IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 73-79
www.iosrjournals.org

CTV: Consistent Trust Value through Data Drop Monitoring Parameters Based Malicious Behaviour Detection in MANET

[1]Siddharth Shukla, [2] Prof (Dr.) Jayant Shekhar, [3] Amit Kumar
[1]M.Tech (CS) Student, [2] Director of Technical Campus, [3] Lecturer CS/IT
SUBHARTI UNIVERSITY, MEERUT (U.P.), INDIA, 250005

Abstract*: Growth of wireless technologies with its increased user demands of applications makes this area more vulnerable for attackers and intruders. The attacker continuously trying to affects the communication and getting the benefits from gamming the network with higher data drop rates. Among them, the most famous and dangerous attacks is blackhole by which a node starts dropping a data and behaving as a normal node. During the last few years various solutions are provided for overcoming the active and passive blackhole detection and termed as malicious node detections. Any node, affecting the actual performance or operation of network will be termed as malicious node and blackhole is its one category. The existing mechanism only detects the static blackhole attacks but is not capable to detect sudden change in the behavior of node from legitimate to malicious. Thus this paper proposes a CTV (Consistent Trust Value) mechanism based on some of the performance parameter analysis such as PDR, throughput, delays and TTL values by which timely triggered and normal blackhole node is detected with higher accuracy. By regular analysis those improper behaviour is detected in timely manner and reduces the probability of data drops. At the initial level of evaluation the approach is proving its strong presence among the existing methods.*

Index Terms: *MANET (Mobile Ad-Hoc Network), AODV, Routing, Attacks, Timely Triggered Blackhole, CTV (Consistent Trust Value), Reliable Path;*

I. Introduction

Network is wide range of applicability having sudden increase in the quantity of users over the last few years, operating various data oriented applications on mobile devices. Thus mobility is considered to be a major component in terms of business sales and connectivity management. Thus the use of wireless network is also exponentially hitting the market. Among various wireless networks few are infrastructure dependent and few are not. For small range communication dependencies of infrastructure lets the operation more complex. A Mobile ad hoc network is a wireless medium used for short range communication having zero infrastructural requirements. In this type of network the communication is directly based on radio frequency of devices which can be used for transmitting and receiving the signals through inbuilt routing mechanisms [1]. Thus the nodes communicate with each other and transfers data from source to destination with cooperative communication between them within a transmission range. Such networks have no centralized control, dependencies, requirements with flexible communications makes it more interesting to operate. There are various application areas of MANET includes military, healthcare, business, transportation etc.

MANET suffers from various issues which address the problems making the operations complex and uncertain like routing, addressing, energy, mobility, bandwidth, QOS, security, data losses etc. Some of the hot issues related to intentional data losses come under the categories of attacks. This attacks needs to be pre-empted before affecting the system and to let them identify earlier is a part of routing mechanism. Over the last few years various attack resistant mechanisms shows their efficiency over the several categories of attacks and protect the system. But as the defending mechanism is going robust the attacks categories is also gets changing and attempting to affect the system in a different way.

The intrinsic features of MANET make them more susceptible to a wide range of attacks by misbehaving nodes in a network. Such attacks can be planned as passive and active attacks. Active attacks, mainly consider the internal attacks for network layer such as black hole attack, gray hole attack, worm hole attack, message tampering, routing attacks. A malicious node drops packets or generates additional packets solely to disrupt the network performance and prevent other nodes from accessing any network services [2]. Misbehaviour can be divided into two categories [3]:

- Routing misbehaviour (failure to behave in accordance with a routing protocol)
- Packet forwarding misbehaviour (failure to correctly forward data packets in accordance with a data transfer protocol).

These two are employed using AODV (Ad hoc on demand distance vector protocol) routing strategy. This approach detects and prevents misbehaving nodes (malicious) capable of launching any of the network layer attacks [4]. This work tries to identify the early detection parameters for black hole node behaviour analysis so as to stop the data or packet losses. The work suggests a novel CTV (Consistent Trust Value) mechanism for overcoming the recent issues of early blackhole detections with malicious behaviour identification before dropping the data packets.

II. Background

MANET is a short range communication system based on wireless medium. Here the mobile devices is used as router having less system specifications so as their working protocols is also light weighted from the actual networking protocols. In this reduction of size different categories and their solutions are not provided with existing protocols. Among them, AODV is the most used protocol for research studies of MANET gives an outcome that it is not having any sufficient mechanism for detecting the maliciously behaving node. The main goal of the security requirements for MANET is to provide a security protocol, which should meet the properties like confidentiality, integrity, availability and non-repudiation to the mobile users. The identification of a malicious node is the estimated percentage of packets dropped, which is compared against a pre-established misbehaviour threshold. Any other node which drops packets in excess of the pre-established misbehaviour threshold is said to be misbehaving, while for those nodes percentage of dropping packets is below the threshold are said to be properly behaving.

Malicious behavior is of any type ranges from dropping the data to routing disturbance creations etc. One of them is black hole attack active attack. In a black hole attack [5], malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, gives a high sequence number to make entry in the routing table of the victim node, before other nodes send a true RREP. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node.

Malicious node attacks all RREQ messages this way and takes access to all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole attack to real meaning which drops all objects and matter. There are two major behaviours that Black hole node actually possesses. They are as follows:-

(i) Black hole node advertise itself by showing larger or highest possible destination sequence no. as we know larger the sequence [6] no. means the route is fresh and latest for a particular destination. This way malicious node bluffs the source node, who wants to initiate communication.

(ii) It is an active DoS attack in MANET [6], which intercepts all incoming packets from an intended source. A black hole node absorbs the network traffic and drops all packets.

(iii) The malicious node is supposed to be positioned in center of the wireless network.

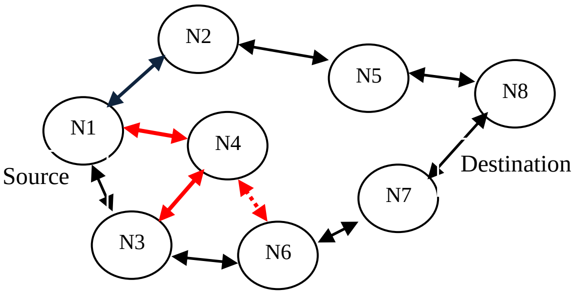

Figure 1: Network Model for Black Hole Illustration

Network Illustration Model

To consider the problem of black-hole node identification through existing methodology included in AODV on demand protocol is shown in figure 1 above. It, assumes that node N4 is the malicious node [6]. Suppose node N1 has to send data packets to node N8, and starts the route discovery process. We assumed node N4 is a malicious node and according to the behavior of Black hole node which has no fresh enough route to destination node N8. However, node N4 claims that it has the shortest route to the destination whenever it receives RREQ packets, and sends the response to source node N1. The destination node and any other normal intermediate nodes that have the fresh route to the destination may also give a reply.

If the reply from a genuine node reaches the source node of the RREQ First, everything works as it is supposed to do; but the false reply RREP from malicious node N4 is probable to reach the source node first, in the case if malicious node is close to the source node. A malicious node does not need to check its routing table as it is known that it's sending a false RREP message; its response is probable to reach the source node first. This makes ensure the source node that the route discovery process is complete, then it discards all other reply messages, as it has got the shortest route reply(from malicious node) first and begin to send data packets over it. As a result, all the packets through the malicious node are intercepted or dropped. The malicious node could be said to form a black hole in the network. In this way the malicious node can easily gulp a lot of network traffic to itself, and could cause an attack to the network with a big loss of data.

Thus while considering the above mentioned problem related to this work suggested a novel consistent trust value (CTV) based blackhole detection.

III. LITERATURE SURVEY

During the last few years various articles had been suggested which presents the strategies to overcome the malicious behaviour identification and removal mechanism. Early and accurate detection is the primary concern of all the approaches.

In the paper [1], a authentication based malicious node detection mechanism is proposed using PKI infrastructure. The mechanism calculates the digital signature of each node before letting them to participate in data transmissions. The approach is capable of detecting the multiple black hole and grey holes using this suggested mechanism. The authentication process is applied by constructing the hash function using MAC and PRF functions.

The paper [3], suggest a modifications in existing black hole detection mechanism by upgrading the AODV protocol through a data routing information (DRI) function table. The function table matches the identity of each node by a cross checking evaluating function. Table contains the entries of each node in a range of network communicating with each other and each time a node demands some data than it has to go through the suggested verification process. The approach gives great results in case of cooperative black hole detection.

Some of the authors and approaches had restricted their working area towards the side channel monitoring to analyse and detect the malicious behaviour before any data losses [4, 5]. The approach initially discovers the secure path for transmitting the data from source to destination. Each time when a node demands the communication then a secure route is established and guarantees the packets to be delivered at destinations. Monitoring the side channel is based on previous participated data analysis for behavior detection.

In the paper [6], a certificate chaining based malicious node identification mechanism is proposed having self organized PKI authentication. The approach uses a chain of nodes authenticating each other without the use of a trusted third party and gives the certificate to each other. Each node in the network has identical roles and responsibilities thereby achieving maximum level of node participation. Every node in the network can issue certificates to every other node within the radio communication range of each other. For successful transmission each node requires at least two certificates of its neighbour nodes.

There are so many other encryption based [7] & robust identification based [8] is given by different authors. They demonstrates an adaptive approach to detecting black and gray hole attacks in ad hoc network based on a cross layer design. In network layer, the paper [9] proposed a path-based method to overhear the next hop's action. This scheme does not send out extra control packets and saves the system resources of the detecting node. In MAC layer, a collision rate reporting system is established to estimate dynamic detecting threshold so as to lower the false positive rate under high network overload. Some approaches trust based calculation for malicious node identification is also proposed which is capable of detecting the nodes trust value on the basis of their historical analysis [10].

The paper [11], gives a dynamic solution for developing a prevention mechanism specifically for cooperative black hole detection. The approach is capable of generating a secure route between the pairs of nodes after which the blackhole node is isolated from the communication. The method detects the useful pattern from previous participation of data and measures the units of data drop. Practical evaluation of the solution with some of the existing mechanism is also given on some parameters for authorizing the effectiveness of the approach.

In the paper [12], a request routing table based approach is given as a solution which requires sharing of information between the nodes of a network. According to the approach, the nodes shares their routing table on regular basis by identifying the node with their sequence number; check is made for whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not. The solution presents good performance in terms of packet ratio and minimum packet end-to-end delay and throughput.

Some of the authors had worked with proof oriented solutions which measures that the node actually forwarded packets to the next hop; the receiver can send acknowledgment in the reverse direction for multiple hops [13]. Two-hop acknowledgment is suggested. However, it fails when more than two malicious nodes are colluding in a row. For example, three malicious nodes one next to another act as a team to drop packets along a data communication path: the one in the middle actually drops packets, while its prior hop simply does not do the watchdog job and its next hop falsely sends acknowledgment.

There are many other detection techniques in literature [14, 15, and 16]. They mainly aimed at early detection of packet drop attackers during routing process. The general idea is to identify forged routing information by double checking, for example, neighbour information, destination sequence number, or network state, with the nodes after the malicious node or directly with the destination [17]. Due to space limit, it introduces only a few recent proposals.

After analysis of various research papers presented over the years, black hole detection seems to be a required entity for improved routing. Still there are some of the issues remains unaddressed and needs to be solved for accurate analysis of data and efficient detection mechanism.

IV. Problem Statement

After studying the various papers given as a solution of black hole detection mechanism, it is identified that the attack detection accuracy is not certain with existing approaches. As blackhole is created to reduce the routing performance, thus the approach must be given in such a way that regular monitoring of the nodes is performed for sudden conversion or timely triggered blackhole detection. Also the attack categories like active and passive need to be measured by the node behaviour and operations. Most of the existing approaches is based on well known trust factors which will not always generates the accurate results. Along with this some new parameters should be added which gives early analysis and detection before the data dropping. The existing mechanism had also not considering the new node coming in the network fro data participation and detects them as a malicious because of their zero transfer. Thus, as according to the study of existing approaches, this work identifies that problem related to malicious or black hole node categorizes in three major security domains or issues. These are

(i) *Privacy:* maximize tracking-resistance of individual nodes, by outsider and insider adversaries.

(ii) *Security:* provide protection against active and passive outsider and insider attacks.

(iii) *Efficiency:* attain the above two goals with reasonably efficient solutions.

Thus following are the some identified problem areas considering the above parameters in mind for effective blackhole detection and removal approach:

Problem 1: Early detection of malicious behaviour according to the historic participation of each node. The routing data needs to be processed before any new communication is started.

Problem 2: Regular monitoring of nodes is not presented due to that if a node suddenly changes its behaviour to malicious then the existing approaches is not able to detect this. Such blackhole attack which starts operating after some period of time comes under the category of timely triggered malicious node.

Problem 3: False detection and infeasible behaviour is not removed from the final results which sometimes affects the legitimate node from transmissions.

Problem 4: Consistent node performance for behaviour analysis is not covered by any mechanism and path reliability with nodes behaviour is also not mentioned which causes delays in detections.

Thus some effective mechanism is required for early and accurate detection of maliciousness behaviour of an each node participating in a network. The degree of misleading up to which the nodes behaviour allowed and from where the node is termed as malicious is also given by the suggested approach given in next section of this paper.

V. Proposed CTV Approach

This paper proposes a novel consistent trust value (CTV) based timely triggered blackhole node detection in MANET. The suggested CTV approach resolves the above identified issues which remains unsolved by existing mechanism and gives effective results with high detection accuracy. The solution is proposed to identify both the category of attacks: Active and Passive. Some of the modifications to existing AODV protocol suggested with less computational overhead with speedy response time. The solution regularly monitors the nodes behaviour and fetching the data from different nodes in the range. Each node in a network will watch the behaviour of its neighbour node by overhearing its transmissions. Normally the AODV identifies the path based on RREQ and RREP messages and generates the route with fastest response RREP from its neighbour node. But this response might be generated from malicious node and assures transmission from this which latter on lets the packets dropped. Here the CTV node captures the information and compare this patters with legitimate node pattern through various conditional checks including PDR, throughput, TTL and drop ratios. Some of the process for newly entered node is also given to pre-empt data loss if it starts working as blackhole node. Thus a combined solution is suggested which guarantees higher delivery ratios and less overhead.

Description:

The approach starts with normal routing operation how the route discovery is performed in AODV. The source node S wants to communicate with destination node D. S broadcast the RREQ message to its entire neighbour which is further forwarded to next nodes with a check of destination address. At the node D the destination address matches and D replies with RREP message from the same route with route cost information. Now during this reply some of the maliciously behaving node also replies quickly without checking its routing table with smallest route to the destination. Thus in absence e of any malicious behaviour detection mechanism this path through blackhole node seems to be shortest and effective. But from here the CTV method start operating. Here after getting all the cost from different nodes the CTV node compares them on some of the measured parameters. Initially the node is checked whether its entry is available with routing table or not. If the node is new than the CTV value which is used for degree of authenticity is assigned to be zero. Now it means the node is new to the network and has not participated previously in data transmission and hence not been taken as blackhole node.

For node having CTV as zero, the source node sends a hello message to the identified shortest route and waits from its acknowledgement from destination and all intermediate nodes. Now in this the blackhole node thinks this hello packet as a data packet at dropped this without acknowledging the source node. Now when the acknowledgement packet is not came in fixed TTL according to the cost of path the newly node is taken as black hole else the node is legitimate.

Now, for existing timely triggered node behaviour as blackhole a constancy check is performed by CTV mechanism. In this step, PDR, throughput, drop ratio and TTL is regularly monitored for identification of degree of maliciousness. The node having fewer values with more drops and delays is taken as blackhole nodes. Now, each node has to go through a verification mechanism and conditional transmission having defined threshold limit. The node having considerable values and greater than threshold can be considered as consistent node and transmission from such node is continued. But the node having lesser values than a threshold is again checked with blackhole drop condition. If all the condition is verified all the other nodes are intimated about this node as black hole node and removes its entries from their routing table.

Thus in this way the suggested CTV based blackhole detection mechanism seems to be more accurate with higher degree of detection. The approach also consumes less computational resources with higher benefits and saves data losses with timely detection and removal; of maliciously behaving nodes.

Expected Outcomes

The CTV based approach will serve as a improvement over the exiting blackhole detection mechanism. The approach is a refined combination of different methods having capable functionalities for early and successful detection of malicious behaviour. The aim of approach is to identify the node giving consistent performance over the data transmission and taking this as a pattern and let the transmission of other node compare with it. After applying the above suggested approach there are some of the expected benefits measures are:

- Early and effective detection of malicious behaviour on the basis of identified parameters.
- Delay tolerant detection which reduces the probability of data losses.
- Timely triggered black hole detection using performance check operations which decreases routing overhead.
- Behaviour analysis of new node in the network with no previous participation.
- Regular basis monitoring for sudden conversion identification and misleading node detections.

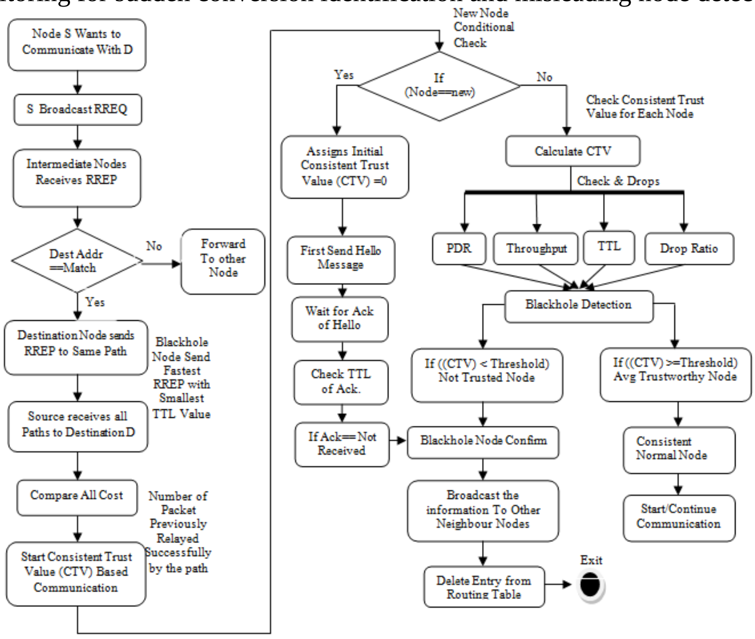
Node S Wants to Communicate With D
S Broadcast RREQ
Intermediate Nodes Receives RREP
Dest Addr ==Match
No
Forward To other Node
Yes
Destination Node sends RREP to Same Path
Blackhole Node Send Fastest RREP with Smallest TTL Value
Source receives all Paths to Destination D
Compare All Cost
Number of Packet Previously Relayed Successfully by the path
Start Consistent Trust Value (CTV) Based Communication
New Node Conditional Check
If (Node==new)
Yes
No
Check Consistent Trust Value for Each Node
Assigns Initial Consistent Trust Value (CTV) =0
First Send Hello Message
Wait for Ack of Hello
Check TTL of Ack.
If Ack== Not Received
Calculate CTV
Check & Drops
PDR
Throughput
TTL
Drop Ratio
Blackhole Detection
If ((CTV) < Threshold) Not Trusted Node
If ((CTV) >=Threshold) Avg Trustworthy Node
Blackhole Node Confirm
Broadcast the information To Other Neighbour Nodes
Delete Entry from Routing Table
Exit
Consistent Normal Node
Start/Continue Communication

FIGURE 2: A NOVEL CONSISTENT TRUST VALUE (CTV) BASED BLACKHOLE DETECTION MECHANISM

- The malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process.
- No delay = malicious node are easily identified
- No modification is made in other default operations of AODV Protocol.
- Better performance produced in little modification and
- Less memory overhead occurs because only few new things are added.

VI. PERFORMANCE EVALUATION

The proposed work considers four of the network parameters for evaluating the performance. Further it can be extended to a few more parameters based upon the network density. The algorithm can also be extended to identify and prevent few more network layer attacks.

- *Packet delivery ratio (PDR)* – the ratio of the number of packets received at the destination and the number of packets sent by the source. The PDR of the flow at any given time is calculated as,

  PDR = (packets received/packets sent)
- *Routing overhead* – The number of routing packets transmitted per data packet delivered at the destination.
- *Power consumption*- the power is calculated in terms of total time taken for transmission of a message from sender to receiver. Since this time elapses in milliseconds, the power consumed by anode will be considered as less.
- *Throughput*- It is sum of sizes (bits) or number (packets) of generated/sent/forwarded/received packets, calculated at every time interval and divided by its length. Throughput (bits) is shown in bits. Throughput (packets) shows numbers of packets in every time interval. Time interval length is equal to one second by default.

Another important fact can be considered with respect to the approach is the power consumption of the nodes in the network. When compared to other approaches, the proposed scheme presents a simple one-hop acknowledgement for new node in the network demanding transmission. The overall transmission for sending and receiving data happens in just few milliseconds, overcoming the time constraint thereby reducing power consumption.

VII. CONCLUSION

MANET, among the various attack resistance protocols some of the protocols stick to a specific attack detection condition. Most of the times these conditions are not activated due to changed attack behaviour and than these detection mechanism and protocols fails to identify the behaviours. Timely triggered blackhole is such a condition which starts its operation as a normal node but suddenly starts doing the packets. None of the exiting mechanism is capable of resolving such issues. Thus this work proposes a novel CTV (Consistent Trust value) based detection mechanism whose main aim is to monitor the consistency between the nodes and their transmissions. This mechanism is executed at each node and will work as monitoring point which checks the node behaviour against the attack based on some network parameters like PDR, throughput, TTL and delay. At the primary level of study and evaluation the approach is giving great results and even some of the approach fails to perform some operations which this approach is promising to perform. In near future some strong proof of results is provided for further guarantying the approach effectiveness.

REFERENCES

[1] D He, C Chen, S Chen, J Bu & A B. Vasilakos, "ReTrust: Attack Resistant & Lightweight Trust Management for Medical Sensor Network" in IEEE Transaction on IT in vol: - 16, No 4, July 2012.

[2] Z Min & Z Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks" in IEEE Transaction ISBN 978-0-7695-3686-6/09, 2009.

[3] S Ramaswamy, H Fu, M Sreekantaradhya, J Dixon & K Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" in Department of Computer Science, IACC 258, 2008.

[4] K E Defrawy & G Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs" in IEEE Transaction of selected Journal in communication, Vol 29 Issue 10, Dec 2011.

[5] Xu Li, R Lu, X Liang, & X Shen, "Side Channel Monitoring: Packet Drop Attack Detection in Wireless Ad Hoc Networks" in IEEE ICC, 2011.

[6] E. A .Mary Anita & V. Vasudevan, "Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining" in IJCA (0975 – 8887) Volume 1 – No. 12, 2010.

[7] P H. Yu and U W. Pooch, "Chapter on Security and Dynamic Encryption System in Mobile Ad-Hoc Network" in A&M University, Dept of CSE, Texas, USA.

[8] G. S. Mamatha & Dr. S. C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS" in IJCSS Vol 4, Isseu 3, 2010.

[9] J Cal, P Yi, J Chen, Z Wang & N Liu, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network" in IEEE Proceedings, 1550-445X/10, 2010.

[10] R Karandikar, R K Khanuja, S Shukla, "Proposed solution to prevent Black Hole Attack in MANET" in IJRIM ,Vol 2, Issue 2, ISSN 2231-4334, February 2012.

[11] H Weerasinghe and H Fu "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation" in IJCA, Vol 2 ,No 3 July, 2008.

[12] Pooja Jaiswal & Dr. Rakesh Kumar Prevention of Black Hole Attack in MANET in IRACST, ISSN: 2250-3501 Vol.2, No5, October 2012.

[13] Sarita Choudhary & Kriti Sachdeva "Discovering a Secure Path in MANET by Avoiding Black/Gray Holes" in IJRTE ISSN: 2277-3878, Volume-1, Issue-3, August 2012.

[14] M S Ashraf & M Raheel, "RGB Technique of Intrusion Detection in IEEE 802.11 Wireless Mesh Networks" in IJCSI, ISSN (Online): 1694-0814 Vol. 9, Issue 2, No 2, March 2012.

[15] A Kumar & M Chawla, "Destination based group Gray hole attack detection in MANET through AODV" in IJCSI, ISSN (Online): 1694-0814 Vol. 9, Issue 4, No 1, July 2012.

[16] Vishnu K, "Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks" in IJCA, ISSN 0975 – 8887, Volume 1 – No. 22, 2010.

[17] H P Singh, V P Singh & R Singh, "Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review" in IJCA, ISSN 0975 – 8887, Volume 64– No.3, February 2013.

[18] G. S. Mamatha & Dr. S. C. Sharma, "A New Combination Approach To Secure MANETS Against Attacks" in IJWMN, Vol.2, No.4, November 2010.

[19] S Jain, J Singhai, M Chawla, "A Review Paper on Cooperative Blackhole And Grayhole Attacks in Mobile Ad hoc Networks" in IJASUC, Vol.2, No.3, September 2011.