protocols that is used in MANET, it establishes route only on demand. In AODV when source node has to send data to destination node, it doesn't have a valid route to it, but it broadcasts a RREQ message containing information: source IP address, source sequence number, destination IP address, destination sequence number, hop count and broadcast ID. The neighbour nodes to the source node to update their routing table accordingly and broadcast the RREQ [6]. This process is repeated until the RREQ reaches the destination node. The destination node uses the pre-establish reverse route to send back the RREP to the source node. It should be noted that source node can receive several RREPs, it chooses the one with highest sequence number for the intended destination. If several RREPs with the same highest sequence number for the same destination are received by the source node from more than one node, then the one with smaller hop count will be selected.

III Cosmic Dust Avoidance

Nodes movements result Cosmic Dust (Link Break). The stable dynamic static path (best path) between source and destination is a very difficult process. When the MANET faces the link break (Cosmic Dust Attack) during the communication, the new path discover takes more time and it introduces more overhead to the nodes which is participating in the network. In addition, it will reduce the security of the network, because the new node which is used to form the new route between the source and destination may not be an intruder. It causes not only the Cosmic Dust attack in addition it introduces Black Hole attack also.So the MANET needs a technology to avoid the Cosmic Dust Attack as well as Black Hole Attack.
This paper evaluates some of the existing techniques which are used to avoid the above problems.

IV Review of Literature

MunishWadhwa*et al.* : [1] the proposed work has special arrangement where any path which has more packet drop rate will be considered as the path having attacker node and while sharing of hash value the two nodes have not the correct hash value which will be declared malicious. Any new path, which has those attacker nodes in the intermediate list will be avoided. So that network performance can be avoided to be downgraded. In the proposed technique all the performance parameters like throughput, end to end delay, success rate and packet Delivery ratio have shown the improvement.

ArtiYadav*et al*.:[2] In our proposed work, we are calculating the distance among each participating nodes but it is the most considering the case of transmission between those nodes. In our mechanism we must calculate distance of each node and then apply multipath for sending data for destination.

The Sender waits receiving the acknowledgement of packet on basis of distance if it does not get acknowledged on calculated distance or RTT time then it sends data to next path if the same thing happens again it sends packet to the neighbour to update the distance table again with the additional the information of previous paths, so that every node can check those paths and their neighbours also if there is any problem occuring it creates boundary for those non malicious nodes and make these nodes as malicious.

Thien T. T. Le *et al*.:[3]In this paper, the proposed link scheduling algorithm with interference predicts formultiple mobile WBANs. We have shown that the Bayesian inference classifier, which is simple andhas a low computational complexity, which can be easily deployed to predict the interference state of WBANs.With interference prediction, a WBAN can obtain knowledge about its current state and its neighbourset, which results in a short link schedule amongst nearby WBANs. In addition, common scheduling isalso proposed.

It allows for multiple concurrent intra-WBAN transmissions without interference.We have also proposed a method to calculate the contention value for each WBAN in the commonscheduling considering the interference level of WBANs, enabling the signal transmission of a WBANeven with interference. The proposed LSIP improves the packet delivery ratio and network throughputremarkably with acceptable delay by overcoming the inter-WBAN interference in comparison tothe conventional scheme. Nonetheless, the negotiation between the WBAN coordinators requiresadditional energy consumption.

Xiaoqin Chen *et al*.:[4] the proposed congestion-aware routing protocol for mobile ad hoc networks (CARM). CARM utilizes two mechanisms to improve the routing protocol adaptability to congestion. Firstly, the weighted channel delay (WCD) is used to select high throughput routes with low congestion.

The second mechanism that CARM employs is the avoidance of mismatched link data-rate routes via the use of effective link data-rate categories (ELDCs). In short, the protocol tackles congestion via several approaches, taking into account causes, indicators and effects. The decisions made by CARM are performed locally.

V Proposed Work

5.1) Avoiding Cosmic and Black Hole Attack (ACBH)

AODV is one of the multiple paths [9] from source to destination. If one path fails immediately, second path will be adopted without identifying the second path individually. According to this algorithm intermediate position will be adopted by black hole node which affects more than one paths. Such paths will be adopted which has minimum number of intermediate nodes and has less sequence number than the total available sequence numbers.

Pseudo code for Avoid Cosmic and Black Hole Attack (ACBH)

```
sndRREQ();
if(hashKey())
        SndPkt();
Else
        sndRREQ();
```

5.2)Avoiding Link Break by Block Hole Attack (ALBBBH)

```
RC()
CalRoTDT() // Calulate Round Trip Delay Time value
SndPkt()// According to Round Trip Delay Time Value
if(pktAcK)
{       rsndPkt(); //remain packet send
}
Else
{
        putNMalicious(); //put node as malicious
        delEntries(); //Delete all related information
}
```

5.3) Pseudo code for Link Break Avoid (LBA) Algorithm [10]

Input: NBi(t), SFm, Ii, NIi, ts
Output: scheduled superframe
Initialize: t = 0
// Phase 1: Calculate length of superframe
Bi broadcasts {Ii, NIi} to all members in NBi(t)
For each Cj 2 NBi(t)
Receive {Ij, NIj}
Create a common list of neighbors: CI(t) = {sj(t) [si(t), Ii [Ij | j 2 NBi(t), i 2 NBj(t)}, CNI(t) = {NIi [NIj | j 2 NBi(t), i 2 NBj(t) }
End For
Calculate LCAP and LSP as in (6) and (7), respectively
TISF = LSP + LCAP
If TISF >SFm
Calculate TSPm as in (12)
Calculate Ti as in (11)
Update LSP = TSPm
End If

VI Research Methodology

Packet delivery ratio (PDR): the ratio of the number of data packet is successfully received at the destinations to the number of data packets generated by the sources.
Average end-to-end delay: the average time taken to transfer a data packet from a source to a destination.
Normalized routing control overhead: the ratio of the number of control packets to the number of delivered data packets.

VII Simulation Parameters

.Table 1 Simulation parameters

Parameter	**Value**
No. of Nodes	10-50
Protocol	AODV
Algorithms	ACBH, ALBBBH and LBA
Communication protocol	TCP, UDP
Pause Time	100 ms
Simulation time	600ms
Simulation area	600m X 600m

VIII Result and Discussion

Table 2. Comparison of different parameters for 10 nodes

Parameters (For 10 nodes)	**Ideal case**	**Cosmic Dust Attack**	**ACBH**	**ALBBBH**	**LBA**	**After removal of Cosmic Dust Attack**
Average Throughput (Kbps)	223.056	51.08	278.82	278.82	289.9728	389.316
PDR (Packet	0.496	0.1136	0.5952	0.62	0.5704	0.488

Delivery Ratio) (%)						
NRL (Normalized Routing Load) (%)	0.096	1.392	0.1152	0.12	0.1104	0.0304

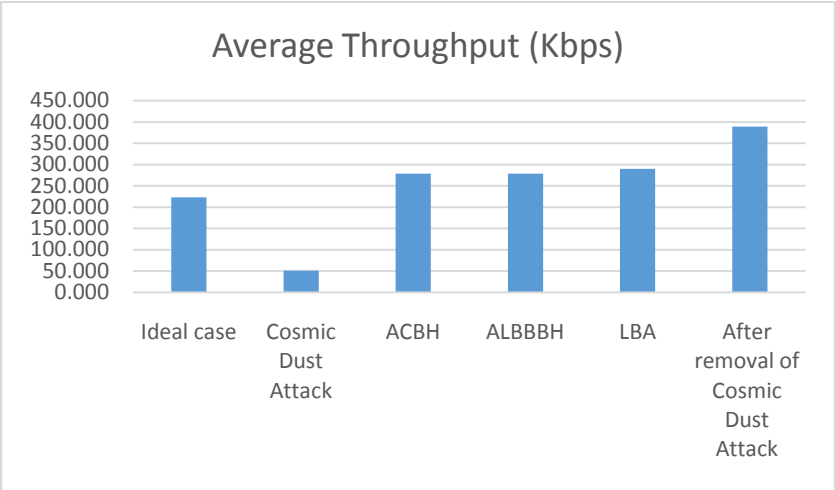

Figure 1. Average Throughput with 10 Nodes

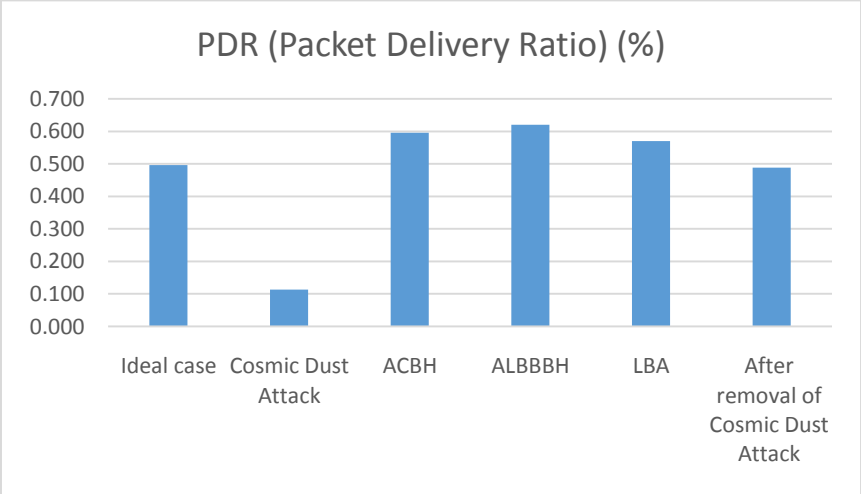

Figure 2. Packet Delivery Ratio with 10 Nodes

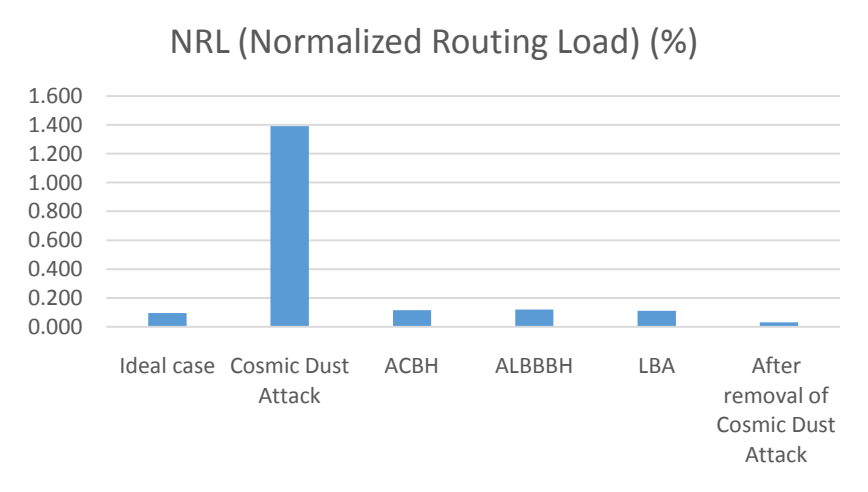

Figure 3. Normalized Routing Load with 10 Nodes

Table 3. Comparison of different parameters for 20 nodes

Parameters (For 20 nodes)	**Ideal case**	**Cosmic Dust Attack**	**ACBH**	**ALBBBH**	**LBA**	**After removal of Cosmic Dust Attack**
Average Throughput (Kbps)	446.112	102.16	557.64	557.64	579.9456	778.632
PDR (Packet Delivery Ratio) (%)	0.992	0.2272	1.1904	1.24	1.1408	0.976
NRL (Normalized Routing Load) (%)	0.192	2.784	0.2304	0.24	0.2208	0.0608

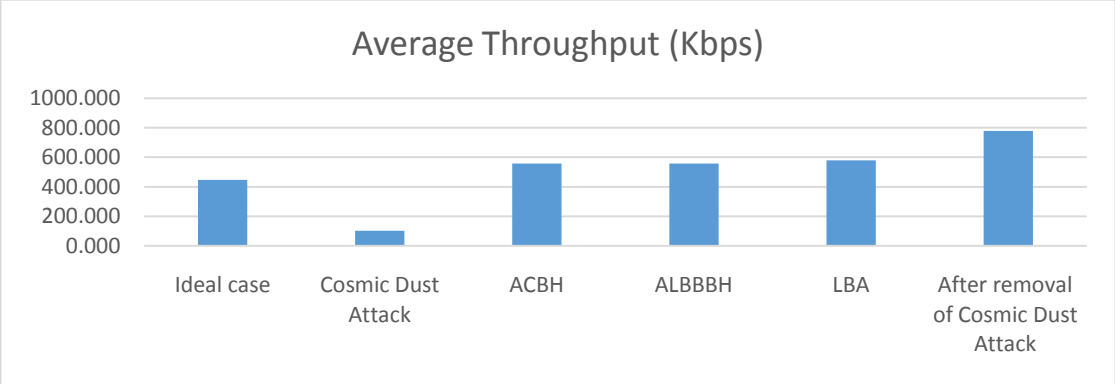

Figure 4. Average Throughput with 20 Nodes

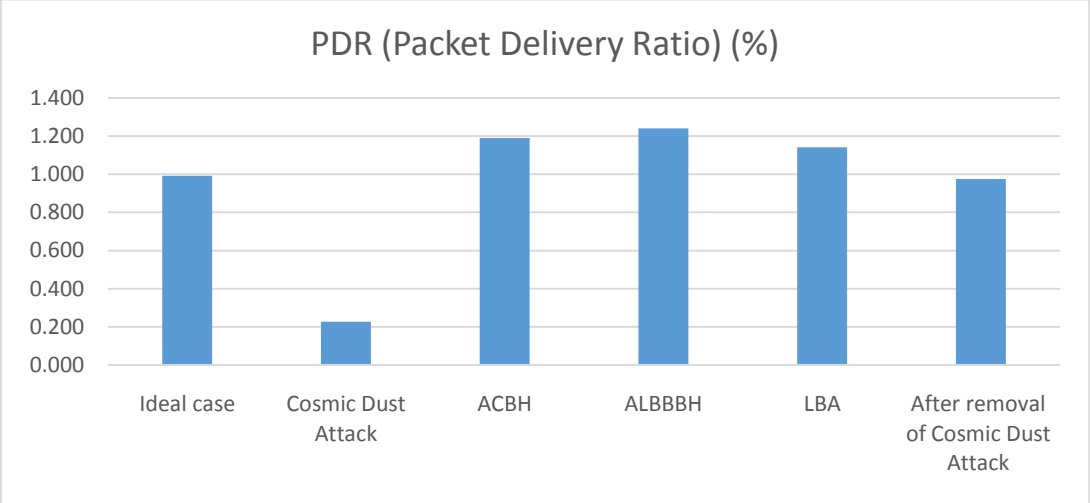

Figure 5. Packet Delivery Ratio with 20 Nodes

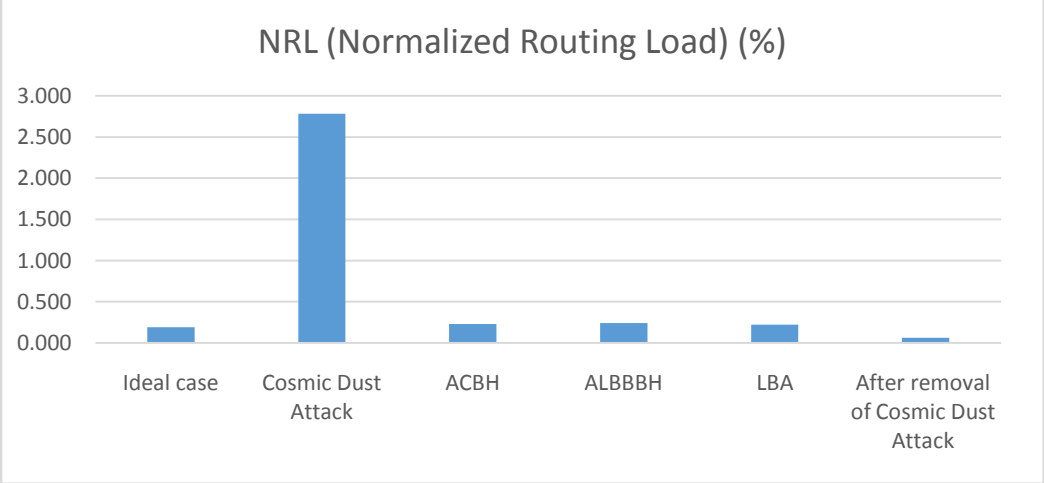

Figure 6. Normalized Routing Load with 20 Nodes

Table 4. Comparison of different parameters for 30 nodes

Parameters (For 30 nodes)	**Ideal case**	**Cosmic Dust Attack**	**ACBH**	**ALBBBH**	**LBA**	**After removal of Cosmic Dust Attack**
Average Throughput (Kbps)	669.168	153.24	836.46	836.46	869.9184	1167.948
PDR (Packet Delivery Ratio) (%)	1.488	0.3408	1.7856	1.86	1.7112	1.464
NRL (Normalized Routing Load) (%)	0.288	4.176	0.3456	0.36	0.3312	0.0912

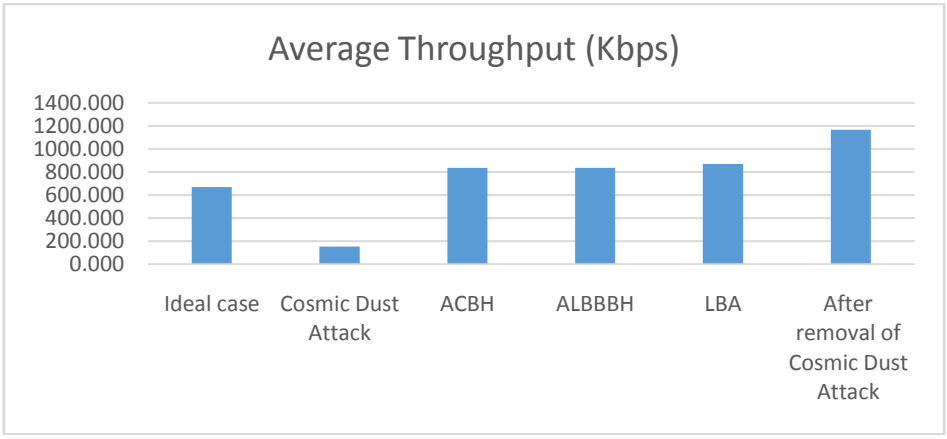

Figure7. Average Throughput with 30 Nodes

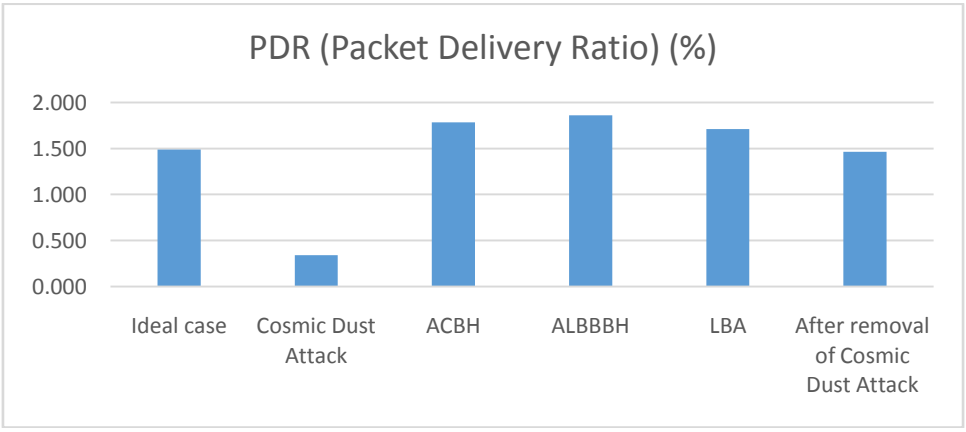

Figure 8.Packet Delivery Ratio with 30 Nodes

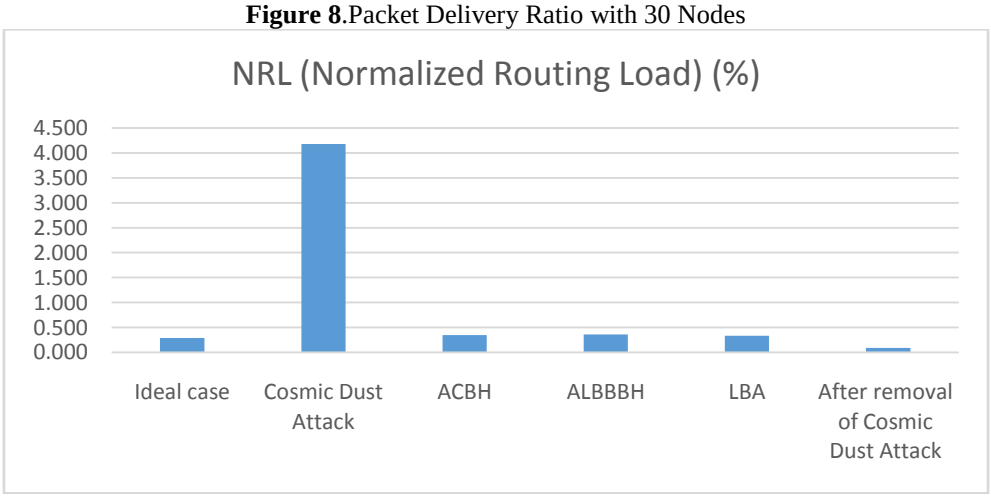

Figure 9. Normalized Routing Load with 30 Nodes

Table 5. Comparison of different parameters for 40 nodes

Parameters (For 40 nodes)	**Ideal case**	**Cosmic Dust Attack**	**ACBH**	**ALBBBH**	**LBA**	**After removal of Cosmic Dust Attack**
Average Throughput (Kbps)	892.224	204.32	1115.28	1115.28	1159.8912	1557.264
PDR (Packet Delivery Ratio) (%)	1.984	0.4544	2.3808	2.48	2.2816	1.952
NRL (Normalized Routing Load) (%)	0.384	5.568	0.4608	0.48	0.4416	0.1216

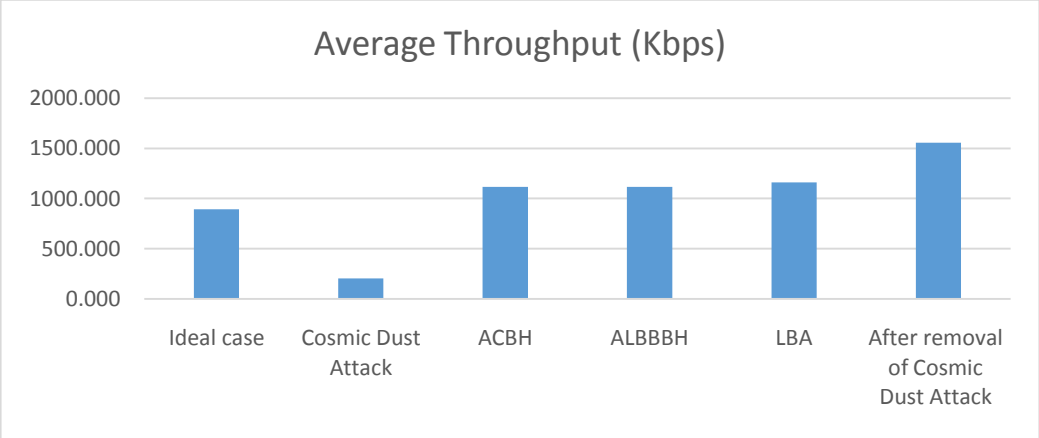

Figure 10. Average Throughput with 40 Nodes

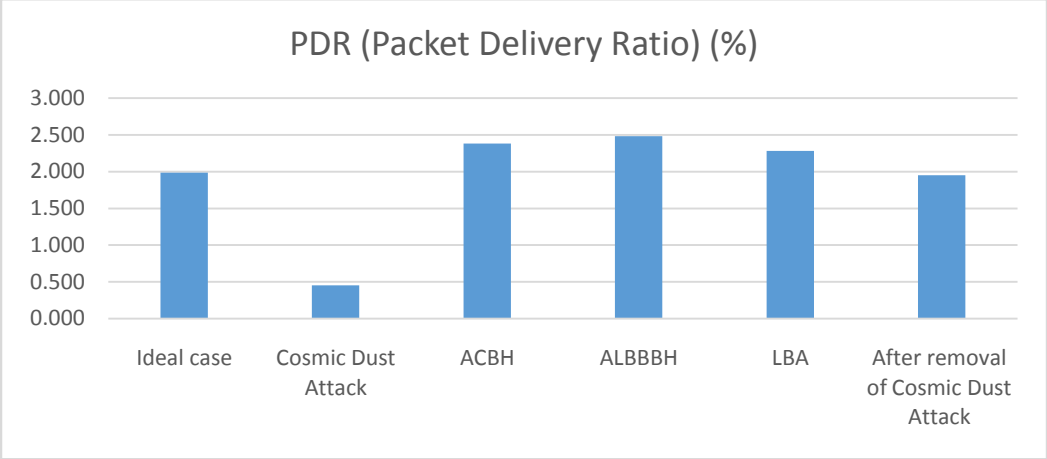

Figure 11. Packet Delivery Ratio with 40 Nodes

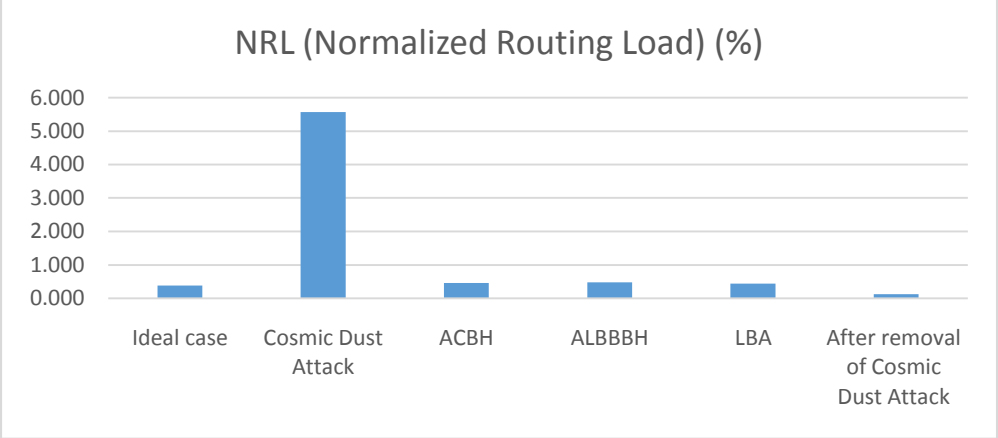

Figure 12. Normalized Routing Load with 40 Nodes

Table 6. Comparison of different parameters for 50 nodes

Parameters (For 50 nodes)	**Ideal case**	**Cosmic Dust Attack**	**ACBH**	**ALBBBH**	**LBA**	**After removal of Cosmic Dust Attack**
Average Throughput (Kbps)	1115.28	255.4	1394.1	1394.1	1282.572	1946.58
PDR (Packet Delivery Ratio) (%)	2.48	0.568	2.976	3.1	2.852	2.44
NRL (Normalized Routing Load) (%)	0.48	6.96	0.576	0.6	0.552	0.152

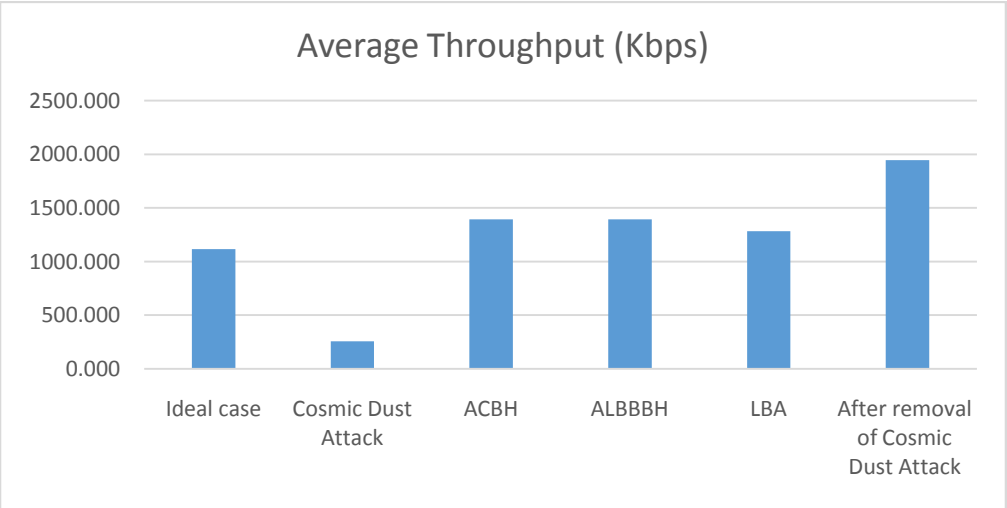

Figure 13. Average Throughput with 50 Nodes

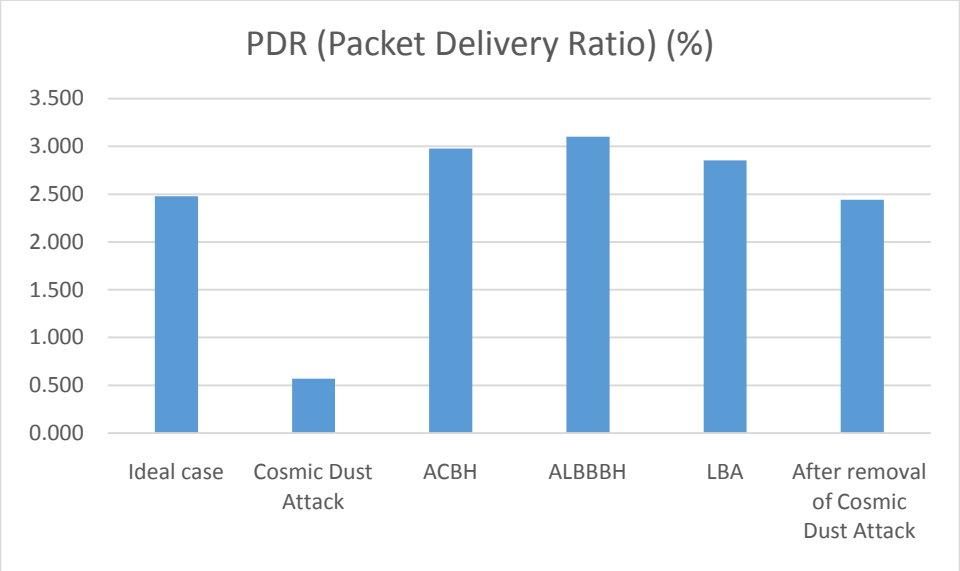

Figure 14. Packet Delivery Ratio with 50 Nodes

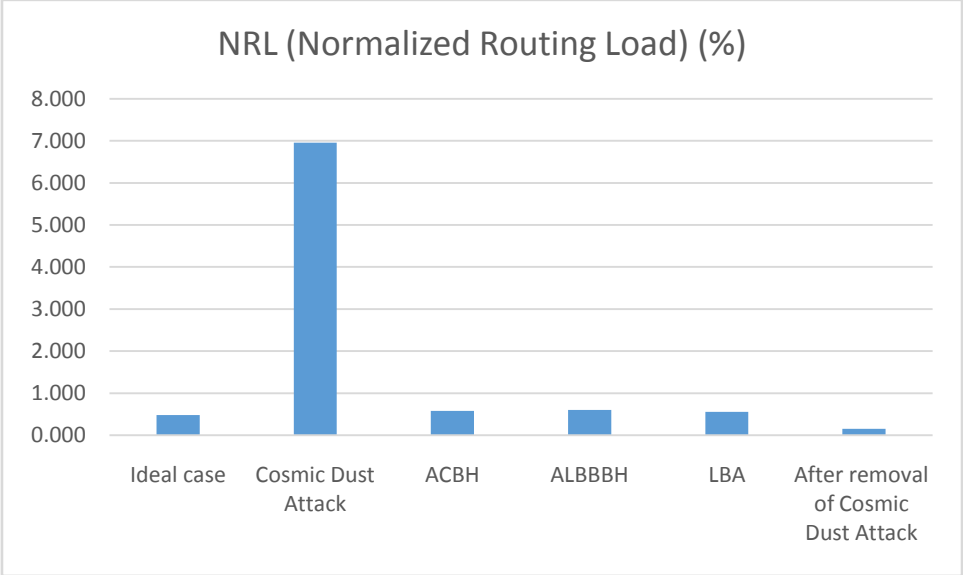

Figure 15. Normalized Routing Load with 50 Nodes

IX Conclusion

This paper has evaluated the existing three algorithms for avoiding the cosmic dust and black hole attack. The existing algorithm reduces the above problem that shows in the result and discussion. But it is not enough for the future network. In future, this work has to introduce new techniques for the further future network.

Reference

[1]. MunishWadhwa,AshwaniSethi, "Avoidance of Black Hole and Gray Hole Attack in MANET using Hash Functionbased", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, Volume: 5 Issue: 6 , pp. 1047 – 1051.

[2]. ArtiYadav, Krishna Kumar Joshi, " Improved Technique for Prevention of Black Hole Attack in Mobile Ad Hoc Network", International Journal of Advance Engineering and Research Development, ISSN :2348-6406,Volume 4, Issue 9, September -2017, pp.459-463.

[3]. Thien T. T. Le and SangmanMoh, "Link Scheduling Algorithm with InterferencePrediction for Multiple Mobile WBANs",Sensors 2017, 17, 2231; doi:10.3390/s17102231, pp. 1-18.

[4]. XiaoqinChen, Xiaoqin and Jones, Haley and Jayalath, Dhammika (2007) Congestion-Aware Routing Protocol for Mobile Ad Hoc Networks. In Proceedings IEEE 66thVehicular Technology Conference, 2007 (VTC-2007 Fall. 2007), pages pp. 21-25.

[5]. Khaled O.Basulaim, Shada Ali Aman, " Solution for Black Hole and Cooperative Black Hole Attacks in Mobile Ad Hoc Networks", Egyptian Computer Science Journal, ISSN-1110-2586, Volume 41– Issue 1, January 2017, pp 66-81.

[6]. Sanjeev K. Prasad and Karamjit Bhatia, "RSAODV :A Route Stability Based Ad Hoc On Demand Distance Vector Routing Protocol For Mobile Ad Hoc Network", International Journal of Wireless & Mobile Networks (IJWMN), ISSN: 2014.6609, Vol. 6, No. 6, December 2014, pp.113-126.

[7]. A.Poonkodi and C. MohanaPriya, " Mobile Ad Hoc Network Based Efficient Broad Casting Using Random Cast Mechanism", International Journal of Computer Science Trends and Technology (IJCST), ISSN: 2347-8578, Volume 5 Issue 6, Nov - Dec 2017, PP.28-35.

[8]. B. Karthikeyan and Dr.S.Hari Ganesh, "Encrypt - Security Improved Ad Hoc On Demand Distance Vector Routing Protocol (En-SIm AODV)", ARPN Journal of Engineering and Applied Sciences (ISSN: 1819-6608), Vol. 11, No. 2, January 2016,pp. 1092-1096.

[9]. B. Karthikeyan,Dr.S.Hari Ganesh and Dr. JG.R. Sathiaseelan, " Optimal Time Bound Ad-Hoc On-demand Distance Vector Routing Protocol (OpTiB-AODV)", International Journal of Computer Applications (ISSN:0975 – 8887), Vol. 140, No.6, April 2016,pp 7-11.

[10]. B. Karthikeyan, Dr.S.Hari Ganesh and Dr. JG.R. Sathiaseelan , "High Level Security with Optimal Time Bound Ad-Hoc On-demand Distance Vector Routing Protocol (HiLeSec-OpTiBAODV)",International Journal of Computer Science Engineering(E-ISSN: 2347-2693),Vol. 4, No. 4, April 2016, pp.156-164.

D. Shanmugasundaram "Analysis of ExistingCosmic Dust and Black Hole Attack Avoidance Algorithms over AODV "'International Journal of Engineering Science Invention(IJESI), vol. 7, no. 9, 2018, pp. 01-09