IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 5, Ver. II (Sep. – Oct. 2015), PP 01-06
www.iosrjournals.org

Combating against Byzantine Attacks in MANET using Enhanced Cooperative Bait Detection Scheme (ECBDS)

Anuj Mehta, Ravina Saini
(Cse ,Skiet kuk , India)
(Cse ,Skiet kuk , india)

Abstract: *Mobile Ad-hoc(MANET) is an accumulation of versatile, decentralized, and self composed nodes. The distributive nature, base less & element structure make it a simple prey to security related dangers. The security dangers may change from dynamic mimic threats to passive eves-dropping. Actualizing Security & alleviating dangers in MANET has Significant difficulties on the grounds that its dynamic properties make it harder to be secured than alternate sorts of static systems. Implementing Security & mitigating threats in MANET has Significant challenges because its dynamic properties make it harder to be secured than the other types of static networks. We are using Enhanced CBDS technique here, so that we can save our network from the Byzantine attacks. This dissertation proposes an enhanced cooperative bait detection scheme (ECBDS) to combat the byzantine attack over MANET.This plan combine the proactive and receptive resistance building design in MANET by utilizing the virtual and non-existent destination location to trap the malicious nodes creating Byanzine attack. Implementation will be done using Mat lab and result will be shown on the basis of energy consumption of nodes and QoS parameters like throughput and delay etc.*

Keywords: *MANET, byzantine attack, cooperative bait detection scheme, Energy, Quality of service (QoS)*

I. Introduction

A MANET is a type of ADHOC network that can change locations and configure itself on the fly. Because MANET are mobile , They use wireless connection to communication to various network. MANET is a network where mobile works as node and it is wireless, infrastructure-less network in which nodes can move freely and can change their positions also. It is wireless, so it needs more security than the wired network._Ad-hoc networks do not rely on any pre-established infrastructure, so therefore they can be even deployed on places with no infrastructure. So it is useful in disaster recovery situations. Ad-hoc networks are helpful in conferences where people participating in conference can form a temporary network without engaging in services of any pre-existing network. Mobile Ad-hoc Network (MANET) is an ad-hoc network but each ad-hoc network is not a mobile network. Mobile Ad-hoc Network (MANET) is a self-constructing mobile network in which each device is free to move independently in any direction & change its links to other devices frequently.

II. Literature Survey

2.1 Related Work

This chapter gives an overview of the related research that has been done regarding Attacks in MANET. In this chapter, various research papers include introduction to MANET and attacks, protocols in MANET and problem and approach to apply the ECBDS to improve the discarding of malicious. These collectively have helped me to extract the dissertation. Some of these are as following:

In this paper [1] , author attempt to tackle the issues of black hole and gray hole attack brought by malicious nodes by planning a Dynamic Source Routing (DSR) system known as Cooperative Bait Detection Scheme (CBDS). It joins the benefits of both proactive and reactive discovery plans to identify malicious nodes as proactive scheme maintain fresh list of destination and maintaining a strategic distance from attack in intital stage and reactive Scheme used when recognition nodes detect noteworthy drop in conveyance proportion..It accomplishes its objective with Reverse following strategy. Cooperative Bait Detection scheme is proposed to distinguish malicious nodes in MANET for the black hole and gray hole attack. Helpful Bait Detection Scheme (CBDS) has been utilized to handle black hole and gray hole attack brought by malicious nodes [1].it accomplishes its objective with Reverse following strategy.

In this paper [2], authors proposed self organized algorithm. Self organizing algorithms are responsible for no. of solutions to the management of MANETs. Best nodes are chosen to act as leaders and the tasks are being assigned to them. selfish nodes act as mischievously with a specific end goal to maintain a strategic distance from being chosen as leaderas they are not inspired by serving different nodes.if we chosen one time malicious nodes as leader then it will launch the Denial of Service(DOS) attack which may lead the problem issue in system working.

In self-organizing mechanism the nodes participating cooperates with each other in detecting the malicious leader. The mechanism declares the malicious behaving leader while protecting normal behaving to be declared as malicious one. The mechanism is applicable to every leader based network and is even applicable to & effective for large MANETs.

III. Proposed Work

3.1 CBDS (Cooperative Bait Detection Scheme)

CBDS is a techniques to detect the malicious nodes in MANET for the gray hole and black hole.it merge the Advantages of both Proactive and Reactive schemes to detect the malicious nodes in network. Proactive detection scheme maintain the fresh list of destination and their routing table by periodically changing the table and Reactive scheme start only when route on demend in which there is no need of updating the routing table .CBDS is used only to detect the malicious node Neither prevent the node .Sometimes if the packet delivery ratio of the node below the threshold value then it consider the normal node as malicious node. It achieve its goals with reverse tracking.

3.2 Enhanced CBDS Technique

ECBDS scheme is such and detection and prevention scheme that prevent a malicious node which disturb the normal functioning of the network . it will be used to detect and prevent malicious node from launching various black hole and gray hole. it is set of intermediate node that is work between sender and receiver. It utilize the address of the adjacent node.

There are two phases of ECBDS:

ECBDS detection phase

ECBDS prevention phase

ECBDS Detection Phase: it techniques detect the malicious node from launching various black hole and gray hole. it also combine the advantages of proactive and reactive scheme .In that scheme source node randomly cooperate with adjacent node. Source node send randomly bait RREQ. if the RREQ is not from desired destination or intermediate node then trace which node sends back the RREP according to RREP packet's Record address field .

After that malicious node is detected by source node and message is broadcast to all other nodes in the network. it also use to reverse tracing techniques to detect the malicious node. it is use for the detection of Byzantine attack. It will detect as if the acknowledgment is not received by sender in specific time.

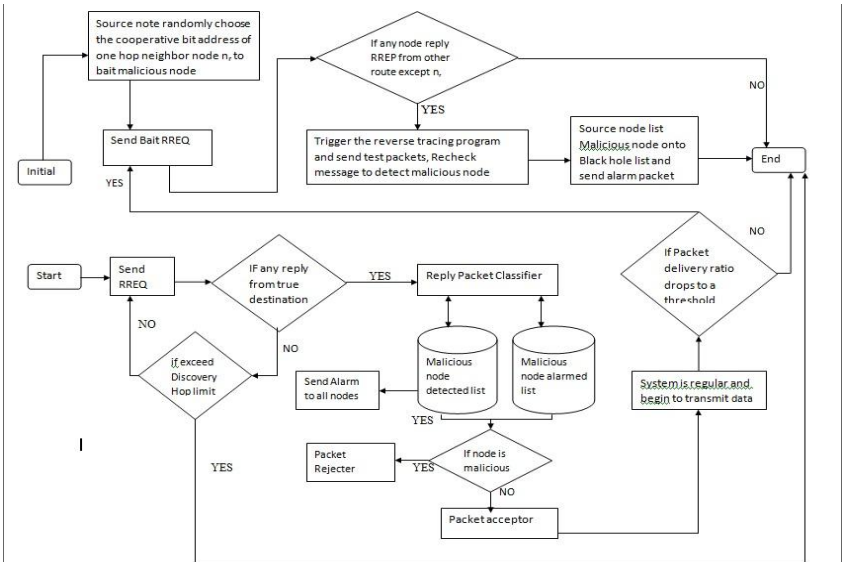

Fig. 1 Flow chart of ECBDS (Detection)

ECBDS Prevention Phase: After the identification of malicious node, we begin the directing procedure. In the ECBDS prevention stage, the most shortest path is picked among all the beforehand calculated paths. These ways are additionally checked again for any malicious node. On the off chance if any Malicious node occur, then alarm packet is send to the other nodes in the system and the path is rejected. This Process is rehashed until the alarm will be gotten by the destination nodes. it scheme increase the system throughput.

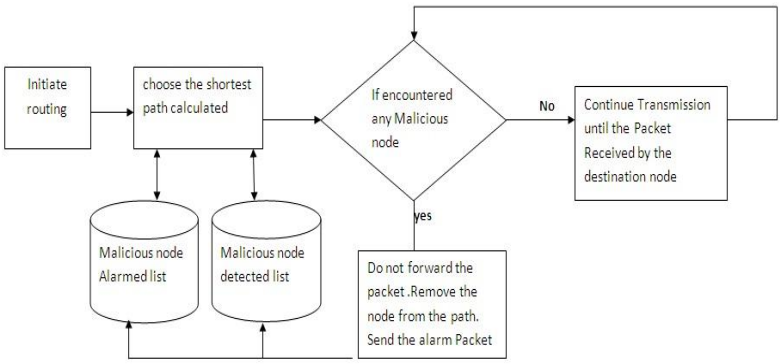

Fig. 2 Flow chart of ECBDS (Prevent

IV. Simulation and Result

The performance of CBDS and ECBDS has been analyzed with varying Number of Rounds and Adaptability to Balance Energy of nodes. The parameters used for simulation are summarized in Table 5.2 and positioning of nodes. Initial position of nodes in the network is shown in Figure 5.7. The performance metrics comprises of various parameters are discussed.

Table 1 Simulation Parameters

Parameters	Values
Number of Nodes	>40
Environment Size	400x400
Source Position	Dynamic
Initial Energy of Each Node	0.5 Unit
Simulator	MATLAB 2013
Operating System	Windows7

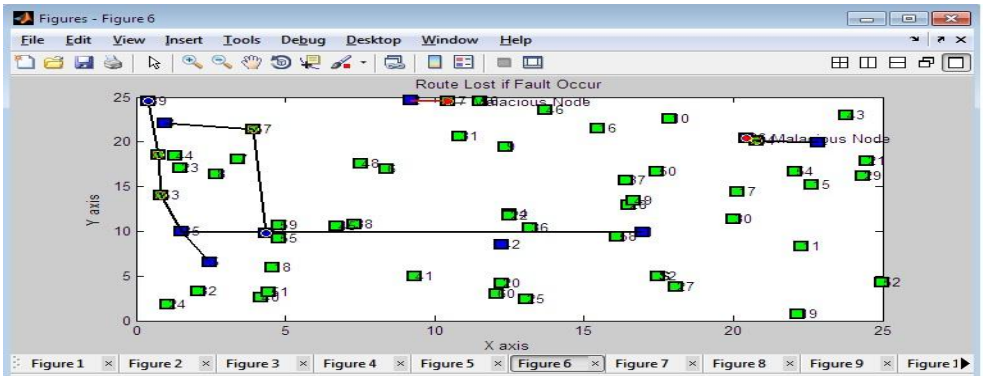

Fig. 3 Implementation of CBDS

Figure 3 shows the CBDS scheme.The route is lost when the malicious nodes get the packet. Only alarm packet is broadcasted.

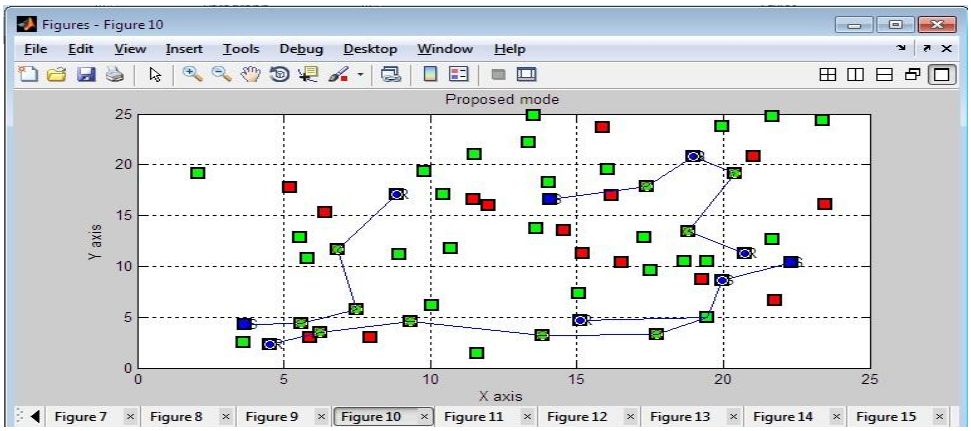

Fig. 4 Proposed modes (ECBDS)

Figure 4 shows how byzantine attack is being prevented by ECBDS Scheme. So nodes does not send data via malicious node as they detect the malicious nodes and avoid them via keeping record of node in black list. Moreover all other nodes are broadcasted physical and MAC address of malicious node on detection. This detection is purely on basis of symptoms of byzantine attack and Resource Consumption attacks .

V. Result

The goal of this implementation is to make communication more reliable then Basic CBDS Approach thus preventing Byzantine Attack. Basic CBDS does not provide any guarantee about data delivery but the ECBDS ensures better data delivery without any loss. Both the CBDS and ECBDS are analyzed on the basis of different parameters as follows:

Throughput

Throughput is the ratio of total number of delivered or received data packets per unit simulation time .In ECBDS throughtput is high than CBDS . CBDS depicts the value of throughput which is again improved by ECBDS.

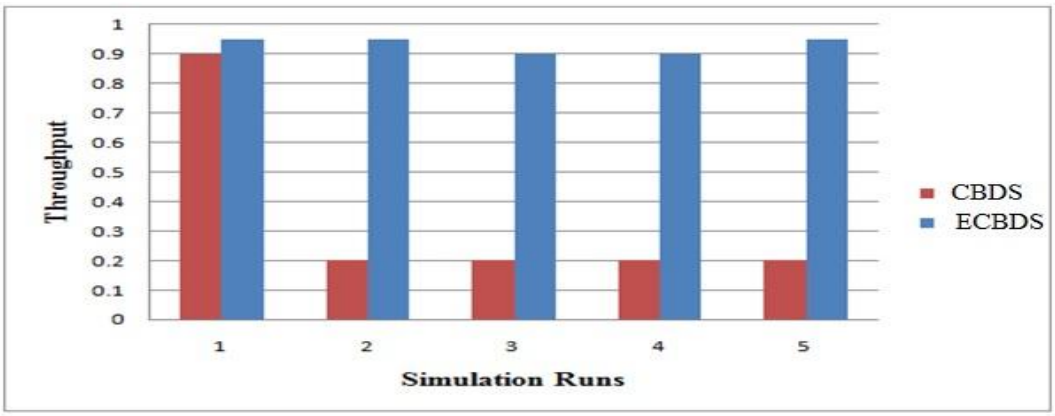

Fig. 5 Throughtput comparison

Throughput Comparison

The throughput is usually measured in bits per second (bps), and sometimes in data packets per second or data packets per time slot. Throughput is the rate of successful message delivery over a communication channel. While in case of ECBDS the throughput is much greater than basic CBDS. So, implementing ECBDS throughput increase by 67% on comparing with Basic CBDS.

Packet Delivery Ratio

Packet Delivery Ratio is the ratio of total number of packets delivered to the total number of packets sends to the destination.

PDR = ∑ Number of packet receive / ∑ Number of packet sent

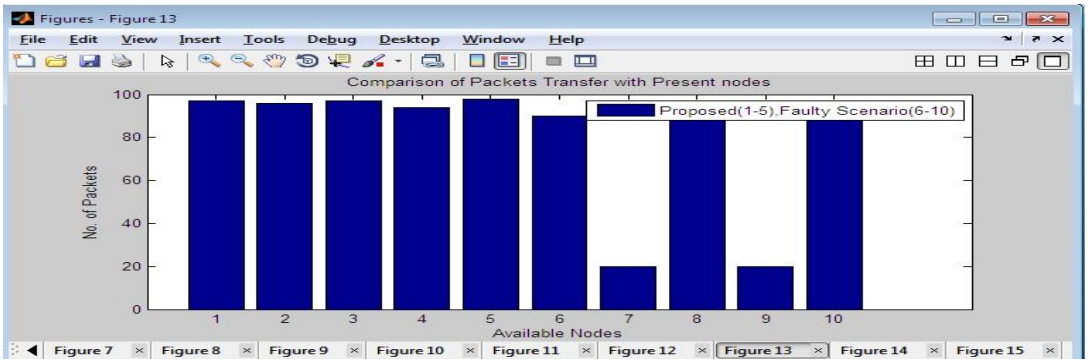

Fig. 6 Packet Delivery Ratio

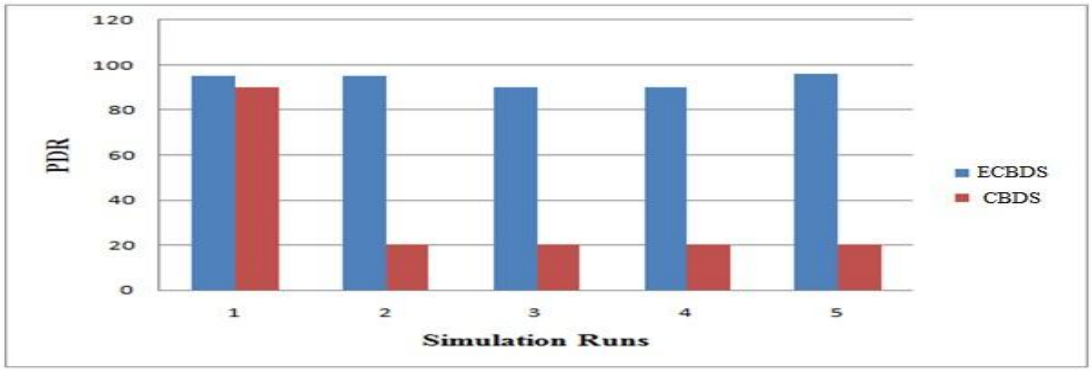

Fig. 7 Packet Delivery Ratio Comparison

Figure 7 shows comparison between Packet delivery ratio of CBDS and ECBDS. Packet delivery ratio in case of ECBDS is greater than CBDS.

Energy Consumption

Energy consumption is the ratio of the remaining energy provided by the available nodes to the total energy of nodes.

Energy Consumption=∑ remaining energy provided by available nodes/∑ total energy of nodes

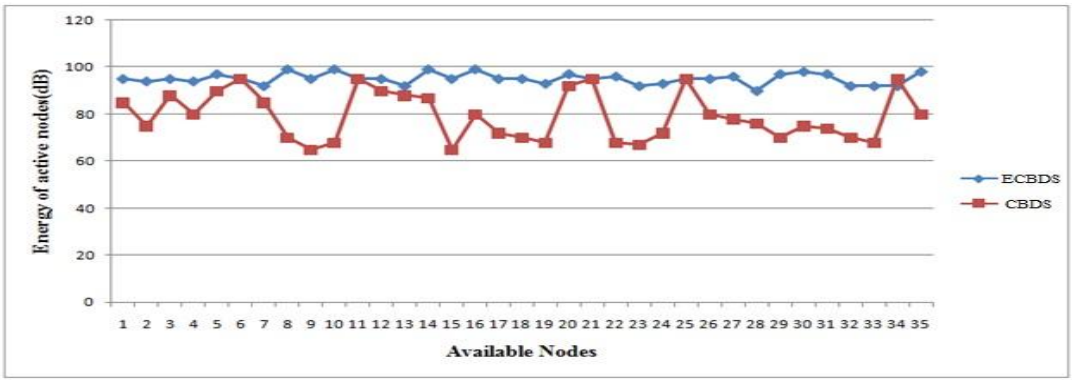

Fig 8 Energy Consumption Comparison

Figure 8 shows the energy consumption in ECBDS mode by the non malicious nodes. The energy consumption is less in the proposed method as compared to CBDS scheme as the attacks will not only be detected but also prevented. So, the energy of active nodes in the ECBDS scheme is higher than in the CBDS.

VI. Conclusions

In this paper, we elaborate the routing issues and objectives. This paper also gives brief summary of Routing protocols and attacks present in the literature. This leaves Ad-hoc organizes totally open for examination to meet these requesting application. The exploration on MANET security is still in its initial stage. The current recommendations are regularly attack situated in that they first distinguish a few security dangers and after that upgrade the current convention or propose another convention to impede such dangers. Since the arrangements are outlined explicitely, the CBDS strategy blends a both proactive and responsive discovery plan which improves its proficiency of location. It can be conveyed for both self sent node topologies and arbitrarily sent hub topologies. It is a system wide location plan wherein on recognition of malicious node the whole system is educated about the identification by Alarm signal. ECBDS has been effectively executed on different attacks like DOS and Sleep deprivation before and has turned out to be similarly productive in the event of resource utilization and byzantine attack in our investigation as well. Reproduction result have demonstrated an improved response and expanded location for ECBDS. ECBDS does not avoid malicious attack But there every node has individual responsibility for transmission and reception of packet data. This results in less over heading of control messages for transmission and reception. This correspondingly results in less end to end delay of packets and increased throughput.

References

[1]. Chin-Feng Lai, Han-Chieh Chao, Jian-Ming Chang, Isaac Woungang, and Po-Chun Tsou, Member,"Defending Against Collaborative Attacks by Malicious Nodes in MANETs:A Cooperative Bait Detection Approach", IEEE, DOI:10.1109/JSYST.2013.2296197,ISSN:1932-8184, Volume:9, Issue:1,Page(s):65-75,March 2015

[2]. BabakHosseinKhala, HamidrezaBagheri, Marcos Katz, Mohammad JavadSalehi, Mohammad Noor mohammadpour, and Seyed Mohammad AsghariPari. "A Self-Organizing Approach to Malicious Detection in Leader-Based Mobile Ad-hoc Networks", Wireless Days (WD), 2013 IFIP, Valencia,DOI: 10.1109/WD.2013.6686475, ISSN:2156-9711, Page(s):1 – 3, 13-15 Nov. 2013

[3]. Richard Yu, Helen Tang, Minyi Huang and Yanwei Wang, Member," A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks",Wireless Communications, IEEE ,ISSN:1536-1276, Volume:13, Issue:3, Page(s):1616-1627, January 2014

[4]. Durgesh Kumar Mishra (Acropolis Institute of Technology and Research, Indore, India),Mahakal Singh Chandel (Arjun Institute of Advaced Studies and Research Centre, Indore, India),Rashid Sheikh,"Security Issues in MANET: A Review", Wireless And Optical Communications Networks (WOCN), Colombo,DOI: 10.1109/WOCN.2010.5587317, Page(s):1 – 4,sept. 2010.

[5]. Li Shi-Chang, Yang Hao-Lan, Zhu Qing-Sheng College of Computer Science Chongqing University Chongqing, China," Research on MANET Security Architecture design", Signal Acquisition and Processing, Bangalore, DOI: 10.1109/ICSAP.2010.19, Page(s):90-93, Feb 2013.

[6]. Luis Javier García Villalba , Julián García Matesanz , Ana Lucila Sandoval Orozco and José Duván Márquez Díaz,"Auto-Configuration Protocols in Mobile Ad Hoc Networks",Sensors , DOI: 10.3390/s110403652,11(4), Page(s):3652-3666,25 March 2011.

[7]. Nikhil R Joshi,Chandrappa D.N,"Manet Security Based On Hybrid Routing Protocol and Unique Cryptographic Identity" Nidhi Saxena,Vipul Saxena, Neelesh Dubey, Pragya Mishra,"REVIEW PAPER ATTACK ANALYSIS IN MOBILE AD HOC NETWORK BASED ON SYSTEM OBSERVATIONS", IJARCSSE, ISSN:2277-128X,Volume:3, Issue:7, Page(s):618-623, July 2013.

[8]. Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Anton Satria,"Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol", Australian Journal of Basic and Applied Sciences, ISSN 1991-8178, Volume:5,Issue:10,Page(s): 1137-1145,2011

[9]. Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi, "Detection and Prevention of Blackhole Attack in MANET Using ACO", International Journal of Computer Science and Network Security, Volume:12, Issue :5, Page(s):21-24, May 2012 .

[10]. Usha,Bose," Understanding Black Hole Attack in Manet", European Journal of Scientific Research, ISSN: 1450-216X, Volume:83,Issue:3, Page(s):383-396, 2012.

[11]. Mansoor Alicherry, Angelos D. Keromytis, "Securing MANET Multicast Using DIPLOMA", Adavances in computers and information security, ISSN: 0302-9743, Volume 6434, Page(s):232-250, 2010.

[12]. K. Biswas anormatid Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March2007.

[13]. G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006

[14]. Mieso K.Denko, "Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme", SYSTEMICS, CYBERNETICS AND INFORMATICS,Volume-3,Issue-4,Page(s):1-9,2011.

[15]. Safdar Ali Soomro, Sajjad Ahmed Soomro , Abdul Ghafoor Memo, Abdul Baqi,"Denial of Service Attacks in Wireless Ad hoc Networks", Journal of Information Communication Technology, Volume:4,Issue:2, Page(s): 01-10,2010.

[16]. Fei Xing, Wenye Wang, "Understanding Dynamic Denial of Service Attacks in MobileAd Hoc Networks", Military Communications Conference, Washington, DC, DOI: 10.1109/MILCOM.2006.302178, ISBN:1-4244-0618-8,Page(s):1-7, Oct. 2006.

[17]. S.B.Aneith Kumar S.Allwin Devaraj J. Arun kumar, "Efficient Detection of Denial of Service Attacks in MANET ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume: 2, Issue :5, ISSN: 2277-128X, May 2012.

[18]. Xiaoxin Wu, David K. Y. Yau, "Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game-theoretic Approach ", ASIACCS, March 20-22, 2007.

[19]. Aditya Bakshi, A.K.Sharma , Atul Mishra"Significance of Mobile AD-HOC Networks (MANETS) ", International Journal of Innovative Technology and Exploring (IJ ITEE) ,ISSN:2278-3075,Volume:2,Issue:4,Page(s)-1-5,march 2013.

[20]. Jian-Ming Chang , Po-Chun Tsou ,Han-Chieh Chao ,Jiann-Liang Chen,"CBDS: A Cooperative Bait Detection Scheme to prevent malicious node for MANET based on hybrid defense architecture", Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic SystemsTechnology (Wireless VITAE) Chennai, DOI: 10.1109/WIRELESSVITAE.2011.5940839, Page(s)-1-5,Feb 28 2011-March 3 2011.

[21]. Onkar V.Chandure, Prof V.T.Gaikwad " A Mechanism for recognition & Eradication of Gray Hole attack using AODV Routing Protocol in MANET" IJCSIT , Volume:2, Issue:6, ISSN:0975-9646,Page(s):2607-2613,Jul 2011.

[22]. Vishnu K and Amos J Paul "Detection and removal of Cooperative Black/Gray hole attack in Mobile Adhoc Networks" IJCA,ISSN:0975-8887, Volume:1, Isuue:22,Page(s)-38-42,Jan 2010.

[23]. Megha Arya and Yogendra Kumar Jain "Gray hole attack and prevention in Mobile Adhoc Network" IJCA ,ISSN:0975-8887,Volume:27,Issue:10,Page(s)-21-26, Aug 2011.

[24]. M. Medadian, M.H. Yektaie, and A.M. Rahmani." Combat with black hole attack in aodv routing protocol in manet. "Internet, AH-ICI 2009. First Asian Himalayas International Conference, Kathmandu ,DOI: 10.1109/AHICI.2009.5340351,page(s): 1–5, nov. 2009.

[25]. Y.C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks in wireless ad hoc network routing protocols," in ACM Workshop on Wireless Security (WiSe), San Diego, California, USA,Page(s)-30-40, 2003.

[26]. Shabir Sofi, Eshan Malik, Rayees Baba, Hilal Baba, Roohie Mir ,"Analysis of Byzantine Attacks in Adhoc Networks and Their Mitigation ",ICCIT, 2012.

[27]. Rakesh kumar Sahu,Narendra S chaudhari "performance evaluation of ad hoc network under black hole attack" Information and Communication Technologies (WICT),Trivandrum,DOI:10.1109/WICT.2012.6409180, Page(s):780-784, Oct.3 2012-Nov. 2 2012.