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. 4, Issue 8, August 2016

Defending Against Black Hole Attack Using DSR in MANET: An Misbehaviour Report Authentication

K.Ranjitha[1], M.Jothilakshmi[2]

Full Time M.Phil Scholar, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women, Elayampalayam, Tiruchengode, Namakkal, India

Assistant Professor, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women, Elayampalayam, Tiruchengode, Namakkal, India

ABSTRACT*:* Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. The Proposed System is designed to resolve the weakness of Watchdog when it fails to detect misbehavior nodes with the presence of false misbehavior report. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. The proposed IDS algorithm maintains the list of all the nodes which send the route reply to the source with sequence number greater than the threshold value. The source route broadcasts an RREQ message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcasts this new message to their neighbors. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in When the RREQ message arrives to its final destination node, the destination node initiates an RREP message and sends this message back to the source node by reversing the route in the RREQ message.

KEYWORDS: Black hole Attack, MANET, DSR, RREQ.

I.INTRODUCTION

A Mobile Ad-Hoc network or MANET is an autonomous system of mobile routers connected by wireless links the union of which from an arbitrary graph. The Router or free to move randomly and organize themselves arbitrary. Thus the networks wireless topology may change rapidly and unproductively. Such a network is developed in ad-hoc basis without any pre-existing in infrastructure and may operating either stand alone fashion or may be connected to the layer internet. The Misbehaviour Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. false misbehaviour report can be generated by malicious attackers to falsely report that innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. a new intrusion detection system named Enhanced Adaptive Acknowledgement (EAACK) specially designed for MANETs. By the implementation of Misbehaviour Report Authentication (MRA) scheme, EAACK is able of detecting malicious nodes despite the existence of false misbehaviour report and compared it against other popular mechanisms in different scenarios during simulation. The results will demonstrate positive performances next to Watchdog, TWOACK and AACK in the cases of receiver collision, limited communication power and false misbehaviour statement. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, with the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such Trend, we strongly believe that it is vital to address its potential security issues.

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. 4, Issue 8, August 2016

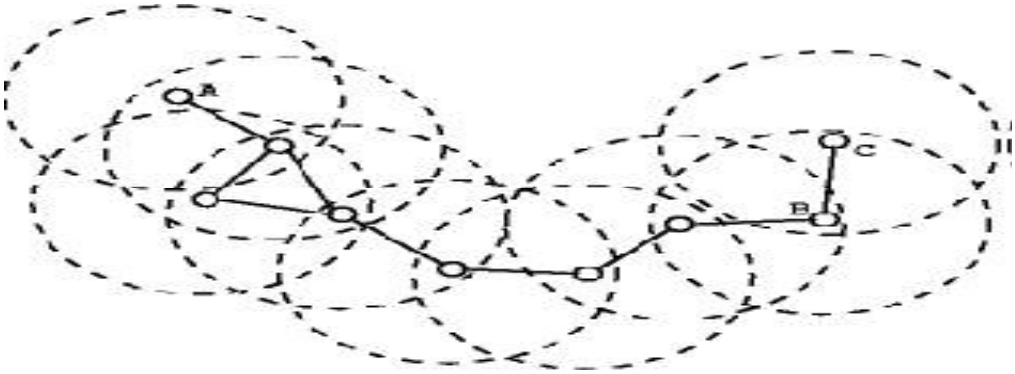

Fig.1: Basic Routing Module between nodes

II.RELATED WORK

2.1CDBS:A Cooperative Bait Detection scheme to prevent malicious node for MANET:

A mobile ad hoc network (MANET), sometimes called a mesh mobile network, is a network of mobile devices connected by wireless links. MANET is a kind of point to point transmission type and is a group of mobile nodes communicating with each other by wireless. Due to infrastructure-less nature of the network, routing and network management is done cooperatively by the nodes i.e. the nodes themselves maintains the functioning of the network. The topology of the network varies rapidly and unpredictable over time because of the mobility of the nodes. Besides, the security of MANET has many defects. These threats make the security of MANET lesser than a cable network and produce many security issues. Because the communication of MANET uses the open medium, attacker can easily overhear message that are transmitted.the design of previous routing protocol trusts completely that all nodes would transmit route request or data packets correctly, dynamic topology, without any central infrastructure, and lack of certification authorities make MANET vulnerable to diverse types of attacks. One of common attack is Black hole attack that is a malicious node can attract all packets by using forged RREP to falsely claiming a fresh and shortest route to the destination and then discard them without forwarding them to the destination. This is shown in Fig. 1. Black hole attack is a kind of Denial-of-Service attacks and derive Gray hole attack, a variant of black hole that selectively discards and forwards data packets when packets go through it. Cooperative black hole attacks mean several malicious nodes cooperate with each other and work just like a group.

Malicious Node: A node under attack due to breaches any of the security principles and is said to be exhibiting a malicious behavior

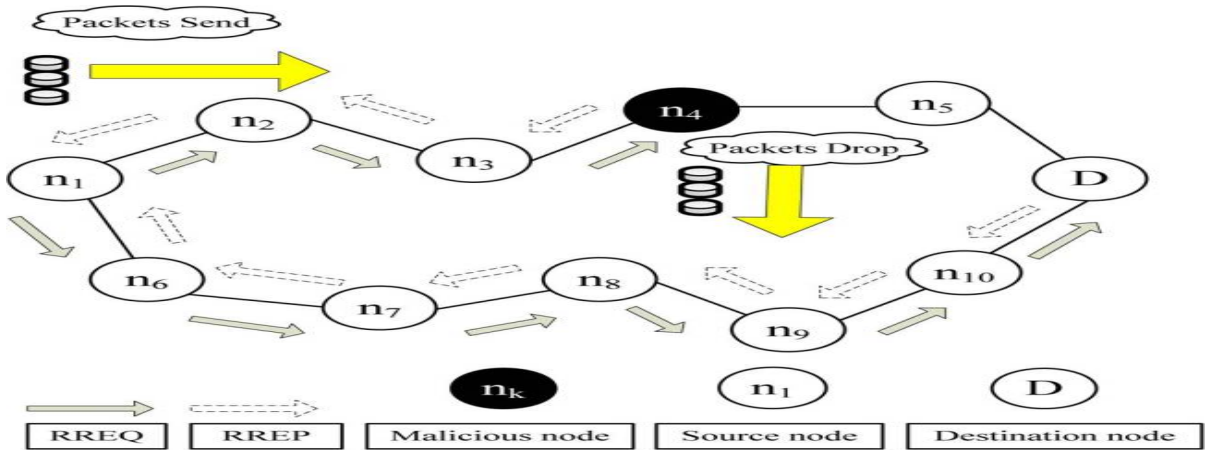

Fig 2: Black hole attack, Node4 drop all packets

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. 4, Issue 8, August 2016

2.2 Alternative Approach to Detect Presence Of Black Hole Nodes In Mobile Ad-Hoc Network Using Artificial Neural:

Black Hole node detection if it exists in any Mobile ad hoc networks (MANETs). The dynamic topology of MANETs allows nodes to join and leave the network at any time instance. This general feature of MANET has exposed to major security attacks including existence of black hole nodes, which adversely affects the entire routing practice. To deal with this routing mess, we have proposed an Artificial Neural Network (ANN) based automated Black Hole node detection tactic, which is capable of detecting the existence of Black hole node(s) in the MANET and thus helps to minimize the smash up in reliable routing procedure. Experimental results in network simulation confirm the hazards caused by presence of Black hole node(s) in MANET, which is same as our earlier research on black hole node detection using Cellular Automata (CA).

2.3 Selective Watchdog Technique For Intrusion Detection In Mobile Ad-Hoc Network

Mobile ad-hoc networks(MANET) is the collection of mobile nodes which are self organizing and are connected by wireless links where nodes which are not in the direct range communicate with each other relying on the intermediate nodes. As a result of trusting other nodes in the route, a malicious node can easily compromise the security of the network. A black-hole node is the malicious node which drops the entire packet coming to it and always shows the fresh route to the destination, even if the route to destination doesn't exist. This paper describes a scheme that will detect the intrusion in the network in the presence of black-hole node and its performance is compared with the previous technique. This novel technique helps to increase the network performance by reducing the overhead in the network.

III.MISBEHAVIOR REPORT AUTHENTICATION INTRUSION DETECTION SYSTEM IN MANETS

The Misbehavior Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. False misbehavior report can be generated by malicious attackers to falsely report that innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node. If there is none other exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. By adopting an alternative route to the destination node, circumvent the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compare if the reported packet was received.

If it is already received, then it is safe to conclude this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report. Watchdog that aims to improve throughput of network with the presence of malicious nodes. In fact, the watchdog scheme is consisted of two parts, namely Watchdog and Path rater. Watchdog serves as an intrusion detection system for MANETs. It is responsible for detecting malicious nodes misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listens to its next hop's transmission. If Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a pre-defined threshold, the Watchdog node reports it as misbehaving. In this case, the Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many following researches and implementations have proved that the Watchdog scheme to be efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme. Watchdog scheme fails to detect malicious misbehaviors with the presence of Ambiguous collisions, Receiver collisions, Limited transmission power, False misbehavior report, Partial dropping.

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. 4, Issue 8, August 2016

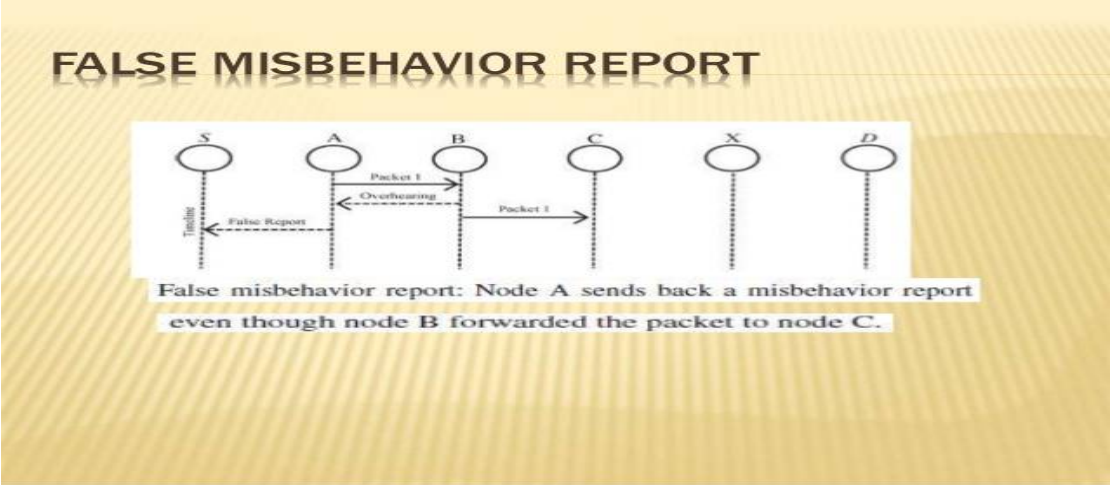

Fig.3 False Misbehaviour Report

IV. MRA SCHEME USING NETWORK SIMULATOR (NS2)

After setting up the platform, software named ns2 was set up on it which was used for all the analysis and simulation work apart from other tools used. This means that most of the simulation scripts are created in Tcl, the components have to be developed for ns2, then both Tcl and C++ have to be used. Ns2 uses two languages because any network simulator, in general it has two different kinds of things it needs to do. On the one hand, detailed simulations of protocols require a systems programming language which can efficiently manipulate bytes, packet headers, and implement algorithms that run over large data sets. For these tasks run-time speed is important and turn-around time (run simulation, find bug, fix bug, recompile, re-run) is less important. On the other hand, a large part of network research involves slightly varying parameters or configurations, or quickly exploring a number of scenarios.

4.1 NETWORK SIMULATOR 2.28(NS2)

NS-2 is a packet – level simulator and essentially a centric discrete event scheduler to schedule the events such as packet and timer expiration centric event scheduler cannot accurately emulate " events handled at the same time" in real world, that is, events are handled one by one.

This is not a serious problem in most network simulations, because the events here are often transitory. CMU Monarch Project, has 2 assumptions simplifying the physical world. Nodes do not move significantly over the length of time they transmit or receive a packet. This assumption holds only for mobile nodes of high-rate and low-speed.

V. FETURE ENHANCEMENT

The MRA (Misbehavior Report Authentication) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. The source route broadcasts an RREQ message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcasts this new message to their neighbours. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in flat routing protocols like DSR, a RERR message is sent to the source node. When the RREQ message arrives to its final destination node, the destination node initiates an RREP message and sends this message back to the source node by reversing the route in the RREQ message.

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. 4, Issue 8, August 2016

ADVANTAGES:

❖The proposed IDS algorithm maintains the list of all the nodes which send the route reply to the source with sequence number greater than the threshold value.
❖The second scenario, we set all malicious nodes to send out false misbehavior report to the source node whenever it is possible.
❖This scenario setting is designed to test the IDS's performance under the false misbehavior report.

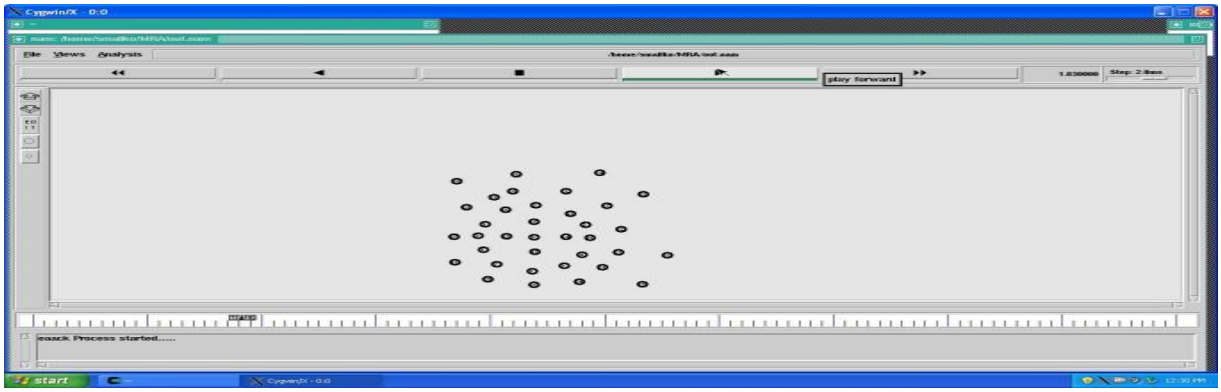

Fig.4: Creation of Node

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer **network**. Essentially, it is the **topological** structure of a **network** and may be depicted physically or logically.

Fig.5: Network Topology

We introduce a new route discovery algorithm for MANETs using chase packets.

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. 4, Issue 8, August 2016

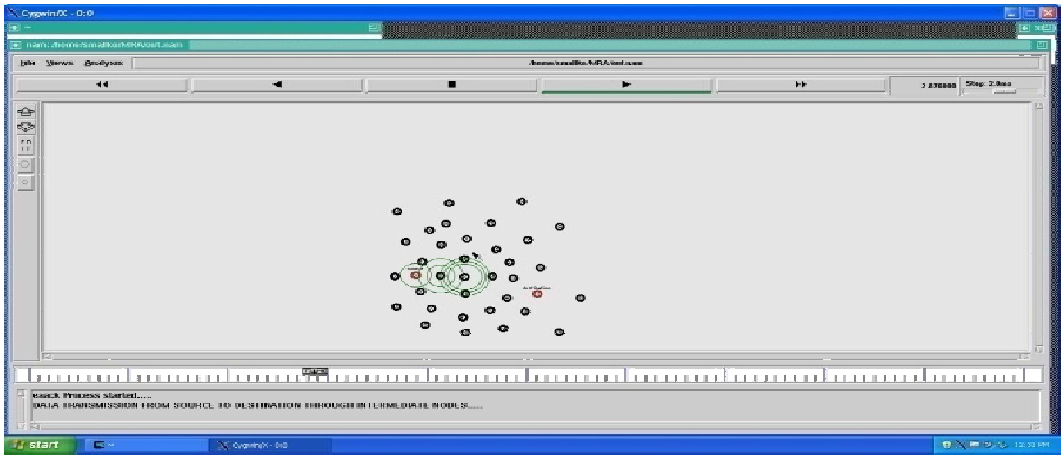

Fig.6: Route Discovery

A Secure Intrusion-Detection System for MANETs using EAACK scheme

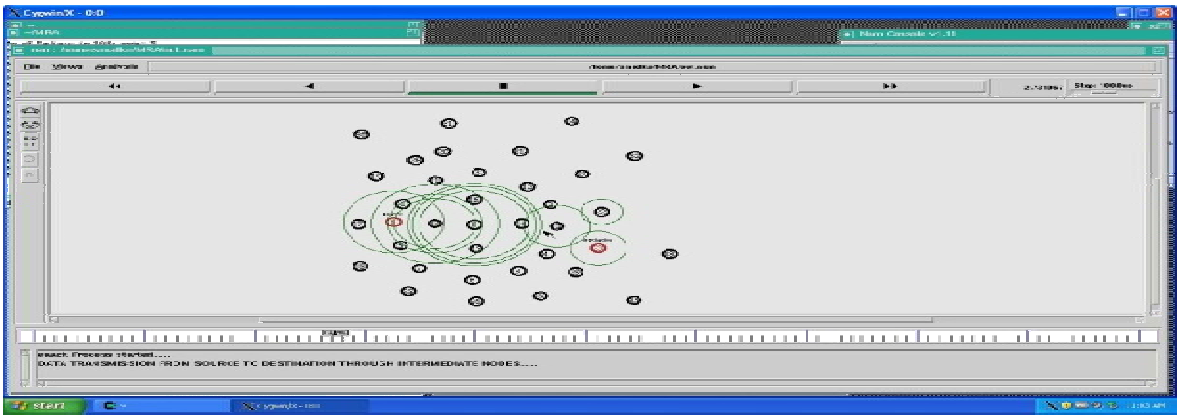

Fig.7: EAACK Process

The MRA (Misbehaviour Report Authentication) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report.

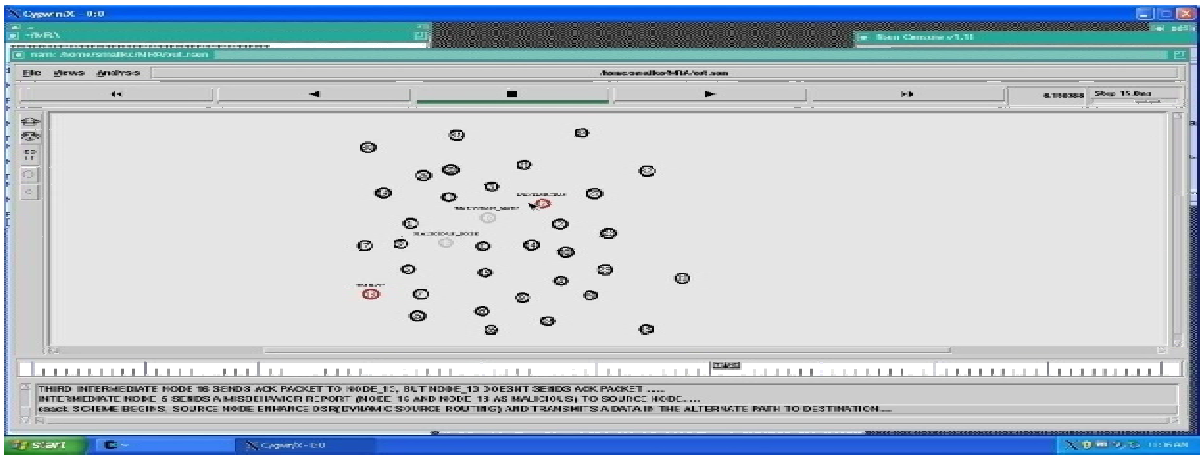

Fig.8: MRA Scheme

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. 4, Issue 8, August 2016

VI. CONCLUSION

The Proposed System is designed to resolve the weakness of Watchdog when it fails to detect misbehaviour nodes with the presence of false misbehaviour report. The false misbehaviour report can be generated by malicious attackers to falsely report innocent nodes as malicious. Packet dropping attack has always been a major threat to the security in MANETs. In this work a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulation. The results described positive performances against Watchdog, TWOACK and AACK in the cases of receiver collision and limited Transmission power and false misbehaviour report.

REFERENCES

1. A. Baadache, and A.Belmehdi, "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks," International Journalof Computer Science and Information Security," Vol. 7, No. 1, 2010.
2. V. K and A. J PAUL, "Detection and Removal of CooperativeBlack/Gray hole attack in Mobile Ad Hoc Networks," 2010 InternationalJournal of Computer Applications, Vol. 1, No.22, 2010
3. Scalable Network Technologies (SNT). QualNet.http://www.qualnet.com
4. Durgesh Kumar Mishra Mahakal Singh Chandel, Rashid Sheikh. "Security Issues in MANET: A Review".
5. Li Shi-Chang, Yang Hao-Lan, Zhu Qing-Sheng College of Computer Science Chongqing University Chongqing, China.Research on MANET Security Architecture design.
6. Vishnu K and Amos J Paul, "Detection and Removal of Cooperative Black/Gray Hole Attack in Mobile ADHOC Networks", International Journal of Computer Applications, Vol. 1, No. 22, 2010.
7. Arnab Mitra, Rajib Ghosh, Apurba Chakraborty, Santanu Kr. Sen; An Approach to Detect Black Hole Nodes in Wireless Network Using Cellular Automata; International Journal of Advanced Research in Computer Science & Software Engineering (IJARCSSE); Volume 2, Issue 9; September 2012
8. Elmar Gerhards et al.; Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs; 32nd IEEE Conference on Local Computer Networks; 2007
9. R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc Networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.
10. K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.
11. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.
12. Ashish Kumar, Vidya Kadam, Subodh Kumar, Shital Pawar, "An Acknowledgement – Based Approach for the Detection of Routing Misbehavior in MANETS" International Journal of advances in Embedded Systems, Vol.1, Issue.1,2011.