IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.7, Special Issue.1, Jan 2019 E-ISSN: 2347-2693

Detection of Blackhole Attack Using RMBOPB Based Agent

Khondekar Lutful Hassan[1], J.K. Mandal[2]* , Md Saquib Zia[3], Deepshikha Shaw[4]

[1,3,4]Dept. Of Computer science and Engineering Aliah university, Kolkata, India
[2]Dept. Of Computer science and Engineering, Kalyani University, Kalyani, West bengal, India

**Corresponding Author: jkm.cse@gmail.com*

Available online at: www.ijcseonline.org

Abstract— In this paper a novel technique has been introduce to detect black hole attack using Recursive Modulo 2 and Bitwise Operations of Paired Bits (RMBOPB) agent, where RMBOPB agent is fired from a monitoring nodes. The RMBOPB agent traverses throughout the network. If the RMBOPB agent reached to any Blackhole node then it will send the message to the monitor node for the malicious status signal to the monitor node. To implement Blackhole attack in Adhoc On Demane Distance Vector (AODV) routing protocol is taken as MANET routing protocol, and Network Simulator 2 (NS 2.34) is taken as simulation tool. Simulations are done through various node densities and various scenarios. Number of packet receive, packet delivery ratio and throughput is taken as the metric for the compassion of performance of the network. After comparing the every simulation it is seen that the proposed method detect the black hole attack in the network and increase the performance of the network.

Keywords- RMBOPB, Blackhole Attack, MANET, AODV, NS2, Wireless Security, etc

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a wireless network. It is self-configuring and infrastructure less network. Every node in the network is free to move independently and acts as a router. The various routing protocols used in the MANET are proactive, reactive and hybrid protocols. Proactive protocols are also called table driven routing protocol since each node has to maintain one or more tables to store routing information, e.g. Destination-Sequenced Distance-Vector Routing protocol (DSDV). Reactive Protocol creates routes only when required by the source node. This protocol keeps the route up till when it is required and as soon as there is no need of that route, it (route) is dismissed. Ad-hoc on Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) protocols are examples of reactive protocols. AODV is the most commonly used routing protocol. Hybrid routing protocol is the mixture of both proactive and reactive protocols, e.g. Zone Routing Protocol (ZRP). In our experiment we have chosen AODV as routing protocol.

Since wireless ad-hoc networks are self-configuring and infrastructure less, every node acting as a router, there are ample chances of vulnerability in the network. Blackhole attack is a kind of Active attack in the mobile ad-hoc network. The source node (i.e., the node which has to send some data packets to the destination node) checks for the optimum or best smallest path to deliver the data packets to the destination node. The Blackhole or malicious node intervenes and sends a false message to the source node claiming it is having the optimum path or best smallest route for the data packets to be delivered. In this way, the source node falls prey to Blackhole attack and sends data packet to it. After gaining data packets, the Blackhole drops it and so the data is destroyed.

Since MANET is wireless network without central administration, there are high risks of attack in the network which compromises the behavior and performance of the network. Blackhole attack is an active attack which reduces the efficiency of the network. In case of this kind of attack, a malicious node which is acting as a router sends false route reply message to the source node (the node which has to send data packets to the destination node), that it has the best optimum path to send data packets to the destination node. With its fake route reply, the source node becomes prey to it and sends it the data packet. The malicious node in this way gets the data packets and drops (destroys) it and hence the efficiency of the network is compromised.

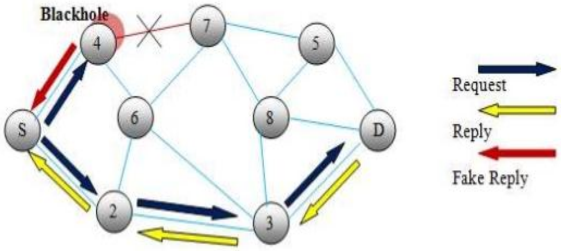


Figure 1(a): Blackhole attack

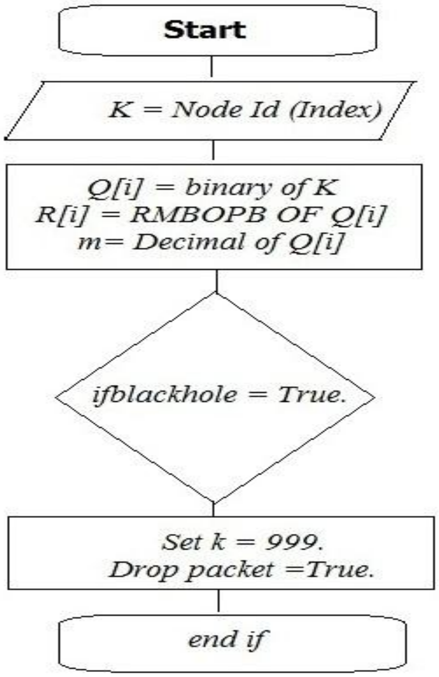
From the figure 1(a), it is seen that the Source Node (S) wants to send data packets to Destination Node (D) and asks for route reply. Node number 4, which is malicious node sends false route reply to S and gains the data packets and destroys it.

II. Proposed Technique

The proposed technique has been described here to detect Blackhole attack in MANET. A mobile agent termed as "RMBOPB" is fired from monitor node which travels through the nodes and monitors the activity of the network. It checks whether there is any unnatural or hostile behavior of the nodes are present or not. The process is followed by encryption and decryption technique based on the algorithm of Recursive Modulo 2 and Bitwise Operations of Paired Bits. This agent checks the process randomly and if it detects any malicious node, it decodes the encrypted information. After decoding the information, the RMBOPB agent compares the information and verifies it. If verification is failed, it means the node is a malicious node and Blackhole attack has been detected. For checking the normality of the network, calculations of few parameters are compared such as Number of Packets received, Packet Delivery Ratio, and Throughput before and after Blackhole attack.

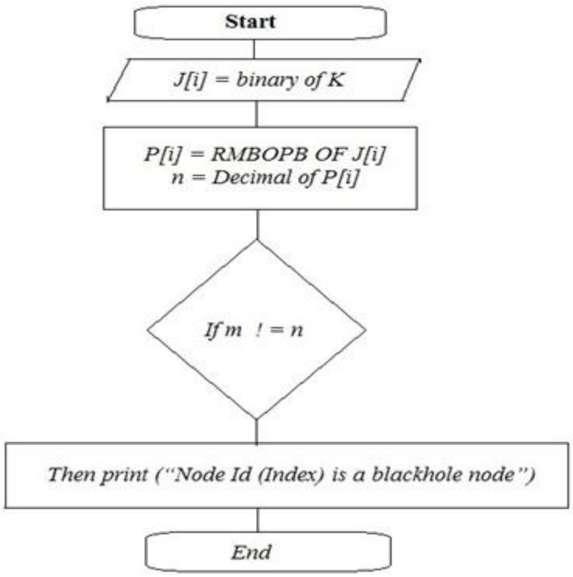
The flowchart for the procedure which is proposed in this paper is as follows:-

Procedure 1:



[Before dropping the data packet the value of m and k are to send to the monitor node with the acknowledgement.]

Procedure 2:



Now recursively module 2 and bitwise operations of paired bits (RMBOPB) technique is described below, this technique operates in two phases one is encryption phase and another is decryption phase.

The technique operates in two phases:

a. The first phase encrypts the message using Recursive Modulo-2 Operation of Paired bits of a stream.

b. The second phase encrypts the output of the first phase using bitwise Operations on Blocks.

Encryption Phase.

Let A = $q^0{}_0q^0{}_1q^0{}_2\,q^0{}_3q^0{}_4 \dots q^0{}_{n-1}$ is a block of size n which is in the plaintext form and then the 1st intermediate block $K_1 = q^1{}_0q^1{}_1q^1{}_2q^1{}_3q^1{}_4 \dots q^1{}_{n-1}$can be generated from A in the following way:

$q^1{}_0q^1{}_1 = q^0{}_0q^0{}_1 \oplus q^0{}_2q^0{}_3$

$q^1{}_2q^1{}_3 = q^0{}_0q^0{}_1 \oplus q^0{}_4q^0{}_5$

$q^1{}_iq^1{}_{j+1} = q^0{}_{i-j}\,q^0{}_{i-j+1} \oplus q^0{}_{i+j+2}q^0{}_{i+j+3}$, $0 <= i < (n-1)$, $0 <= j < (n-1)$; $\oplus$ here it is stands for XOR operation.

Now the second intermediate block of k2 of same size (n), $K_2 = q^2{}_0q^2{}_1q^2{}_2q^2{}_3q^2{}_4 \dots q^2{}_{n-1}$, can be generated by:

$q^2{}_0q^2{}_1 = q^1{}_0q^1{}_1 \oplus q^1{}_2q^1{}_3$

$q^2{}_2q^2{}_3 = q^1{}_0\,q^1{}_1 \oplus q^1{}_4q^1{}_5$

$q^2{}_iq^2{}_{j+1} = q^1{}_{i-j}q^1{}_{i-j+1} \oplus q^1{}_{i+j+2}q^1{}_{i+j+3}$, $0 <= i < (n-1)$, $1 <= j < (n-1)$; $\oplus$here it is stands for XOR operation.

The source block A is regenerated by forming a cycle, by continuing this process for a finite number of iterations, and it depends on the value of block size n. Intermediate encrypted block is called at any intermediate block in the recursive process and the input for the decryption phase can be taken as any block.

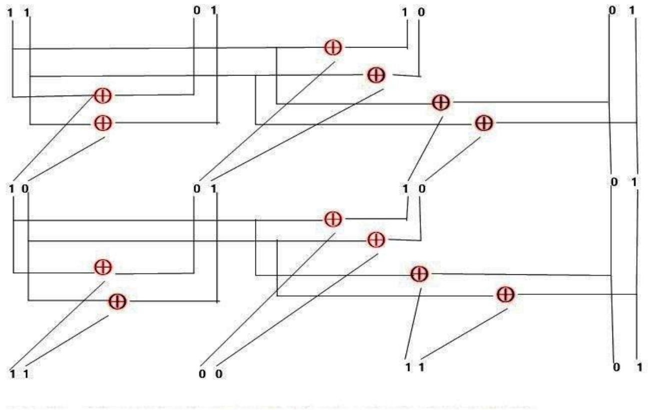


Figure.1 (b). Encryption phase of the RMBOPB technique

2.2 Decryption Phase:

Consider the encrypted message from the 1st phase (here third encrypted block is taken) as a finite number of N bits , and it is also divided into a finite number of blocks and each block containing a finite number of bits n , where, 1<= n <= N. The rules for generating cycles are given bellow:

Let A = $q^0{}_0q^0{}_1q^0{}_2q^0{}_3q^0{}_4 \ldots q^0{}_{n-1}$. Then the first intermediate block

$K_1 = q^1{}_0q^1{}_1q^1{}_2q^1{}_3q^1{}_4 \ldots q^1{}_{n-1}$ can be generated from A in the following way:

$q^1{}_0 = q^0{}_0$

$q^1{}_3 = q^0{}_3$

$q^1{}_i = q^0{}_{i-1} \oplus q^0{}_i$, 1 < i < (n-1); ⊕is here stands for XOR operation.

In the same way, the second intermediate block $K_2 = q^2{}_0q^2{}_1q^2{}_2q^2{}_3q^2{}_4 \ldots q^2{}_{n-1}$ can be generated by:

$q^2{}_0 = q^1{}_0$

$q^2{}_3 = q^1{}_3$

$q^2{}_i = q^1{}_{i-1} \oplus q^1{}_i$, 1 < i < (n-1); ⊕is here XOR operation.

If this process continues for a finite number of iterations, the source block A is regenerated forming a cycle, it is depended on the value of block size n.

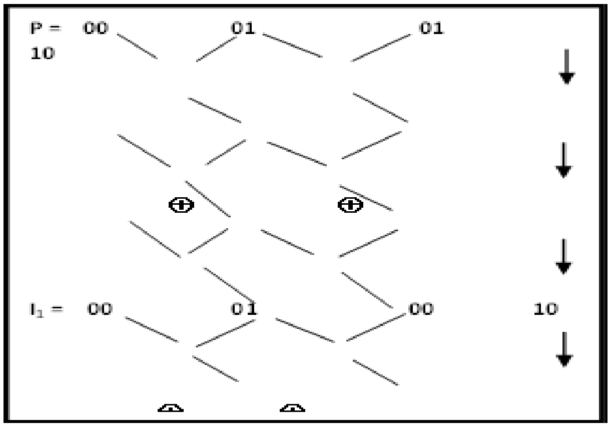


Fig. 1 (c). Decryption phase of the RMBOPB technique

III. SIMULATION ENVIRONMENT

Network Simulator 2.34 is taken as a tool for simulation purpose. The Network Simulator 2.34 is a tool of discrete event simulation in the network, and capable of simulating various types of networks. This simulator runs on Linux platform. NS2.34 consists of two languages, C++ and Otcl. C++ defines the internal mechanism of the simulation object, and Otcl set up simulation by assembling and configuring objects as well as scheduling discrete events. C++ helps to increase the efficiency of simulation and it is used to provide details of the protocols and their operation. It is also utilized for reducing packet and event processing time. With the help of Otcl we can describe different network topologies, specify the protocols and their applications and allow fast development.

To simulate NS2, a .tcl script file is required. After simulation it creates two types of file, one is trace file (tr) and another is .nam file. Trace file is used for calculation and statistical analysis, and that of .nam file is used to visualize the simulation process.

a. Simulation Parameter

Simulation parameter is divided into two categories, viz. Fixed and Variable parameter.

Table 1: Table of fixed parameter of simulations.

Routing Protocol	AODV
IFQ Length	50
Simulation Time	200 sec
Speed of Node	10 m/s
Channel Type	Channel/Wireless Channel
Radio-propagation model	Propagation/TwoRayGround
Network Interface Type	Phy/WirelessPhy
MAC type	Mac/802_11
Interface queue type	CMUPreQueue
Link Layer Type	LL
Antenna Model	Antenna/Omniantenna
Max packet in ifq	50

b.

For variable parameter, the examples are:

1. Number of Nodes: 20,25,30,35,40,45,50,60, 80,100,120, 140,200,300
2. Scenarios: 500X500, 1000X1000, 2400X2400

IV. RESULT AND ANALYSIS

For checking the effect of Blackhole attack in the network, results of few parameters were taken before and after Blackhole attack. Those parameters are number of packets received, packet delivery ratio, and throughput.

Number of Packets received: Number of packets receives implies that total number of packets is received by receiving nodes.

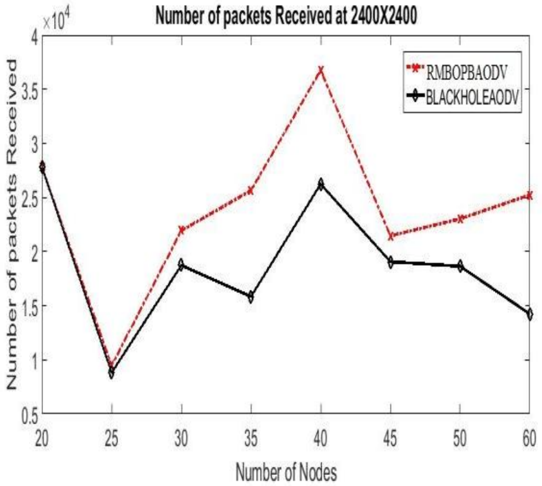


Figure 2. Number of packets receives at 2400X2400 in low node density.

From the figure 2, it is seen that at the start, the packets quantity decrease, and then increases from node number 25, while reaching node 40, again the packets quantity decrease but it again increases from node number 45 in case of AODV whereas in case of Blackhole AODV the number of packets have shown increase at only two nodes, viz node number 25 and node number 35.

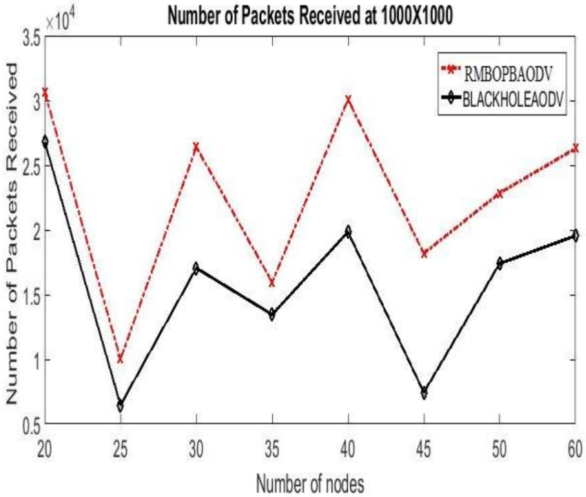


Figure 3. Number of packets receives at 1000X1000 in low node density.

From the above figure 3, we see that there is a fluctuating result for both the cases, however the number of packets received for AODV is greater than that of Blackhole AODV.

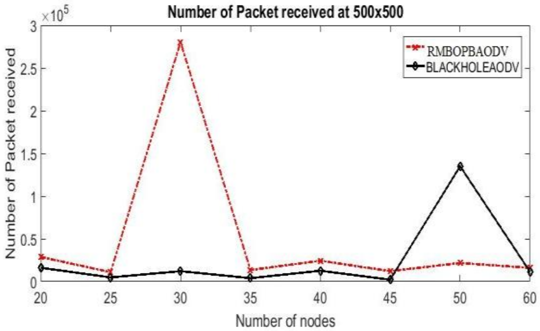


Figure 4. Number of packets receives at 500X500 in low node density.

From the figure 4, for the AODV, we can see that the no. of packets received is highest at node no. 30 whereas for Blackhole AODV, the no. of packets received is highest at node no. 50. However, the AODV graph shows rise in the starting node numbers and goes down after that while the Blackhole AODV graph shows graph rises in the ending nodes.

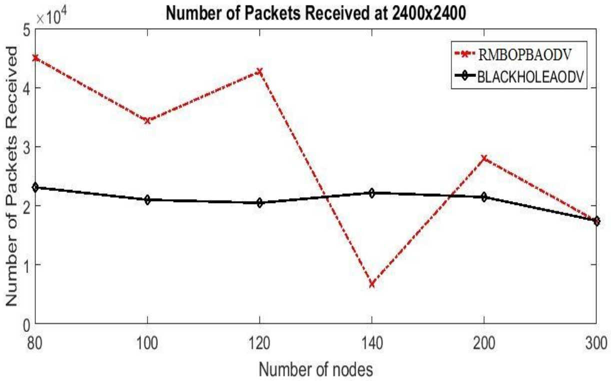


Figure 5. Number of packets receives at 2400X2400 in high node density.

The figure 5 shows that number of packets received in Blackhole AODV fluctuates at constancy, whereas the number of packets received in AODV shows a dramatic graph of decreasing and a little bit increasing.

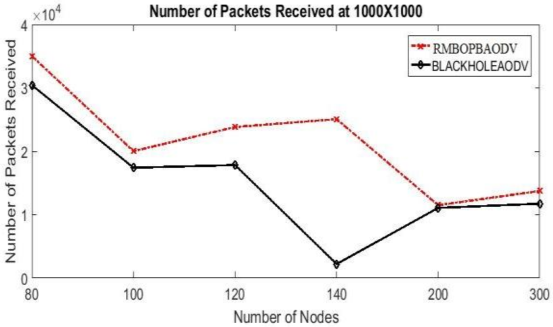


Figure 6. Number of packets receives at 1000X1000 in high node density.

From the figure 6, we can see here that at the start the number of packets received decreases up to node number 100, after that increase a little bit up to node number 140, then again decreases till node number 200 in case of AODV. Whereas in case of Blackhole AODV, the number of packet after decreasing up to node number 100, becomes constant up to 120 and then again decrease till 140, from where it shows a rise up till 300.

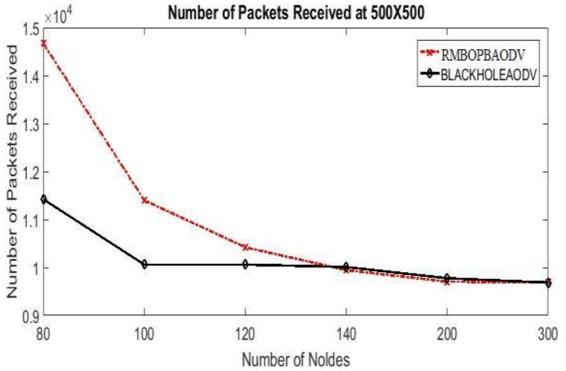


Figure 7. Number of packets receives at 500X500 in high node density.

From the figure 7, we can see that, with the increase in the number of nodes, the number of packets received decreases in both the cases. The number of packets received in the Blackhole AODV is relatively lower than that of AODV.

Packet Delivery Ratio: Packet delivery ratio implies that the ratio of number of total packets receives by the receiving nodes and number of total packets sends by sending nodes.

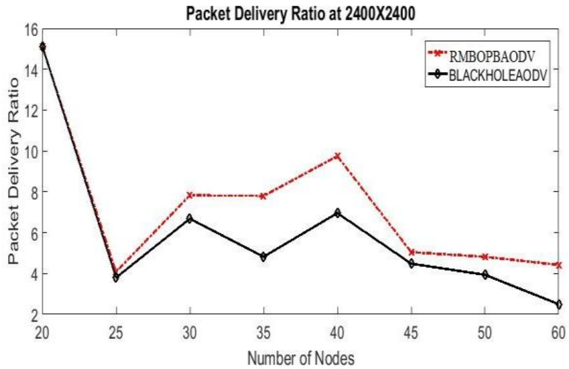


Figure 8. Packet Delivery Ratio at 2400X2400 in low node density.

From the figure 8, it is seen that in the network area 2400X2400, the packet delivery ratio at the starting point is same in both cases but they show steep decrement at the beginning. While the ratio tends to increase from node number 25 in each case, it again deviates towards lower range from node number 40.

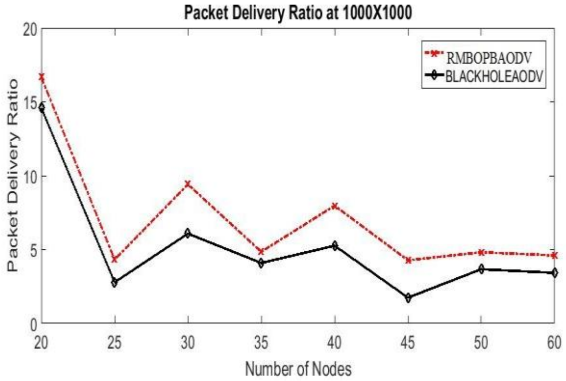


Figure 9. Packet Delivery Ratio at 1000X1000 in low node density.

From the figure 9, it is noticed that although AODV has greater packet delivery ratio, but in both the cases it is decreasing with the increase of node.

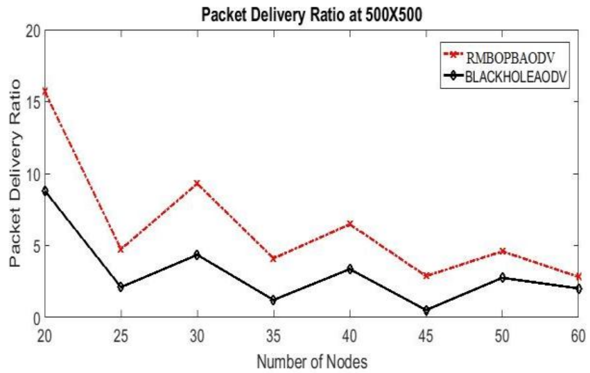


Figure 10. Packet Delivery Ratio at 500X500 in low node density.

The figure 10 shows that the packet delivery ratio is higher in the AODV than Blackhole AODV, but in both the cases, the ratio is decreasing at the interval of 10 nodes.

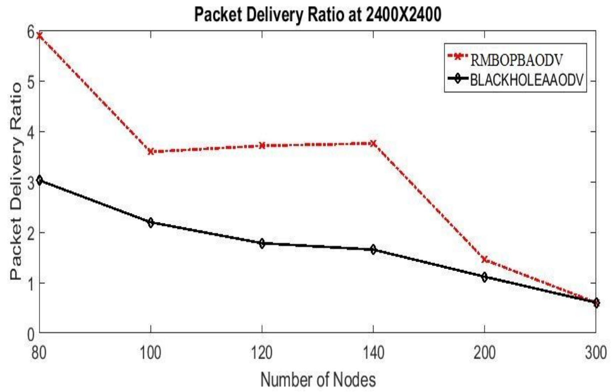


Figure 11. Packet Delivery Ratio at 2400X2400 in high node density.

From the figure 11, it is seen that while the packets delivery ratio is higher in AODV than Blackhole, the graph shows that AODV has a constancy of ratio up to a certain limit, whereas the Blackhole graphs show that there is always a decrement of ratio with the increase in number of nodes.

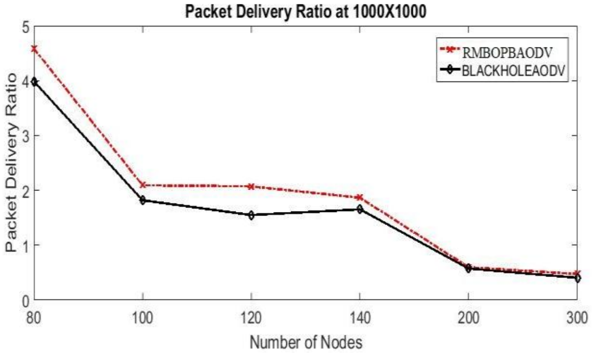


Figure 12. Packet Delivery Ratio at 1000X1000 in high node density.

From the figure 12 we can say that with the increasing number of nodes the packet delivery ratio is decreasing in both the cases. However the ratio at the starting node number is greater in AODV than Blackhole AODV.

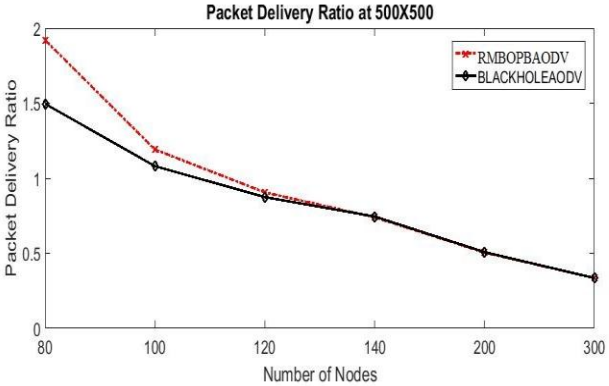


Figure 13. Packet Delivery Ratio at 500X500 in high node density.

From the figure 13, it can be noticed that the packet delivery ratio is higher in AODV but in both the cases, the graph shows deviation or decrement of the ratio with the increase in number of nodes.

Throughput: Throughput implies that the rate of data transferred in the network.

From the figure 26 it is seen that at node number 40 both AODV and Blackhole AODV have maximum throughput .Once again the AODV has higher throughput than Blackhole AODV

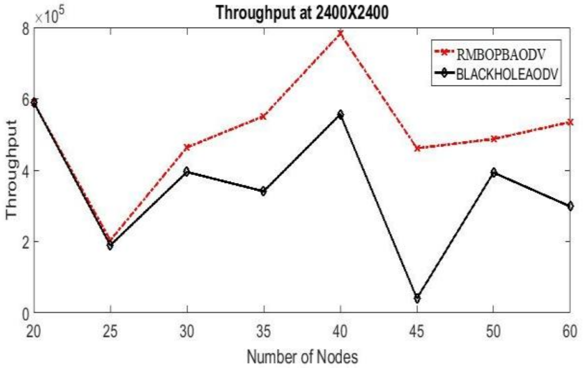


Figure 26. Throughput at 2400X2400 in low node density.

.

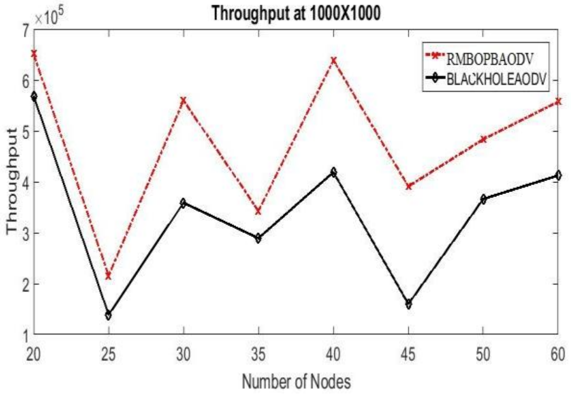


Figure 27. Throughput at 1000X1000 in low node density.

From the figure 27 it is seen that AODV has maximum throughput in this network area. However the graph shows fluctuating result in each case.

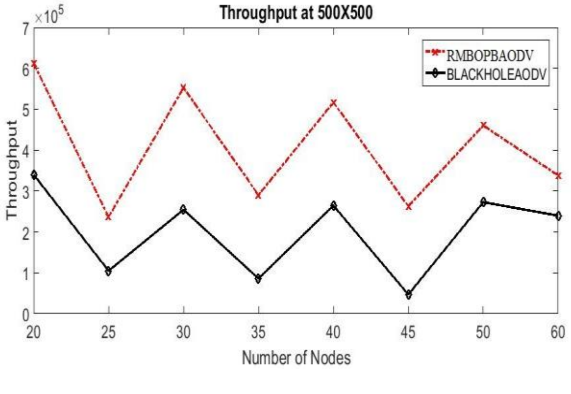


Figure 28. Throughput at 500X500 in low node density.

From the figure 28 it is seen that although the throughput is fluctuating in both the cases, it is always higher in AODV in comparison to Blackhole AODV. With the increase in number of nodes the throughput is decreasing in each case. In both cases, the throughput is maximum at node number 20.

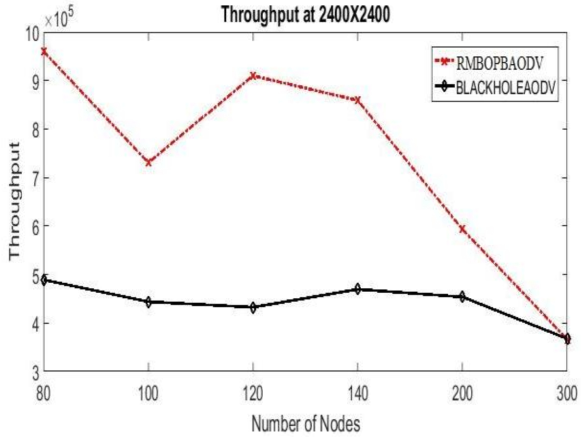


Figure 29. Throughput at 2400X2400 in high node density.

From the figure 29 it is seen that with the increase in number of nodes, the throughput of AODV decreases in this case although it shows a rise at node number 100. In case of Blackhole AODV there is a bit rise in throughput at node number 120, but it is decreasing with increasing nodes. In both cases the minimum throughput is at the last node i.e., node number 300.

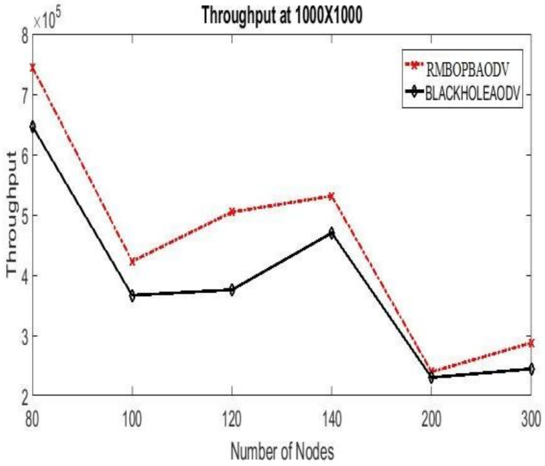


Figure 30. Throughput at 1000X1000 in low node density.

From the figure 30 it is seen that with increase in node number the throughput is decreasing for both the cases. However there is a rise at node number 100 but again the throughput falls from node number 140. Again the AODV is having maximum throughput than Blackhole AODV.

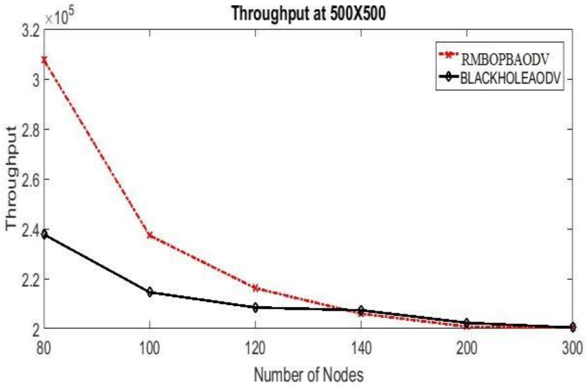


Figure 31. Throughput at 500X500 in high node density

From the figure 31 we can observe that with increase in number of nodes the throughput is decreasing. AODV has highest throughput at the starting node than Blackhole AODV.

V. CONCLUSIONS

In this paper, it has been tried to detect the blackhole attack with the help of RMBOPB based agent. This agent was triggered from the index node and it travelled through the nodes within the network monitoring their activities and detected the malicious node, then verified the information and confirmed the Blackhole attack. The technique was based on encryption-decryption method. In the first phase, an input was taken, then performing XOR operation on it a finite number of times we got it encrypted. Then the encrypted information was taken as input in the second phase and again XOR operation was performed a finite number of times and the information was decrypted. After that the input was compared with the output (i.e, the decrypted information). When it was seen that the output was different from the input, Blackhole attack was confirmed. Also we have noticed from the results the difference on the performance of the network before and after Blackhole attack.

ACKNOWLEDGMENT *(HEADING 5)*

The authors are thankful to their colleague for their support and especially thankful to Aliah University which gave them this opportunity to study the subject and their resources were used accordingly.

REFERENCES

[1] C.Siva Ram Murthy and B.S manoj" Ad Hoc Wireless networks architecture and protocols" Pearson Education India 2005.

[2] PrasantMohapatra, Srikanth Krishnamurthy "Ad hoc networks: technologies and protocols" Springer 2005.

[3] Chai-KeongToh "Ad hoc mobile wireless networks: protocols and systems " Prentice Hall.

[4] Amitava Mishra "Security and Quality of Service in Adhoc Wireless Network", Cambridge University Press .

[5] Sarkar, S.K., Basavaraju, T.G., Puttamadappa, C.: Ad hoc Mobile Wireless Networks: Principles, Protocols and Applications.Auerbach Publications (2008).

[6] TeerawatIssariyakul, EkramHossain "Introduction to Network Simulator NS2" Springer (2009)

[7] Marc Greis' Tutorial http://www.isi.edu/nsnam/ns/tutorial/208 Computer Science & Information Technology (CS & IT) (last visited on 15/5/2017 at 15:02 IST).

[8] Mubashir Husain Rehmani, Sidney Doria, and Mustapha RedaSenouci "A Tutorial on the Implementation of Ad-hoc On Demand Distance Vector (AODV) Protocol in Network Simulator (NS-2)"

[9] Mandal, J. K.,Dutta, S.,Mal, S., "A Multiplexing Triangular Encryption Technique – A Move Towards Enhancing Security in E-Commerce, Proc. of Conference of Computer Association of Nepal, December, 2001.

[10] Mandal, J. K., Chatterjee R, "Authentication of PCSs with Triangular Encryption Technique", Proceedings of 6th Philippine Computing Science Congress(PCSC 2006), Ateneo de Manila University, Manila, Philippine, March 28-29,2006.

[11] Dokurer, S. Ert, Y.M. ;Acar, C.E." Performance analysis of ad-hoc networks under black hole attacks", Proceedings. IEEE. pp. 148 – 153, 2007.

[12] Perkins, C.E., Royer, E.M., "Ad-hoc on-demand distance vector routing", www.cs.ucsb.edu/~ravenben/classes/papers/aodv-wmcsa99.pdf (last visited on 18/5/2017 at 09:45 IST).

[13] Deng, H., Li, W., Agrawal, D., "Routing Security in Wireless Ad Hoc Networks" IEEE Communication Magazine (October 2002) pp. 70-75.

[14] Al-Shurman, M., Yoo, S., Park, S., "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference (2004) pp. 96-97.

[15] Mishra, A., Nadkarni, K., Patcha, A., "Intrusion detection in wireless ad-hoc networks", IEEE Wireless Communications, February 2004, pp. 48-60.

[16] MangeshGhonge, Prof. S. U. Nimbhorkar, "Simulation of AODV under Blackhole Attack in MANET" IJCSIR, Volume 2, Issue 2, February 2012.

[17] Johnson DB, Maltz DA: Dynamic Source Routing in Ad Hoc Wireless Networks. In Mobile Computing. Volume 353. Edited by Imielinski T, Korth H. Kluwer Academic Publishers; 1996:153–181. 10.1007/978-0-585-29603-6_5.

[18] Park V, Corson S: Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification. Internet Draft, Internet Engineering Task Force MANET Working Group 1998.

[19] Deng H, Li W, Agrawal DP: Routing Security in Wireless Ad-hoc Networks. IEEE Communications Magazine 2002,40(10):70–75. doi: 10.1109/MCOM.2002.1039859. 94 .

[20] Sun B, Guan Y, Chen J, Pooch UW: Detecting Black-hole Attack in Mobile Ad Hoc Networks. Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22–25 April 2003.

[21] Al-Shurman M, Yoo S-M, Park S: Black Hole Attack in Mobile Ad Hoc Networks. Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2–3 April 2004.

[22] Tamilselvan L, Sankaranarayanan V: Prevention of Blackhole Attack in MANET. Paper presented at the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27–30 August 2007.

[23] Djenouri D, Badache N: Struggling Against Selfishness and Black Hole Attacks in MANETs. Wireless Communications & Mobile Computing 2008,8(6):689–704. doi: 10.1002/wcm.v8:6.

[24] Kozma W, Lazos L: REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16–18 March 2009.

[25] Raj PN, Swadas PB: DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET. International Journal of Computer Science 2009, 2: 54–59. doi: abs/0909.2371.

[26] Jaisankar N, Saravanan R, Swamy KD: A Novel Security Approach for Detecting Black Hole Attack in MANET. Paper presented at the International Conference on Recent Trends in Business Administration and Information Processing, Thiruvananthapuram, India, 26–27 March 2010.

[27] Mistry N, Jinwala DC, IAENG, Zaveri M: Improving AODV Protocol Against Blackhole Attacks. Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17–19 March, 2010.

[28] Su M-Y: Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems. IEEE Computer Communications 2011,34(1):107–117. doi:10.1016/j.comcom.2010.08.007.

[29] Oliveira R, Bhargava B, Azarmi M, Ferreira EWT, Wang W, Lindermann M: Developing Attack Defense Ideas for Ad Hoc Wireless Networks. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009.

[30] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K: Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23–26 June 2003.

Authors Profile

Mr. Khondekar Lutful Hassan pursed Bachelor of Technology from Govt College of Engineering and Ceramic Technology, and Master of Technology from University of Calcutta, Calcutta, India in the year of 2010 and 2012 respectively. Currently he is working as an assistant professor in the Department of Computer Science and Engineering, Aliah University, Kolkata, India. His research interest is Mobile Ad-hoc Network, Network Security etc.

.

Professor Jyotsna Kumar Mandal Completed his M.Sc. in Physics from Jadavpur University in 1986, M.Tech in Computer Science from University of Calcutta, he was awarded PhD.(Engg.) in Computer Science & Engineering by Jadavpur University in 2000. Presently he is working as Professor of Computer Science & Engineering and former Dean, Faculty of Engineering, Technology and Management, Kalyani University, Kalyani, Nadia, West Bengal for two consecutive terms. He started his career as lecturer at NERIST, Arunachal Pradesh in Sept., 1988. He has teaching and research experience of more than 30 years. His area of research is Coding theory, Data and Network Security; Remote Sensing & GIS based Applications, Data Compression, Error correction, Visual Cryptography and steganography. He has produced 22 Ph. D degrees. He is life member of Computer Society of India since 1992, CRSI since 2009, ACM since 2012, IEEE since 2013 and Fellow member of IETE since 2012, Executive member of CSI Kolkata Chapter, Vice Chairman(Elect. 2015-2016). He has chaired number of sessions in various International Conferences. He is reviewer of various International Journals and Conferences, since 1994. He is chief editor of various National/International Journals of AIRCC, editors of various National/International Conferences and proceedings. He has published 11 books and more than 400 articles in various national and international journals and conference proceedings.

.

Mr Md Saquib Zia pursued Master of Computer Applications from Aliah University, Kolkata, India in the year of 2017. Currently he is pursuing Master of Technology in the department of Computer Science and Engineering from Aliah University, Kolkata, India. He has interest in the field of network security, Mobile Ad-hoc Network etc.

Ms. Deepshikha Shaw pursued Master of Computer Applications from Aliah University, Kolkata, India in the year of 2017. Currently she is working as an Android developer in Android Developer at Onqanet Technologies. Her research interest is Mobile Ad-Hoc Network , Network Securityetc etc.