ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

A Secure Cooperative Bait Detection Approach for Detecting Malicious Nodes in MANETs

Mohan.M,[1]M.Ramakrishna[2], K.N. Narasimha murthy[3]

PG Scholar, Department of Computer Science and Engineering, Vemana Institute of Technology Visvesvaraya Technological University, Belgaum, Karnataka, India

Associate Professor and HOD, Department of Computer Science and Engineering, Vemana Institute of Technology, Visvesvaraya Technological University, Belgaum, Karnataka, India

Professor and Head PG, Department of Computer Science and Engineering, Vemana Institute of Technology, Visvesvaraya Technological University, Belgaum, Karnataka, India

ABSTRACT: In mobile adhoc-hoc Networks (MANETs), the important concern is the security as well as establishment of verbal exchange amongst nodes is that nodes have got to work at the side of each different? Averting or sensing malicious nodes initiation gray hole or collaborative black hole attacks is the fundamental undertaking. Cooperative bait detection approach mixes the benefits of each proactive and reactive defense manners. Right here it makes use of the method of transposition for implementing safety and the CBDA procedure outfits a reverse tracing procedure to aid achieve the certain goal. The demo in the existence of malicious-node assaults, the CBDA beats the DSR, and Best-Effort Fault-Tolerant Routing (BFTR) protocols in relations to packet supply ratio and routing overhead. Within the transposition method we use the key which is the ascii worth of the personality which is encrypted at sender aspect and decrypted at receiver.

KEYWORDS: Cooperative Bait Detection Approach (CBDA), collaborative black hole attacks, grey hole, black hole, malicious node

I. INTRODUCTION

Mobile ad hoc network (MANET) falls within the class of wi-fi ad hoc network, and is a self-configuring network. Each and every device is allowed to move freely in any course, and accordingly will adjust its link with different devices ordinarily. Each and every node need to ahead traffic which is not involving its own use, and hence be each a router and a receiver. This option additionally comes with a extreme concern from the protection point of view. Obviously, the above-stated applications impose some extreme constraints on the security of the network topology, routing, and information site visitors. For instance, the presence and collaboration of malicious nodes in the community may disrupt the routing approach, main to a misguided of the network operations. The protection of MANETs deals with prevention and detection ways to battle man or woman misbehaving nodes. With admire to the effectiveness of these ways becomes weak when more than one malicious nodes conspire together to initiate a collaborative assault, which can outcome to more shocking damages to the community. These networks are enormously susceptible to routing assaults comparable to blackhole and grayhole (referred to as versions of blackhole attacks).

II. ROUTING PROTOCOLS

There are mainly 3 types of routing protocols they are:
1. Proactive routing
2. Reactive routing
3. Hybrid routing

DOI: 10.15680/ijircce.2015.0305103

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Proactive routing:

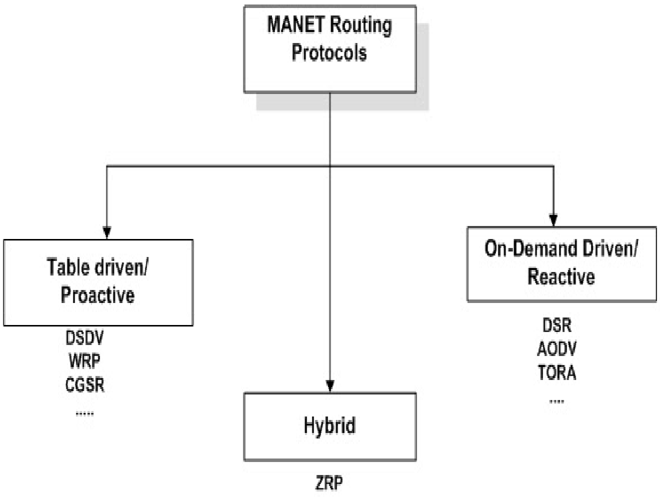
It's a table pushed protocol and it continues renewed lists of destinations and the routes with the aid of periodically meting out routing tables through the entire network. The disadvantage of these algorithms is with respective amount of knowledge for protection in a similar fashion slow response on rearrangement and screw ups. Examples of proactive algorithms are Optimized hyperlink State Routing Protocol (OLSR),vacation spot Sequence Distance Vector (DSDV).

Reactive routing:

It's an On-demand routing protocol it finds the route on demand by way of overflowing the network with Route Request packets. The drawback of these algorithm is excessive inaction time in route finding, pointless flooding which can lead to community blockage. Examples of on-demand algorithms are ad hoc On-demand Distance Vector(AODV), Dynamic source Routing(DSR).

Hybrid routing*:*

It is the combination of each proactive and reactive routing. The routing is firstly recognized with the proactively examined routes and then aids the demand from in addition began nodes over reactive flooding. The most efficient of 1 or the opposite process desires prearrangement for common instances. The drawback of those algorithms is it is dependent upon quantity of additional nodes caused the response to traffic go with the flow demand will depend on ramp of visitors quantity. Examples of hybrid algorithms is ZRP (Zone Routing Protocol)



III. BACKGROUND

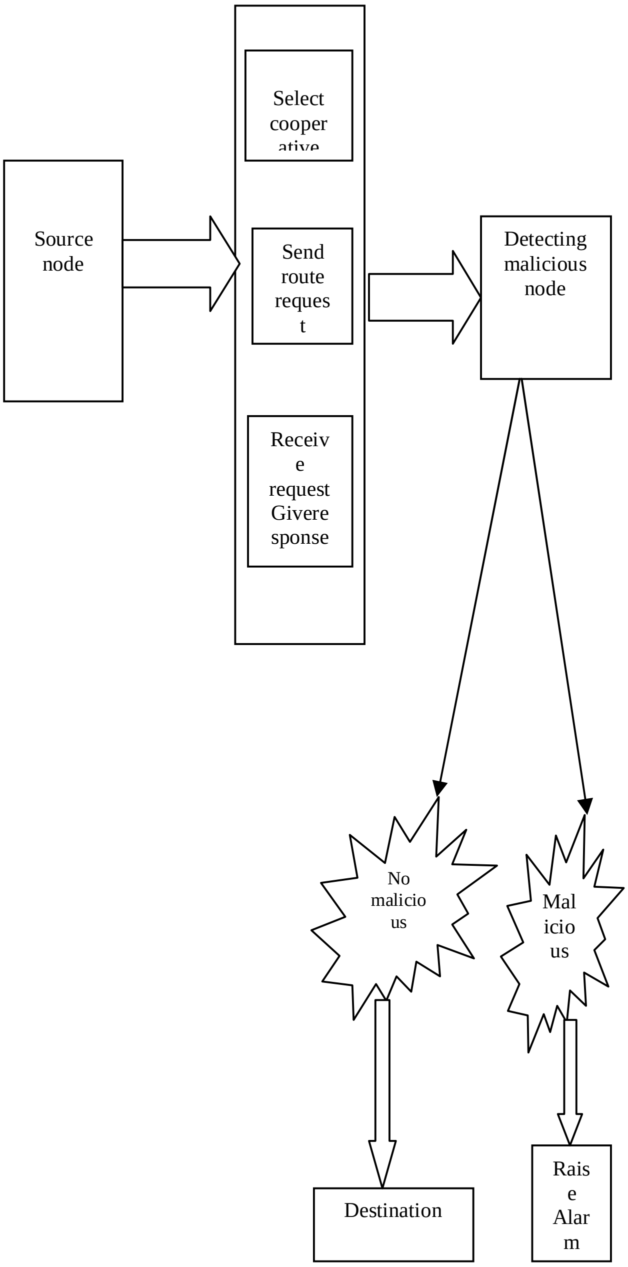
Black hole: A black holemeans that the malicious node exploits the routing protocol to claim that it has the shortest path to the vacation spot node, it does not ahead packets to its neighbors instead it drops the packets. The principal predicament is that the PDR decreases

Gray hole: A Gray holeattack is tougher to notice considering that nodes can drop packets partly as a result of its malicious nature or due to overload, congestion and egocentric nature of the nodes that are worried within the routing approach.

Collaborative Black hole:The malicious nodes cooperate with every other with the intention to mesmerize the average into their invented routing knowledge, to hide from the prevailing detection scheme.

IV. SYSTEM ARCHITECTURE

The supply node first identifies all of the nodes which forms its neighbors node i.e. That are at specified distance from that node as soon as the neighbor nodes are chosen it then sends the vacation spot deal with to all of the neighbor nodes if it is at one hop distance then it has a right away if now not then the adjacent node updates the source handle by using updating it's region within the supply address and then it does the identical system until a route to the destination is observed as soon as the path is observed then a experiment packet is sent and the packets is forwarded to the vacation spot.



Algorithm

1 Here we first set up the nodes.
2 Then we define the node parameters
3 Node Mobility is set
4 Initially we set a bait node in between the source node and the destination node
5 The RREQ is sent from the source to destination
6 The intermediate nodes is used to transfer data from the source node to the destination node
7 The RREP message is sent from the destination to the source
8 Once the RREP is obtained a threshold value is set and if the packet delivery ratio falls below it then it will trigger and RREQ phase will begin
9 The is sent in a secure manner by encrypting the data
10 The destination node decrypts the data
11 The valves are recorded and a graph is plotted respectively

V. METHODOLOGY

1.Network Model:

It remember a dense multihop static wireless mobile network deployed within the sensing field, it expect that each and every node has plenty of neighbors. When a node has packets to ship to the destination, it launches the on-demand route discovery to discover a route if there is no longer a contemporary path to a vacation spot and the MAC layer presents the hyperlink first-class estimation carrier.

2.Initial Bait:

The purpose of the bait section is to entice a malicious node to ship a reply RREP by sending the bait RREQ that it has used to promote itself as having the shortest route to the node that detains the packets that had been modified. To obtain this intention, the next process is designed to generate the destination deal with of the bait RREQ .The source node stochastically selects an adjacent node, within its one-hop regional nodes and cooperates with this node through taking its tackle as the destination tackle of the bait RREQ. First, if the neighbor node had no longer launched a black gap attack, then after the supply node had despatched out the RREQ , there can be different nodes' reply RREP in addition to that of the neighbor node. This suggests that the malicious node existed within the reply routing. The reverse tracing program in the next step can be initiated with a view to notice this route. If best the neighbor node had despatched the reply RREP, it implies that there used to be no other malicious node reward in the community and that the CBDA had initiated the DSR route discovery segment.

3. Initial Reverse Tracing:

The reverse tracing software is used to become aware of the behaviors of malicious nodes by way of the route reply to the RREQ message. If a malicious node has received the RREQ , it is going to reply with a false RREP. Hence, the reverse tracing operation will be conducted for nodes receiving the RREP, with the purpose to infer the doubtful route knowledge and the briefly trusted zone within the route. It will have to be emphasized that the CBDA is able to discover more than one malicious node at the same time when these nodes send reply RREPs.

4. Shifted to Reactive Defense Phase:

When the route is centered and if at the destination it's determined that the packet delivery ratio significantly falls to the edge, the detection scheme could be brought on again to become aware of for steady upkeep and real-time reaction efficiency. The edge is a various value in the variety [85%, 95%] that may be adjusted in line with the current community effectivity. The initial threshold price is ready to 90%.

A dynamic threshold algorithm is designed that controls the time when the packet delivery ratio falls beneath the identical threshold. If the descending time is shortened, it implies that the malicious nodes are still reward in the community. In that case, the edge must be adjusted upward. Otherwise, the threshold will likely be lowered.

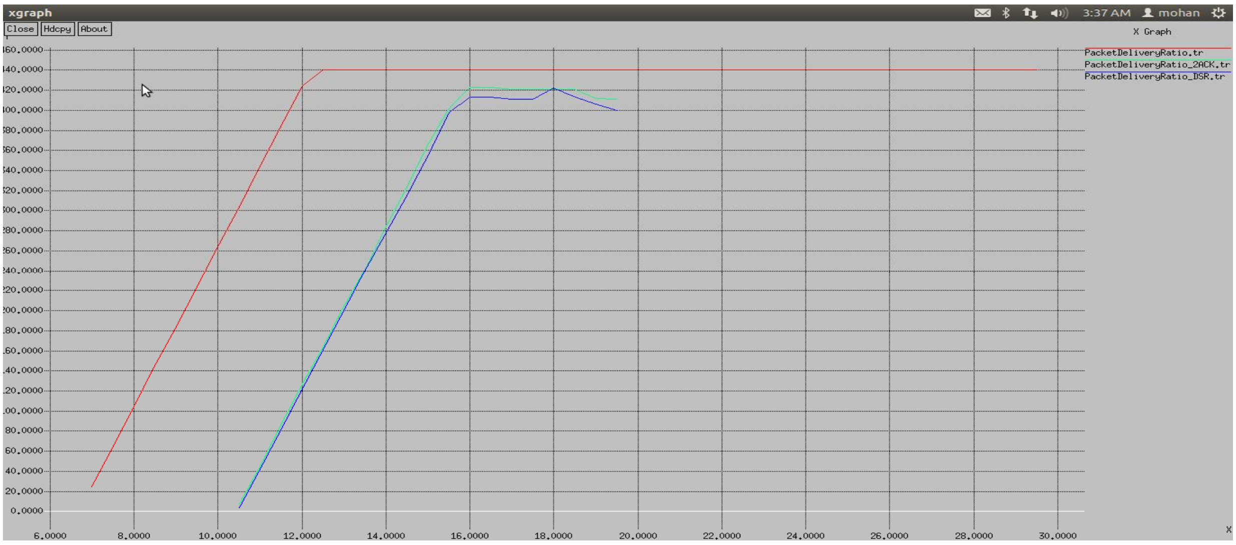
5. Security Module:

The info transmission comfy after the detection of black hole assault. Key Distribution center (KDC) provides key 'k' which is shared between source and the destination. Supply generates the key KEY, making use of quantity of hops

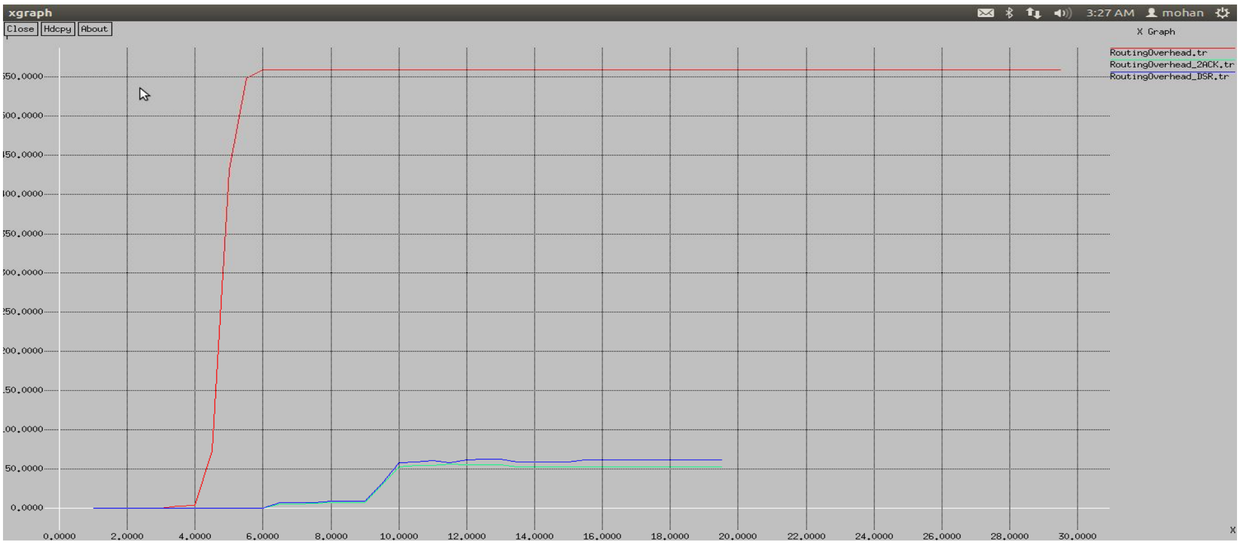
(HR) concerned within the route and message sent time (TS). Utilizing KEY knowledge is encrypted at the first stage and generates Ciphertext1. In the second degree, Ciphertext1 ,TS and HR are encrypted making use of k. In the 2nd degree before encrypting the TS and HR , they will have to be shuffled utilising some shuffling algorithm the Ciphertext2 is sent to the destination the destination makes use of ok and decrypt the Ciphertext2. By way of making use of shuffling algorithm, destination obtains values of TS and HR making use of TS and HR, destination generates KEY using KEY, Ciphertext1 is decrypted.

VI. RESULTS

Packet Delivery Ratio: It is defined as the ratioof the number of the number of packets sent by the source to the packets received at the destination. A graph is plotted

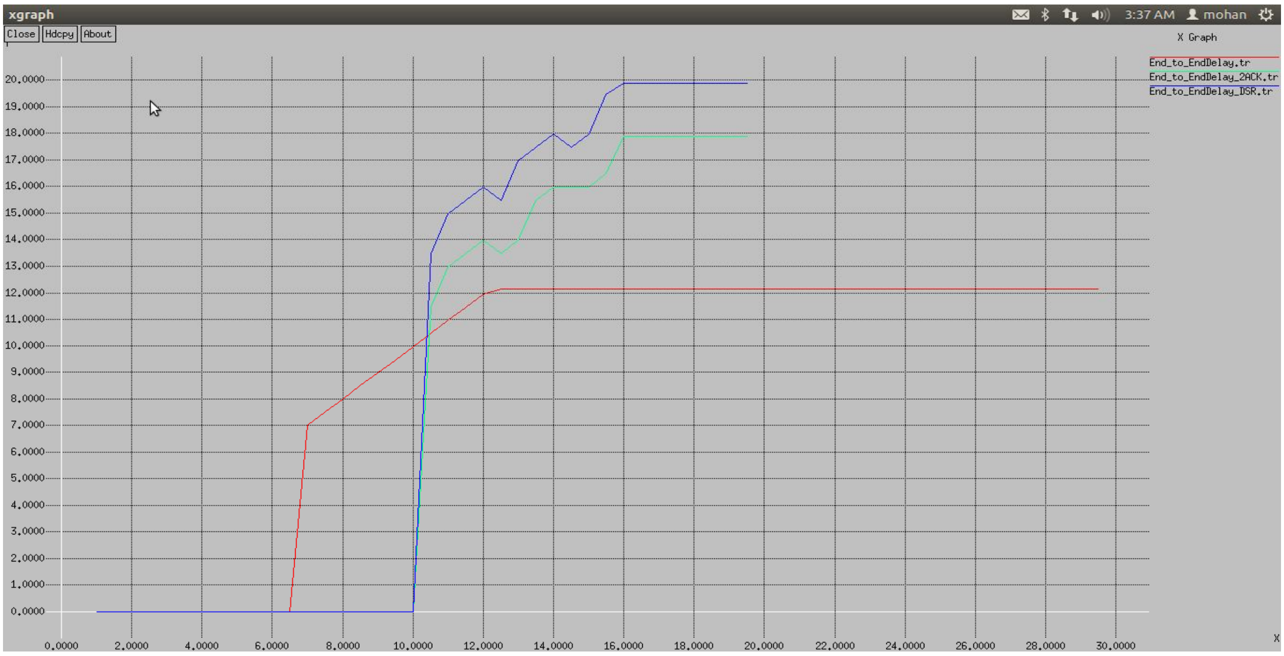


Routing Overhead: This metric represents the ratio ofthe amount of direction finding related control packet transmissions to the amount of data transmissions.

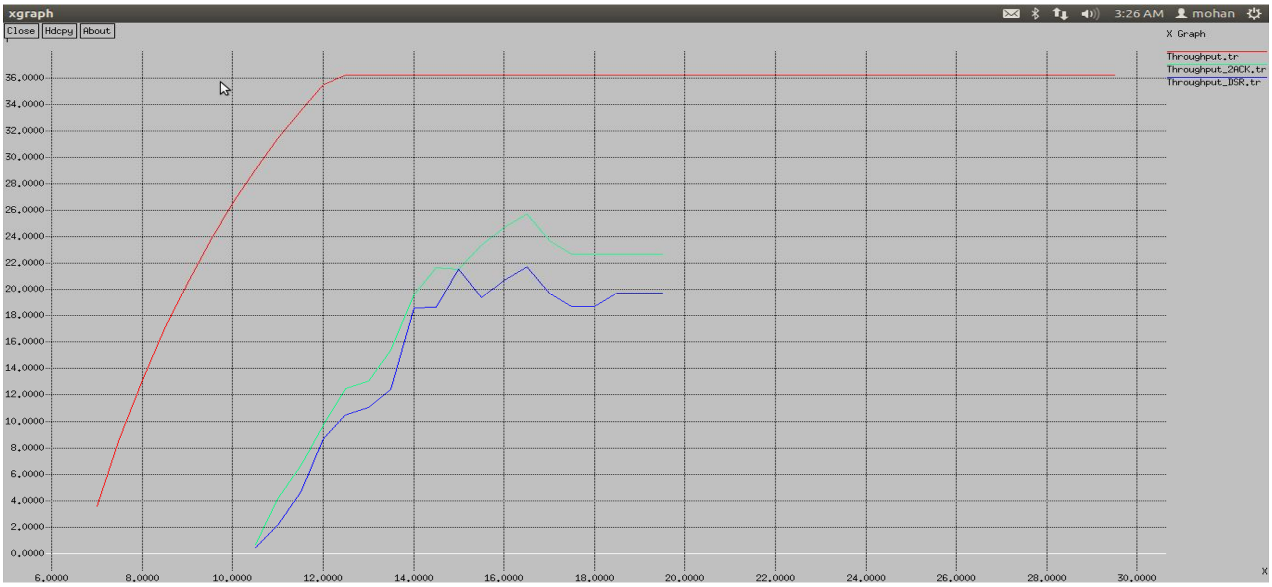


DOI: 10.15680/ijircce.2015.0305103

Average End-to-End Delay:It is well-defined as the average time taken for a packet to be transmitted from the source to the destination.



Throughput: It is defined as the total amount of data, that the destination receives them from the source which is divided by the time it takes for the destination to get the final packet.



VII. CONCLUSION

As the transposition protection model is applied to the co-operative bait detection approach the information is distributed in a secured manner and the packet delivery ratio can be expanded and the loss of knowledge packets is lowered. Enhancement can be completed with distinct types of Ad-Hoc routing protocols.

REFERENCES

[1] A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," *Intl. J. Comput. Sci. Inf.Security*, vol. 7,pp 1-5, 2010 .

[2] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure Routing and Intrusion Detection in Ad Hoc Networks," in IEEE International Conference on Pervasive Computing and Communications, pp. 8–12, 2005.

[3] C. Chang, Y.Wang, and H. Chao, "An efficient Mesh-based core multicast routing protocol on MANETs," *J. Internet Technol.*, vol. 8, no. 2, pp. 229– 239, Apr. 2007.

[4] Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) Routing," Internet Draft, November 2002 Book.

[5] D. P. Agrawal and Q.-A. Zeng, "*Introduction to Wireless andMobile Systems*", Brooks/Cole Publishing, Aug. 2002 Book.

[6] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput.*, pp. 153–181, 1996.

[7] Elizabeth M. Royer, and Chai-KeongToh, "A Review of Current Routing Protocols for AdHoc Mobile Wireless Networks," IEEE Personal Communications, pp. 46-55, April 1999.

[8] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," *IEEE Commun. Mag.*, vol. 40, no. 10, Oct. 2002.

[9] H. Weerasinghe and H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in *Proc. IEEE ICC*, 2007, pp. 362–367.

[10] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, pp. 10, October 2002.

[11] *IEEE Standard for Information Technology*, IEEE Std 802.11-14997, 1997, Telecommunications and Information exchange between systems: wireless LAN medium access control (MAC) and physical layer (PHY) Specifications, pp. i-445.

[12] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in *Proc. IEEEAerosp. Conf.*, 2002, vol. 6, pp. 2727–2740.

[13] J. Lundberg, "Routing Security in Ad Hoc Networks," Helsinki University of Technology, http://citeseer.nj.nec.com/400961.html

[14] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[15] K. Liu, J. Deng, P. Varshney, K. Balakrishnan, "An Acknowledgment- Based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Transactions on Mobile Computing, 6(5), pp. 536- 550, 2007.

[16] K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," *Int. J. Comput. Appl.*, vol. 1, no. 22, pp. 28–32, 2010.

[17]L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Net.*, vol. 13, pp. 6-10, Nov./Dec. 1999.

[18]P.-C. Tsou, J.-M.Chang, H.-C.Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based onhybrid defense architecture," in *Proc. 2nd Intl. Conf. Wireless Commun.,VITAE*, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

[19] P. Michiardi, and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proceedings of IFIP Joint Working Conference on Communications and Multimedia Security, pp.107-121, 2002.

[20]QualNetSimulaton Tool, Scalable Network Technologies. (Last retrieved March 18, 2013). [Online]. Available: http://www.qualnet.com

[21] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation based incentive scheme for ad hoc networks," in IEEE WCNC, 2004 Book.

[22] S. Buchegger and J.-Y. L. Boudec, "Self-policing mobile ad-hoc networks by reputation systems," IEEE Communications Magazine, pp. 101-107, 2005.

[23] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013).[Online].Available: ttp://www.elook.org/computing/rfc/rfc2501.html

[24] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routingmisbehavior in mobile ad hoc networks," in Proceedings of the 6th Annual international Conference on Mobile Computing and Networking(MobiCom), pp. 255-265, 2000.

[25] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in *Proc. Int. Conf. Wireless Netw.*, Jun. 2003, pp. 570–575.

[26] W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in *Proc.WiSec*, 2009, pp.103–110.

[27] W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in *Proc.* 28*th IEEE Int. Symp.ReliableDistrib. Syst.*, New Delhi, India, Sep. 2009.

[28] Y.-C. Hu, A. Perrig, D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in IEEE INFOCOM, pp. 1976- 1986, 2003.

[29] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, 11(1):21–38, 2005.

[30] Y. Xue and K. Nahrstedt, “Providing fault-tolerant ad hoc routing service in adversarial environments,” *Wireless Pers.Commun.*, vol. 29, pp. 367– 388, 2004.

[31]Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao “A survey of black hole attacks in wireless mobile ad hoc networks” Human-centric Computing and Information Sciences 2011, 1:4

[32]Madhusudhananagakumar KS, G. Aghila “A Survey on Black Hole Attacks on AODV Protocol in MANET” International Journal of Computer Applications (0975 – 8887) Volume 34– No.7, November 2011.

[33] Mohan.MRamakrishna.M “A Survey on A Secure Cooperative Bait Detection Approach for Detecting Malicious Nodes in MANETs” International journal on Recent and Innovation Trends in Computing and Communication (2321-8169) Volume 3– Issue-3, March 2015.