iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** V **Month of publication:** May 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Intrusion Detection System Against Multiple Blackhole Attacks In Ad-Hoc Networks Using Wireless Antnet

Sunny Chanday[1], Rajeev Kumar[2], Dilip Kumar[3]
[1]*M.Tech student, Department of Computer Science Engineering, DAV Institute of Engineering & Technology, Jalandhar, Punjab, India*
[2]*Assistant Professor, Department of Information Technology, DAV Institute of Engineering & Technology, Jalandhar, Punjab, India*
[3]*Associate Professor, Department of Electronic Communication Engineering, Sant Longowal Institute of Engineering and Technology Longowal, Punjab, India*

Abstract— A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. The open medium and wide distribution of nodes makes MANET vulnerable to malicious attacks. To address the security, it is essential to develop an Intrusion Detection System (IDS) specially designed for MANET which can detect malicious attacks before they do any significant damage to the network. For this concern a secure intrusion detection system, EAACK was developed which solves the limitations of earlier systems. In this paper we are implementing the Intrusion Detection System against the multiple Blackhole attacks in Mobile Ad-Hoc Networks using ANTNET. Our proposed Intrusion Detection System is compared to previous state of system without any IDS technique and found out to be better.
Keywords—Ant Colony Optimizationt (ACO) ; Blackhole attack; Intrusion Detection System (IDS); Mobile Ad-Hoc Networks (MANET); AODV; Wireless ANTNET.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a network consisting wireless mobile nodes that conversation with each other without centralized control or established infrastructure. These nodes which are inside each and every one radio range can convey precisely, while distance nodes count on their neighboring nodes to forward packets. In MANETS every node can be a host or router. Mobility, an advantage of wireless communication, allows a freedom of moving around although being linked to a network environment. Ad-hoc networks are so adaptable that nodes can join and move a network easily as compare to wired network. Such networks can be used in the battlefield application, in disaster management and in remote areas where establishment and management of fixed network is not possible.

The distinctive attributes of MANET has made it useful for a large number of applications. These applications include various types of commercial (intelligent transportation system, ad hoc gaming, smart agriculture) and non-commercial applications (military applications, disaster recovery, wild life monitoring) etc. One of the serious attacks to be considered in ad hoc network is DDoS attack. A DDoS attack is a large-scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending an extremely large volume of packets to a target machine through the simultaneous cooperation of a large number of hosts that are distributed throughout the network. The attack traffic consumes the bandwidth resources of the network or the computing resource at the target host, so that legitimate requests will be discarded. A bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system. If the ad hoc network lacks some form of network level or link layer security, a MANET routing protocol will be more vulnerable to many forms of malicious attacks. It can be simple attack like snooping network traffic, transmissions replay, manipulation of the packet headers, and redirecting the routing messages, within an Ad hoc network without any appropriate security provisions. In Black hole attack, malicious nodes get a chance to attack during route discovery process. A black hole means that one malicious node apply the routing protocol to affirm itself of having shortest path to the destination node, and drops routing packets and does not send packets to its adjacent node. A single Black hole node can easily attack on mobile Ad hoc networks. There is various detection schemes for detecting single black hole, but failed when cooperative black hole attack occurs. Cooperative black hole attack means malicious nodes act in a group. In this attack, one

malicious node receives data and forwards it to other malicious node instead of forwarding it towards destination.

Ant Colony Optimization (ACO) [1] was proposed by Italian scholar M. Dorigo and colleagues as a method for solving hard combinatorial optimization problems. The inspiring source of ACO algorithms are real ant colonies. More specifically, ACO is inspired by the ants' foraging behavior. At the core of this behavior is the indirect communication between the ants by means of chemical pheromone trails, which enables them to find short paths between their nest and food sources.

II. LITRATURE SURVEY

The various techniques that have been applied to detect malicious node in network are discussed in this section. Following are several different approaches for intrusion detection system.

S. Marti, T. J. Giuli, K. Lai, and M. Baker [2] proposed a watchdog and pathrater scheme of intrusion detection system for MANET is introduced that aims to improve the throughput of network with the presence of malicious nodes [3]. Watchdog is able to detecting malicious nodes rather than links. The watchdog is based on reactive feedback that is overhearing to confirm whether the next node has forwarded the packet or not. Pathrater works as response system. Once Watchdog node identifies malicious node in the network, the pathrater cooperates with the routing protocols to avoid the reported node in the future transmission. The standard is Dynamic Source Routing protocol (DSR) in that the routing information is defined at the source node [4].So because of this it might not detect a misbehaving node in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior report, collusion and partial dropping.

N. Nasser and Y. Chen [5] proposed ExWatchdog which extends from Watchdog proposed in that solving the problems of the Watchdog scheme which is the false misbehaving problem, where a malicious node falsely reports other nodes as misbehaving while in fact it is the real intruder. When the source receives a report about misbehaving node, it will find another path to ask the destination node about the number of received packets. If it is equal to the packets that the source has sent, then the real malicious node is the node that reports other nodes as misbehaving. Otherwise node being reported malicious do misbehave. But there is limitations in this scheme if the true misbehaving node is in the all available paths from source to destination then it is impossible to confirm and check the number of packets with the destination

Kassabalidis et al. [6] proposed Ant-Net algorithm which realizes routing optimization through the forward ants and return ants (forward ants collect node information; return ants use this information update routing table). And ABC algorithm [7] (ant based control algorithm) is based on probability of mode selection and updates the path. This algorithm is only one kind of ants released from source nodes and these ants arrived at destination node after death. The node's routing table will be updated, when the ant arrives at the destination node.

In this paper [8], they proposed a method uses Intrusion Detection using Anomaly Detection (IDAD) to defend against black hole attacks established by both single and multiple black hole nodes. It proved the specific result increases network performance by reducing formation of control (routing) packets including effectively defend black hole attacks opposed to mobile ad-hoc networks.

In this paper [9], they proposed two possible solutions to study black hole attack. The first solution is to study several route to the destination. The second is to apply the packet sequence number contained in any packet header. In study to AODV routing scheme, the second solution is superior and of the route to the destination rely upon on the pause time at a lowest cost of the delay in the networks.

In this paper [10], they have proposed a solution the requesting node wait and check the replies from all neighboring node to find a safe route. It is provide better performance than the conventional AODV in the existence of Black holes with smallest additional delay and overhead.

Al-Roubaiey, T. Sheltami, A. Mahmoud , E. Shakshuki and H. Mouftah [11] proposed a AACK is a network layer acknowledgement based scheme which detects misbehaving node instead of misbehaving link and an end to end acknowledgment based scheme, to reduce the routing overhead of TWOACK. The AACK scheme may not work well on long paths that will take a significant time for the end to end acknowledgments. This limitation will give the misbehaving nodes more time for dropping more packets. AACK still suffers from the partial dropping attacks and false misbehavior report.

Elhadi M. Shakshuki, Nan Kang and Tarek R. Sheltami [12] proposed EAACK scheme with digital signature to prevent the attacker from forging acknowledgment packets. All acknowledgment packets described in this research are required to be digitally signed by its sender and verified by its receiver, because of that it causes the network overhead.

Durgesh Wadbude and Vineet Richariya [13] proposed secure Ad hoc On Demand Distance Vector Routing (AODV) a novel algorithm for the operation of such ad hoc networks. Each Mobile node operates as a specialized router and routes are obtained on demand.

III. BLACKHOLE ATTACK

Black hole attack is a special attack in which there are many types it can be occurred. One type of black hole attack can occur when the malicious node on the path directly attacks the data traffic by intentionally dropping, delaying (or) altering the data traffic passing through it [5]. By setting the promiscuous node to each node and listening to see if the next node on the path forward the data traffic as expected, this type of black hole attack can be easily mitigated. Another type of black hole attack used by a malicious node which makes all the traffic travel through it by claiming to have the shortest route to all other nodes in the network[5]. So after this, the malicious node simply drops the packets instead of forwarding the packets. The main concept of black hole attack is that it creates a fake root reply packet that initiates a route delivery to a source node. A variant of black hole is the grayhole attack in which it transmits some packets selectively and drops others.

An example is shown as Figure 1, node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. As what mentioned above, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs.

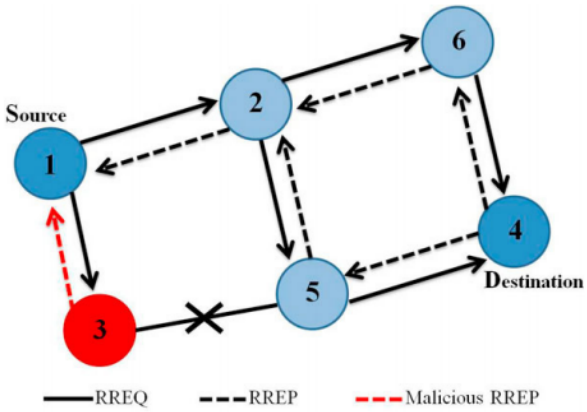


Figure 1: Single Blackhole Attack Problem

As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem.

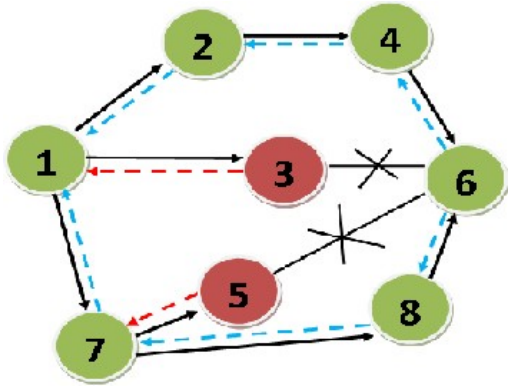


Figure 2: Multiple Blackhole Attack

IV. PROPOSED MECHANISM

The proposed algorithm is designed to prevent any alterations in the default operations of either the intermediate nodes or the destination nodes. After analyzing the effect of black hole attack in MANETS, we modify the AODV Protocol and ANTNET Protocol to Wireless ANTNET. We used Ant colony optimization to find path from source to destination.

The proposed algorithm is divided into major steps:

The first step is based on the routing messages of both RREQ and RREP messages that are exchanged in the route discovery in AODV Protocol.

The second step is based on the DSN of the RREP message, the number of RREP message(s) calculated in the first step and the

arrival time of RREP at the source.

The first stage of the proposed algorithm includes monitoring all the RREQ and RREP messages between the source and destination nodes. A Route Reply Table (RRT) is created to store any RREP message(s) from destination node.
As mentioned above, black hole node sends a fake RREP message with maximum node sequence number to the source node in order to pose itself as a destination or an intermediate node. So, the source node sends data to it. To avoid this process, we consider that the source node must wait a time equals the double value of RREP-WAIT-TIME, before sending data, in order to receive more RREP messages. Once the source node receives the RRRP message(s) it will store its sequence number and the time at which the message(s) arrives in a table. In our implementation we refer to this table by Route Reply Table (RRT).
Throughout the second stage, when the source node receives the RRRP message(s) it will store its destination sequence number and the arrival time in RRT. When the timer RREP-WAIT-TIME expires, then the proposed algorithm checks the number of RREP messages in RRT. The emergence of more than one RREP message means there is a threat of black hole attack. In the case of receiving only one RREP message, the destination node is considered trusted node and all data will be send to it. Receiving more than one RREP message means that one of these messages is created by the trusted destination node and the other message(s) are created by black hole node(s).

V. SIMULATION AND PERFORMANCE EVALUATION

Network Simulator (Version 2), widely known as NS2, is popular simulator in scientific environment. It is a discrete event simulator targeted at network research and focused on modeling network protocols such as ad hoc routing, sensor networks etc also NS2 is based on two languages. They are object oriented simulator (C++) and OTcl (object oriented Tcl) interpreter. In this paper, we presented our research model testing result, which is shown in graph. Here we analyzed some performance metrics like, Packet Delivery Ratio, Normalized Routing Load,

Table No 1. Set personal preference value on different factors

Parameters	Values
Simulator	NS 2
Simulation Time	80 s
Number of Nodes	10
Routing Protocol	AODV, ANTNET
Traffic Model	cbr
Pause Time	5 s
Mobility	Upto 3m/s
Terrain	500 x 400 m
Malicious Nodes	3

A. Packet Delivery Ratio

Packet delivery ratio is defined as a number of packets successfully send and receive transmitted packets between source and Destination.

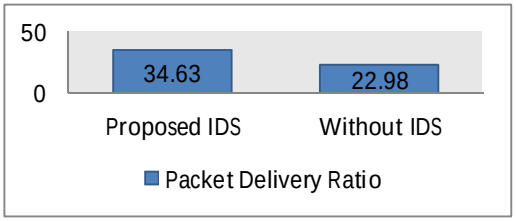


Fig.3 Comparison of (a) Packet Delivery Ratio of Proposed IDS with system without IDS.

Figure 3 clearly shows the that the proposed IDS is having more packet delivery ratio as compared to without IDS.
The proposed IDS is having packet delivery ratio of 34.63 in contrast to 22.98 which is the packet delivery ratio without IDS.

B. Normalized Routing Load

The number of routing packets transmitted per data packet delivered at the destination. Each hop -wise transmission of a routing packet is counted as one transmission. The figure 4 shows that the proposed IDS is having less normalized routing load of 0.0284 as compared to 0.0391 of normalized routing load of system without IDS.

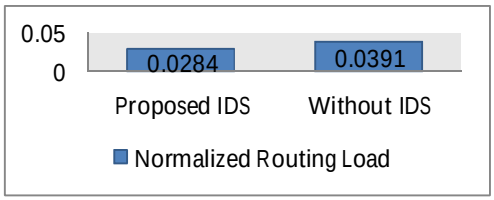


Fig. 4 Comparison of (a) Normalized Routing Load of Proposed IDS with system without IDS.

VI. CONCLUSIONS

We have proposed Intrusion Detection System based on Wireless ANTNET. The results clearly show that it is more successful in detecting the malicious nodes as compared to without having any detection system. Moreover, the normalized routing load is less in proposed method. The packet delivery ratio of proposed IDS with Wireless ANTNET is more as compared with without any IDS system. Our future work will be focused on how to apply the proposed IDS using other swarm intelligence techniques.

REFERENCES

[1] Dorigo, M.; Di Caro, G., "Ant colony optimization: a new meta-heuristic," Evolutionary Computation, 1999.

[2] S. Marti, T. J. Giuli, K. Lai and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks”, in Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255-265, ACM 2000.

[3] U. SharmilaBegam and Dr. G. Murugaboopathi, “A Recent Secure Intrusion Detection System for MANETs”, International Journal of Emerging Technology and Advanced Engineering (IJETAE), Vol. 3, Special Issue 1, pp. 54-62, January 2013.

[4] Anantvalee, Tiranuch and Jie Wu., “A survey on intrusion detection in mobile ad hoc networks”, in Wireless Network Security, pp. 159- 180, Springer US, 2007.

[5] N. Nasser and Y. Chen, “Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network”, in IEEE International Conference on Communications (ICC’07), pp. 1154- 1159, Jun 24–28, 2007.

[6] I.Kassabalidis, M. A. El-Sharkawi,R. J.Marks, P. Arabshahi, and A. A. Gray, “Swarm intelligence for routing in communication networks,” Global Telecommunications, vol. 6, no. 6, pp. 3613– 3617, 2001.

[7] B. McBride, C. Scoglio, and S. Das, “Distributed biobjective ant colony algorithm for low cost overlay network routing,” in Proceedings of the International Conference on Artificial Intelligence (ICAI ’06), vol. 2, pp. 518–521, June 2006.

[8] Yibeltal Fantahun Alem Zhao Cheng Xuan, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection" IEEE 2nd International Conference on Future Computer and Communication (ICFCC), pp.V3-672 - V3-676, 21 to 24 MAY 2010.

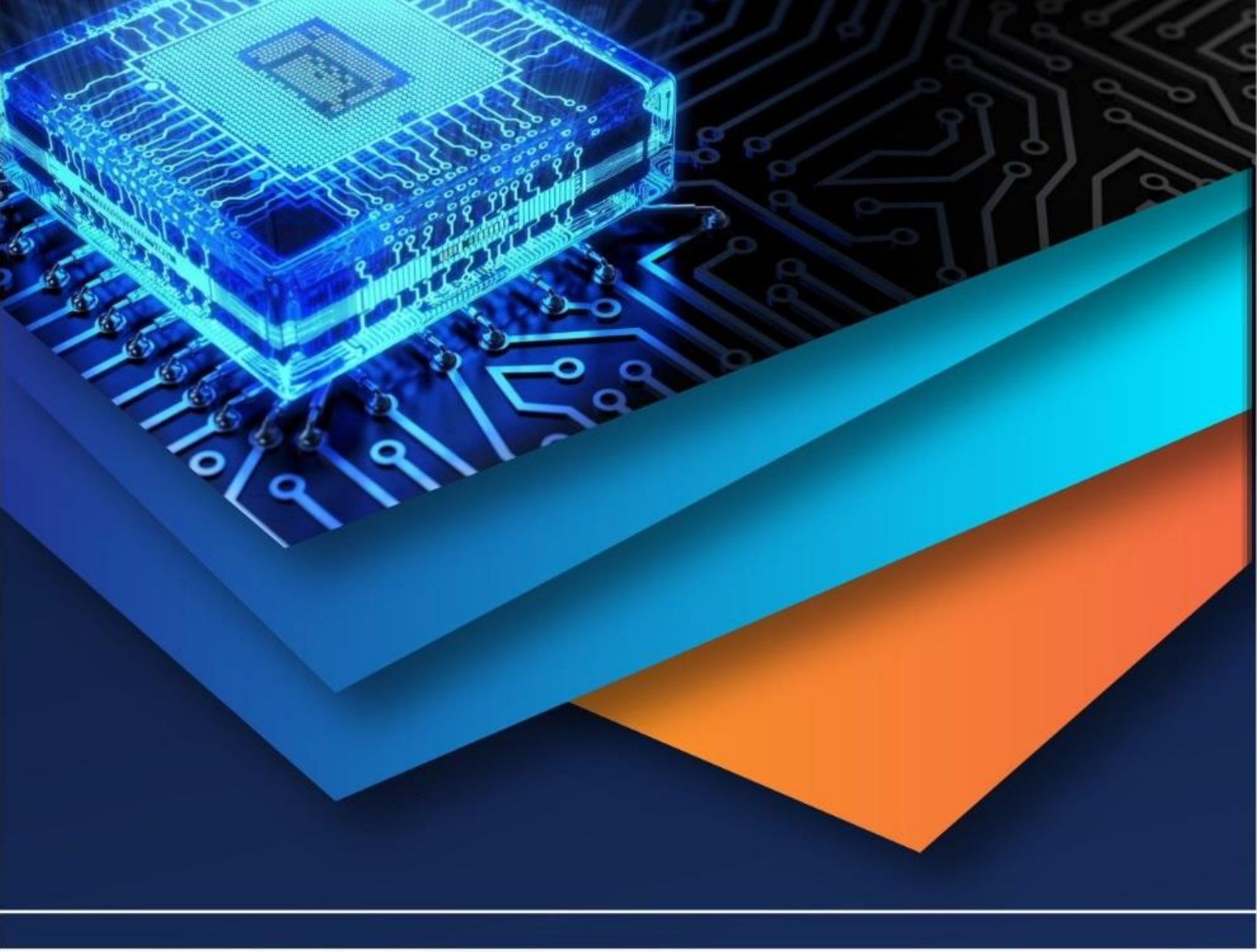
[9] Ms Nidhi Sharma, Mr Alok Sharma “The Black-hole node attack in MANET" 2012 Second International Conference on Advanced Computing & Communication technologies, 546-550 2012 IEEE.

[10] Latha Tamilselvan, Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", In Proceedings of IEEE 2nd International Conference on Communications, IEEE 2007.

[11] Al- Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki and H. Mouftah, “AACK-Adaptive Acknowledge Intrusion Detection for MANET with Node Detection Enhancement”, in 24thIEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 634-640, 2010.

[12] Nan Kang, Elhadi M. Shakshuki and Tarek R. Sheltami, “ EAACK –A Secure Intrusion-Detection System for MANETs”, IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, pp. 1089- 1098, March 2013.

[13] DurgeshWadbude and VineetRichariya, “An Efficient Secure AODV Routing Protocol in MANET”, International Journal of Engineering and Innovative Technology (IJEIT), Vol. 1, Issue 4, pp. 274-279. April 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY