International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 03, Issue: 05 (SEPTEMBER -OCTOBER, 2017)

Security Schemes against Black hole Attack in Mobile Ad Hoc Network

Prof. Shrikant Ahirwar[1]*, Ajesh Kumar Jhariya*[2]
Department of Digital Communication Engineering
U.I.T., Barkatullah University
Bhopal, M.P., (India)
shrikant.ahirwar@gmail.com, ajeshj@yahoo.com

Abstract— The Mobile Ad hoc Network (MANET) are easily organized at any place where the mobile devices are available for communication. MANETs are normally self-organized networks and intermediate nodes ought to bearing the end-to-end communication in dynamic network. To achieve this, each node depends on its neighbour to forward the data packet to the destination. In fact, most of previous studies on MANET have implicitly assumed that nodes are cooperative As such; the node cooperation becomes a very important issue in MANETs. The attacker in MANET are easily affected the routing performance by that the data receiving ratio is affected as compare to normal performance of network and dropping of data is enhanced. In this research we proposed new IDS (Intrusion Detection System) of detecting routing misbehaviour through black hole attack. The characteristics of black hole attack is to reply the positive acknowledgement destination at time of route request and drop all the data deliver through black hole node. The attacker is identified by the historical information of data receiving and forwarding in dynamic network. The attacker is block through the broadcasting scheme used by IDS from their actual identification to neighbours. The IDS nodes are block the communication of attacker and provide the secure communication among the mobile nodes in MANET. The performance of proposed scheme is measure through performance metrics like Throughput, PDF and attacker Infection.

Keywords—Security, MANET, Routing, Attack, Survey

I. Introduction

Mobile Ad-Hoc Network (MANET) is an infrastructure less assortment of mobile nodes which will randomly modification their geographic locations specified these networks have dynamic topologies and random quality with affected resources. They even have capability of network partition. A mobile ad hoc network (MANET) is a self-organized multi-hop system comprised of mobile wireless nodes [1].

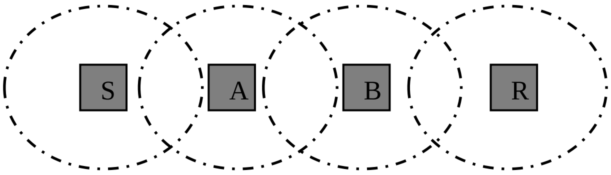

Figure1. MANET

Two nodes out of direct communication range would like intermediate nodes to forward their messages shown in figure one. The Sender S has communicate with Receiver R through intermediate nodes A and B. Common applications of MANET are: military or police networks, business operations like oil drilling platforms or mining operations and emergency response operation similar to once natural disaster like a flood, tornado, cyclone and earthquakes. Because of multi-hop routing and open operating atmosphere, MANETs are liable to attacks by self-seeking or malicious nodes, such as packet dropping (black-hole) attacks and selective forwarding (gray-hole) attacks. Black hole attack may be a style of attack that is work on established path in between sender and receiver [2]. However if the sender has begin knowledge transmission then in this case the black hole offender has produce an immediate node link to sender, observed as a black hole attack between them, it means that additional of the amount of trusty nodes it means that higher flourishing electronic communication method rates may expected. During this desertion we tend to proposed detection also as bar technique against black hole attack, for detection we tend to use profile base detection technique and obtain offender node info like node variety, variety of attack packet, attack time etc [3]. Afterward we tend to prevent black hole attack using neighbor trust worthy base technique and secure the mobile ad-hoc network communication, through our proposal we offer secure also as reliable communication and simulate through network simulator-2 and analyze the network behavior in attack and prevention case. Afterward we will also evaluate performance of network on the bases of network parameter like turnout, packet delivery ratio, throughput, routing load etc.

II. ROUTING

There are primarily three types of routing protocols [4, 5, 6]: **Proactive protocols** in networks utilizing a proactive routing protocol, each node maintain one or additional tables representing the complete topology of the network. These tables are updated often so as to keep up up-to-date routing info from every node to each alternative node. To keep up up-to-date routing info, topology info must be changed between the nodes on an everyday basis that successively ends up in comparatively high overhead on the network. The advantage is that routes can continually be obtainable for the asking.

Reactive protocols in contrast to proactive routing protocols, reactive routing protocols don't create the nodes initiate a route discovery method till a route is needed. This ends up in higher latency than with proactive protocols, however lower overhead.

Hybrid protocols every node maintains each the topology info at intervals its zone and therefore the info relating to neighboring zones meaning proactive behavior at intervals a zone and reactive behavior among zones. Thus, a route to every destination at intervals a zone is established instantaneously, whereas a route discovery and a route maintenance procedure are needed for destinations that are in alternative zones.

III. SECURITY IN MANET

Vulnerabilities of operational systems and higher layer applications that belong to user programs such as databases, browsers, or client-server applications don't seem to be thought-about as a security issue for unexpected networks [5, 6]. General attack varieties are the threats against the routing layer of the MANET adore physical, MAC and network layer that is that the most vital perform of wireless ad-hoc network for the routing mechanism, familiarizing the packets once a route discovery method. Alternative vulnerabilities are application security, network security, information security that is studied in several works that don't seem to be explained well here. Attacks to the wireless ad-hoc network within the networking layer sometimes have 2 purposes: not forwarding packets or adding and ever-changing some parameters of routing messages; adore sequence variety and information processing addresses. These are elaborate within the resulting sections. Using one in all the key mechanisms adore cryptography or authentication [7], or each in an exceedingly network, is a preventive approach and might be used against 'attackers'. However, these mechanisms defend the network against attacks that return from outside, malicious 'insiders' that use one in all the important keys also can threaten the safety. to Illustrate, in an exceedingly battle field wherever MANET are used, even though keys are protected by temper proof hardware that are utilized in the vehicles within the network, it's tough to mention that these vehicles exhibit constant behavior if the enemy captures them. On the opposite hand, a node could un-deliberately misdemeanor as if it's broken. A node with a failing battery that is unable to perform network operations could also be perceived as an attack. Another malicious behavior of the nodes is stinginess. Self-seeking nodes refrain from overwhelming its resources; adore battery, by not collaborating in network operations. Therefore, failing and self-seeking nodes conjointly have an effect on the network performance as they are doing not properly method network packets, adore in routing mechanism. We should, so make sure that everything is properly operating within the network to support overall security and identify how an insider capable to attack the Mobile ad hoc network. Wireless ad-hoc networks ought to be protected with an intrusion detection system that can perceive the doable actions of attackers and might produce a solution against these attacks.

IV. TYPES OF ATTACKS

Mobile ad hoc networks are liable to varied attacks not solely from outside however conjointly from at intervals the network itself. Ad hoc network are principally subjected to two completely different levels of attacks. The primary level of attack happens on the essential mechanisms of the unexpected network adore routing. Whereas the second level of attacks tries to break the safety mechanisms used within the network. The attacks in MANETs are divided into 2 major varieties. Network either as internal, external or/ also as active or passive attack against the network.

The connectivity of mobile nodes over a wireless link in MANETS that is multi hop in nature powerfully depends on the actual fact that ensures cooperation among the nodes within the network. Since network layer protocols forms property from one hop neighbors to all or any alternative nodes in MANET, the reassurance of cooperation among nodes is needed. The attacks in MANETS are classified into two major classes, particularly passive attacks and active attacks, consistent with the attack suggests that [5, 6, 8]. Passive attacks are those, launched by the adversaries only to snoop the info network. Such attacks identification becomes terribly tough since network itself doesn't affect and that they will reduced by exploitation powerful coding techniques. However a lively attack tries to change or destroy the data that's being changed, thereby heavy the conventional practicality of the network changed within the network. These adversaries in any approach don't disturb the operation.

a) Impersonation

A malicious node can launch several attacks during a network by masquerading as another node (Spoofing). Spoofing happens once a malicious node misrepresents its identity and also the traffic that belongs to the impersonated node is redirected to the malicious node.

b) Modification

A malicious node could attack by fixing the protocol fields of messages passed among the nodes. Malicious node will simply cause traffic subversion and denial of service by setting the false values of assorted fields within the packet like route sequence numbers.

c) Fabrication

In such sort of attack, a wrongdoer or malicious node generates the false routing info. As a result of the routing constructs comes as valid thus such reasonably attacks are tough to indentify. As an example, a false RERR route error message is generated by an assaulter that claims that a neighbor can no longer be contacted.

d) Wormhole Attack

In this sort of attack, 2 colluding malicious nodes produce a tunnel between them employing a non-public high speed network(s). This attack permits a node to short-circuit the conventional flow of routing message. The wrongdoer at one end collects the info and replays them at the opposite end exploitation tunnel.

e) Black hole Attack

An intruder can launch this attack by causing false routing information and advertise itself as having an optimum path to the destination node. As an example, a malicious node will reply for route request incorrectly while not having a lively route to the destination and causes alternative sensible nodes to route knowledge packets through the malicious node.

f) Denial of Service (DoS)

The first type of attack is denial of service, that aims to crab the provision of sure node or maybe the services of the whole unplanned networks. Within the ancient wired network, the DoS attacks are dispensed by flooding some reasonably network traffic to the target so on exhaust the process power of the target and create the services provided by the target become unavailable. However, it becomes not sensible to perform the normal DoS attacks within the mobile ad hoc networks as a result of the distributed nature of the services. Moreover, the mobile unplanned networks are additional vulnerable than the wired networks as a result of the interference-prone radio channel and the restricted battery power. Within the practice, the attacker packet delivering from predefined path.

V. Previous Work

The previous work provides the information of security scheme that provides security in MANET. Some of the scheme is mention below:-

V. Keerthika ET. Al [2] proposed Direct/indirect trust is computed using normalized Route Reply misbehavior factor, link quality, and successful deliveries to mitigate black hole attack. Trust recommendation protocol has 3 types of new routing messages, first is Trust Request Message (TREQ), second is Trust Reply Message (TREP) and third is Trust Warning Message (TWARN) These share a common message structure. Nodes travel a long distance in space among one in MANETs and are not specific of another's reliability because of not gathering sufficient evidence. The model is needed to represent uncertainty accordingly with common uncertainty. Direct/indirect trust is computed to track a node's trustworthiness in this work.

Hussain et al [9] proposed Denial of Service Attack in AODV &amp; Friend features Extraction to style Detection Engine for Intrusion Detection System in Mobile Adhoc Network. During this work Denial of Service attack is applied within the network, evidences are collected to style intrusion detection engine for MANET Intrusion Detection System (IDS). Feature extraction and rule inductions are applied to seek out the accuracy of detection engine by exploitation support vector machine. True Positive generated by the detection engine is extremely high and False Positive is suppressed to negligible. True positive are reported in no time in Lids &amp; Friend list generated by Lids are sent to the Gids module for more investigation. Global Detection Engine can generate the friend list in line with trust level, higher the trust level of the node is also used for different totally different processes like routing, and deciding the cluster head for ascendable ad-hoc networks. Feature extracted for Routing parameters and MANET Traffic generation parameters is used for various routing protocols. For detection engine machine learning algorithmic program Support Vector Machine is employed that is lightweight weighted and regarded best among the supervised learning algorithms, prediction (accuracy) generated by the SVM for input options and totally different values of C &amp; λ to established the system for given coaching and testing information sets are satisfactory.

Jing-Wei Huang et al [10] proposed Multi-Path Trust-Based Secure AOMDV Routing in unexpected Networks. During this work uses a trust based mostly multipath AOMDV routing combined with soft encoding, yielding our so-called T-AOMDV scheme. a lot of exactly, this approach consists of 3 steps: (1) Message encoding – wherever at the supply node, the message is segmented into three components and these components are encrypted using one another using some XOR operations, (2) Message routing – wherever the message components are routed on an individual basis through totally different trust based mostly multiple ways using a novel node disjoint AOMDV protocol, and (3) Message coding – wherever the destination node decrypts the message components to recover the first message.

Shreenath et al [11] planned Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs. This work concentrates on raising the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to safeguard it against flooding and black hole attacks. The planned mechanism is for flooding attack works even once the identity of the malicious nodes is unknown and doesn't use any extra network bandwidth. The performance of a little multicast cluster can degrade seriously below these kinds of attacks even the answer is obtainable. The planned algorithm provides protection against region attack in MANET.

Sujatha et al. [12] planned style of Genetic algorithmic program based mostly IDS for painter. During this work a method to research the exposure to attacks in AODV, specifically the foremost common network layer hazard, region attack and to develop a specification based Intrusion Detection System (IDS) exploitation Genetic algorithm approach. The planned system relies on Genetic algorithm that analyzes the behaviors of each node and provides details regarding the attack. Genetic algorithm control (GAC) may be a set of varied rules supported the important options of AODV like Request Forwarding Rate, Reply Receive Rate and then on.

Konate et al [13] proposed AN Attacks Analysis in mobile unexpected networks: Modeling and Simulation. In this paper present work is devoted to review attacks and countermeasures in MANET. When a brief introduction to what MANETs are and network security we tend to gift a survey of varied attacks in MANETs relating fail routing protocols. We tend to additionally gift the various tools employed by these attacks and also the mechanisms utilized by the secured routing protocols to counter them. During this outlined the conception of DoS like its varied varieties. They given many alternatives of DoS attacks met in MANETs, their operational method so the mechanisms used and also the protocols that implement them to counter these attacks.

Gandhewar et al [14] planned Detection and prevention of sinkhole Attack on AODV Protocol in Mobile Adhoc Network. This work in the main focuses on sinkhole problem, its consequences &amp; presents mechanism for detection &amp; prevention of it on the context of

AODV protocol. Depression is one among severe quite attack that makes an attempt to draw in most of network traffic towards it &amp; degrade the performance of network. AODV is principally analyzed below black hole, wormhole &amp; flooding attack, that must analyze below other forms of attack additionally. It additionally shows performance of AODV with no depression attack, vulnerable &amp; when applying our mechanism in the form of simulation result obtained surely variation of nodes in network, by considering performance metrics as output, PDR, end to end delay &amp; Packet loss.

P.K Singh et al [15] proposed an efficient prevention of black hole problem in AODV Routing Protocol in MANET. In this work a solution to the region attack in one among the foremost outstanding routing algorithmic program, ad-hoc on demand distance vector (AODV) routing, for the MANETs. The region attack is one among such security risks. During this attack, a malicious node incorrectly advertise shortest path to the destination node with a meaning to disrupt the communication. The proposed methodology uses promiscuous mode to discover malicious node (black hole) and propagates the knowledge of malicious node to any or all the opposite nodes within the network.

Table 1 Simulation parameters

Simulator Used	NS-2
Number of nodes	30, 60
Attacker	Blackhole
Security Technique	IDS
Dimension of simulated area	800m×600m
Routing Protocol	AODV
Simulation time	100 sec
Application Layer Protocol	FTP, CBR
Packet size	512 bytes, 1024 bytes
Node movement at maximum Speed	random (30 m/s)
Transmission range	550m
Propagation Type	Two Ray Ground

VI.SIMULATION AND RESULT ANALYSIS

a. **Network Simulator:** The NS-2 (Network Simulator) [49] is the discrete event driven simulator used for implementation and the simulations of the various network protocols. It is freely distributed, open source and is widely used for the research.NS-2 is also providing infrastructure for tracing, visualization, error models, etc. and to modify or creates your own modules. Using components in ns, many traffic and topologies can be generated and NAM (Network Animator) can be used for visual outputs. Network simulator is the open source event driven simulator, which is basically design for simulating the communication networks such as wire oriented network, wireless ad hoc network and wireless sensor network. NS-2 (Network Simulator) contains the various modules for the network such as routing, application layer protocol, and transport layer protocol. Performance of network can be evaluated by researchers by configuring the network in any scripting language such as tcl and Otcl. They can get the result created by NS2. NS2 is a network simulator that is open source available, described by T and it has wide area used. Network Simulator is a tool which contains various packages that are used for simulating the behavior of the network. Network topology is established using network simulator and it is used for monitor the behavior of events operating in the network. Network topology is established using network simulator and it is used to monitor the behavior of events operating in the network. Tcl is a scripting language similar to C language that uses the various functions. One alternative of using these library functions is that write code in C language. Tcl scripting language has an understanding of compiler, linker and C language. Tcl scripting language has easy syntax, so it provides easy to the functionality. It is simple to use Tcl and functionality of Tcl. OTcl script is a Tcl script, which has objected oriented functionality. OTcl script uses the OTcl classes in which.

b. **Simulation Parameter:** Table 1 represents the simulation parameters to make the scenario of routing protocols. The detailed simulation model is based on network simulator-2 (ver-2.34) [50], is used in the evaluation. The NS instructions can be used to define the topology structure of the network and the motion mode of the nodes, to configure the service source and the receiver etc.

c. **Result Analysis:**

1 PDR Performance Analysis

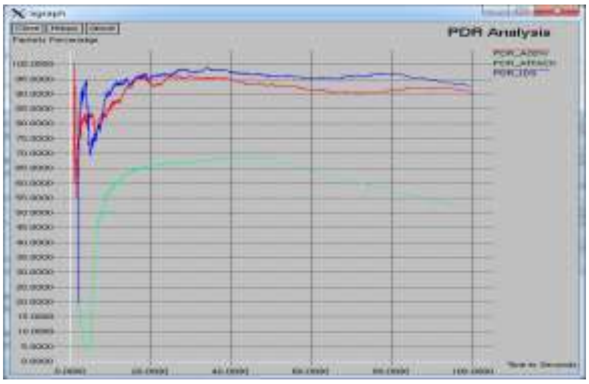

Figure.2 PDR Analysis

2 Throughput Analyses

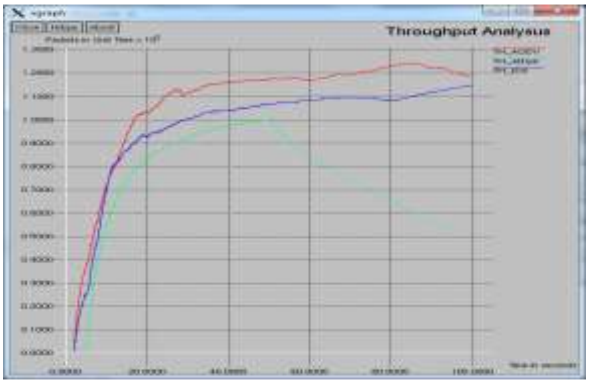

Figure.3 Throughput Analysis

3. Routing Load Analysis

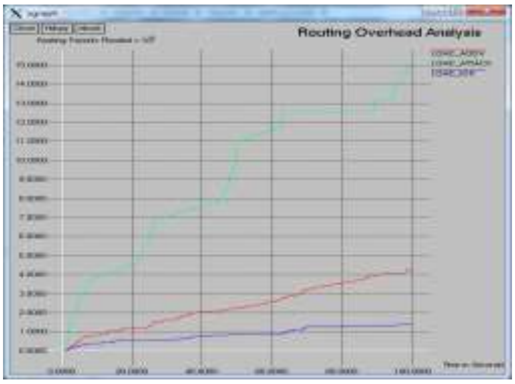

Figure 4. Routing Load Analysis

4 UDP End Packets Receiving Analysis

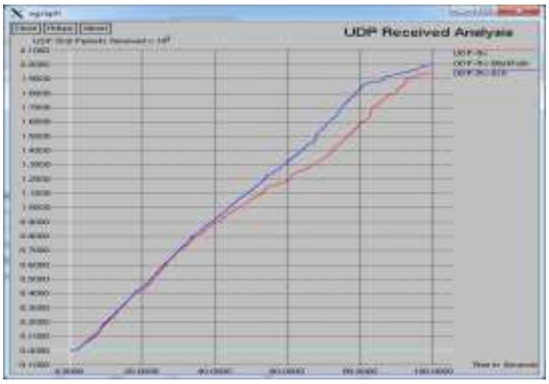

Figure 5 UDP Packet Analyses

5 Attacker Loss Analyses

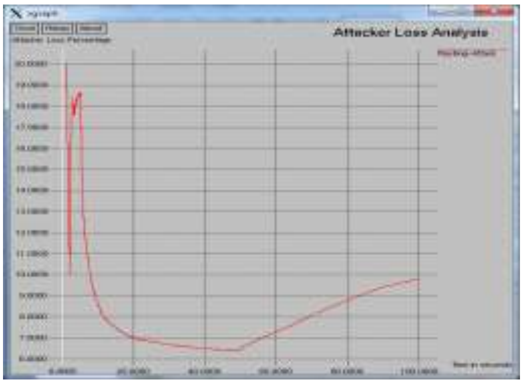

Figure 6 Attacker Loss Analyses

VII.Conclusion

Mobile Ad hoc Networks (MANETs) are eminent from other wireless networks or wired network by many features. First of them is mobile nodes in MANETs can moves freely in the lack of a fixed infrastructure unit. As a result, frequent changes in routes may happen due to unpredictable topology changes and link disconnections. Another one is nodes in MANETs has limited resources such as energy, bandwidth, and computational power and MANETs have no trusted centralized authority. The proposed IDS method is not only detect the black hole attacker but also prevent the network from it. The proposed IDS is improves the routing performance and provides the secure communication. The information of attacker is broadcast to all the nodes that are participating in routing procedure and these nodes are ignores the request of attacker if it identified again after block their existence. The attacker infection is very harmful for MANET the routing overhead, throughput and PDF are provides the negligible output but after applying proposed secure IDS scheme the routing packets flooding is minimized with enhancement of performance of throughput and PDF. The performance of proposed IDS is supposed to be equivalent to normal routing performance.

References

[1]. C. Siva Ram Murthy and B. S. Manoj, “Ad Hoc Wireless Networks, Architectures and Protocols”, Low Price Edition, Pearson Education, pp. 521, 2007.

[2]. V. Keerthika, N. Malarvizhi, " Migrate Black hole Attack using Trust with AODV in MANET", 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016.

[3]. Oscar F. Gonzalez, God win Ansa, Michael Howarth and George Pavlou. “Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks”, Journal of Internet Engineering, Vol. - 2, no.1, 2008.

[4]. Sunil Taneja and Ashwani Kush A Survey of Routing Protocols in Mobile Ad Hoc Networks International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010.

[5]. Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", Journal Of Computing, Volume 3, Issue 1, January 2011.

[6]. K.P. Manikandan, Dr. R. Satyaprasad, Dr. K. Rajasekhararao, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.

[7]. S. Yi and R. Kravets, “Composite Key Management for Ad Hoc Networks”. Proceedings of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous’04), pp. 52-61, 2004.

[8]. K. Sivakumar, Dr. G. Selvaraj, “Overview of Various Attacks in MANET and Countermeasures for Attacks” International Journal of Computer Science and Management Research Vol 2 Issue 1 January 2013.

[9]. Husain. Shahnawaz, Gupta S.C., Chand Mukesh “Denial of Service Attack in AODV & Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Adhoc Network”, International Conference on Computer & Communication Technology (ICCCT-2011), pp. 292- 297, 2011.

[10]. Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, Ting-Yun Chi, Sanjay K. Dhurandher “Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks”, proceedings of IEEE Global Telecommunications Conference (GLOBECOM 2011), pp. 1-5, 2011.

[11]. Dr. N. Sreenath, A. Amuthan, & P. Selvigirija “Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs”, International Conference on Computer Communication and Informatics (*ICCCI* -2012), pp. 1-7, 2012.

[12]. K. S. Sujatha, Vydeki Dharmar, R. S. Bhuvaneswaran “Design of Genetic Algorithm based IDS for MANET”, International

Conference on Recent Trends in Information Technology (ICRTIT), pp. 28-33, 2012.

[13]. Dr Karim KONATE, GAYE Abdourahime “Attacks Analysis in mobile ad hoc networks: Modeling and Simulation”, 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, pp. 367 – 372, 2011.

[14]. Gandhewar, N., Patel, R. “Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network”, Fourth International Conference on Computational Intelligence and Communication Networks (CICN), pp. 714 – 718, 2012.

[15]. P.K Singh, G. Sharma, “An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET”, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 902 – 906, 2012.

[16]. K. S. Sujatha, Vydeki Dharmar, R. S. Bhuvaneswaran “Design of Genetic Algorithm based IDS for MANET”, International Conference on Recent Trends in Information Technology (ICRTIT), pp. 28-33, 2012.

[17]. Dr Karim KONATE, GAYE Abdourahime “Attacks Analysis in mobile ad hoc networks: Modeling and Simulation”, 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, pp. 367 – 372, 2011.

[18]. N. Gandhewar, R. Patel, “Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network”, Fourth International Conference on Computational Intelligence and Communication Networks (CICN), pp. 714 – 718, 2012.

[19]. P.K Singh, G. Sharma, “An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET”, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 902 – 906, 2012.

[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”, 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), pp. 1-5, 2011.

[21]. Yi Zhang, QiangLiu “A Real-Time DDoS Attack Detection and Prevention System based on per-IP Traffic Behavioral Analysis”, 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), pp. 163 – 167, 2010.