iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VII **Month of publication:** July 2015

DOI:

www.ijraset.com

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

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

Eaack Based Intrusion Detection Technique for Manet's

Mr Ganesh Murgod[1], Asst Prof Deepa Bendigeri[2], Dr Jagadeesh Pujari[3]
[1,3]*Information Science Department, VTU University*

Abstract— The defection to wireless technology from wired technology has been a global shift in the past few decades. The open system and remote distribution of nodes make MANET endangered to intruders. An emerging technique EAACK (Enhanced Adaptive Acknowledgement) method designed for MANET was proposed for intrusion detection. EAACK exhibit higher mis-behavior detection rates in situation where it does not cost for the network performances.
Keywords— Enhanced Adaptive ACKnowledgement (EAACK), Mobile Adhoc NETwork (MANET), and Elliptic Curve Cryptography (ECC).

I. INTRODUCTION

Due to their natural quality and quantifiability wireless networks area unit perpetually most popular since the primary day of their invention. Because of the improved technology and reduced prices, wireless networks have gained rather more preferences over wired networks within the past few decades. Formally, MANET is a set of mobile nodes equipped with each a wireless unit of transmitter and a receiver that communicates with one another via two way wireless links. One in all the key blessings of wireless networks is its ability to permit electronic communication between completely different parties and still maintain their quality. However, this communication is restricted to the vary of transmitters. This implies that 2 nodes cannot communicate with one another once the space between the 2 nodes is on the far side the communication varies of their own. MANET solves this drawback by permitting intermediate par- ties to relay information transmissions. This is attained by separating MANET into two types of networks, namely, single-hop and multi hop. During a single-hop network, all nodes among a similar radio frequency communicate directly with one another. On the opposite hand, during a multi hop network, nodes allow different intervening nodes to communicate if the destination node is out of their transmission range. In contrary to the normal wireless network, MANET incorporates a suburbanized network infrastructure. MANET doesn't need a hard and fast infrastructure; therefore, all nodes area unit unengaged to move arbitrarily .MANET is capable of making a self-configuring and self-maintaining network while not the assistance of a centralized infrastructure, that is commonly unfeasible in crucial mission areas like Warfield. Tokenish configurations Associate in fast preparation create MANET able to be utilized in emergency circumstances wherever an infrastructure is unavailable no cooperative nodes into the network. What is more, as a result of MANET's distributed design and dynamical topology, a conventional centralized observance technique isn't any longer possible in MANETs. In such case, it's crucial to develop Associate in nursing intrusion detection system (IDS). or impracticable to put in cases like natural or human-induced disasters, military Warfield etc.

II. RELATED WORK

Intrusion detection is defined as the technique to identify "the activities that attempt to incorporate the uprightness of a resource". For MANETs, the general function of IDS is to detect disoperation by watching the networks traffic in a mobile network. There are two important models of Intrusion detection systems namely: signature based and anomaly based approaches. A signature-based IDS monitors activities on the networks and compares them with known attacks. However, a drawback of this approach is that new unknown threats cannot be detected. In anomaly-based detection, contour of normal behavior of systems, usually achieved with automated training, are compared with the actual activity to flag any noticeable difference. A training phase in anomaly-based intrusion detection determines characteristics of normal activity; in operation, unknown activity, which is usually statistically and significantly different from what was determined to be normal, is flagged as suspicious. Anomaly detection can detect unknown attacks, But the issue is that anomaly based approaches yield high false positives for a wired network. If these statistical approaches are applied to MANET, the false positive problem will be worse because of the unpredictable topology changes due to node mobility in MANETs. The specification based approach, is recently presented and is ideal for new environments, such as MANETs. In specification-based detection, the correct behaviors of critical objects are taken as security specifications, which are compared to the actual behavior of the objects. Intrusions, which usually cause an object to behave in an incorrect manner, can be detected without exact knowledge about the nature of the Intrusions. Currently, specification-based detection has been applied to privileged programs, applications, and several network

protocols. Security is most important service in MANETs.
Discovering malicious nodes

A. *Watchdog*

It is very popular and highly efficient IDS for improving the output of network with the presence of corrupted nodes. These IDS can be classified into two methods such as Watchdog and Path rater. It is responsible for discovering corrupted node disoperation in the network. Watchdog finds out malicious disoperation by listening to its next hop's transmission in the network. If a Watchdog IDS overhears that its next node fails to send the packet within a predefined time interval, the failure counter is incremented. Whenever a node's failure counter exceeds a predefined threshold value, the Watchdog node reports it as disoperation. In this scenario, the Path rater collaborates with the routing Protocols to avoid the attacker nodes in further communication. The Watchdog-IDS fails to discover malicious nodes in the following situations: 1) partial dropping; 2) false misbehaviour report; 3) ambiguous collisions; 4) receiver collisions; 5) collusion and 6) limited transmission power.

B. *Two-Ack*

It is another important IDS TWOACK for discovering malicious nodes in MANETs [6] .The main aim of this IDS to solve the receiver collision and less transmission power issues, TWOACK detects misbehaving paths by acknowledging every data packet sent over every three successive nodes in the path between source and destination. Upon recovery of a packet, every node along the path has to return back an acknowledgment packet to the starting that is two distance(hops) away from it in the path. TWO-ACK involves a routing procedure like Dynamic Source Routing (DSR).

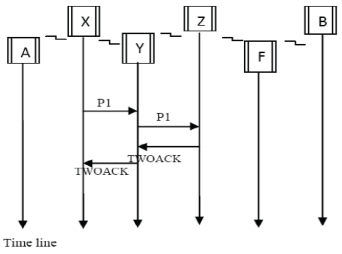


Fig. 1 TWOACK IDS for MANETs

In Fig 1: Node X wants to transmit the Packet 1 to node Y, and then, node Y transmit the Packet 1 to node Z. When node Z receives Packet 1, because it is two hops away from node X, node Z is produce a TWOACK packet, that contains reverse route from node X to node Z, and sends it back to node X. The Reclaim of this TWOACK packet at node X tells us that the imparting of Packet 1 from node X to node Z is correct and successful. Else, if TWOACK packet is not received within predefined time, both nodes Y and Z are reported as harmful. The same method is applied to every three consecutive nodes along the remaining path. The TWO-ACK IDS effectively processes the receiver collision and limited transmission power issues of Watchdog. However, the acknowledgment process involved in every packet dispatch process added a remarkable network overhead. Due to the battery problem of MANETs, such redundant transmission process will degrade the life of the whole system.

C. *AACK*

It is same as TWOACK IDS, AACK IDS is an acknowledgment-based network layer IDS. It can be treated as a combination of an ID called TACK (similar as TWOACK) and an end-to-end acknowledgment intrusion detection technique called Acknowledge (ACK). Compared to TWOACK IDS, AACK IDS reduced network overhead. The end-to-end ACK IDS is shown in Fig. 3. The source node A sends out Packet 1 without any overhead. All the intervening nodes simply send this packet. When the destination node B gets Packet 1, the source node needs to get back an ACK acknowledgement packet in reverse order of same path. Within a predefined time slot, if the source node A receives this ACK packet, then the packet transmission from node A to node B is successful. Otherwise, the source node A will switch to TACK IDS by delivering a TACK packet. The idea to take on a hybrid IDS in Adaptive ACK greatly reduces the overhead of network, but both TWOACK and Adaptive-ACK still suffer from the problem of detecting malicious nodes with the existence of false misbehavior report and fake ACK packets. As many of intrusion detection systems in MANETs have an acknowledgment-based scheme, such as TWOACK and Adaptive-ACK. The functions of these systems all largely depend on the ACK packets. Hence, there is no assurance that the acknowledgment packets are bona fide and genuine. In view to this, a digital signature is adopted in recent secure IDS named Enhanced AACK (EAACK).

Volume 3 Issue VII, July 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

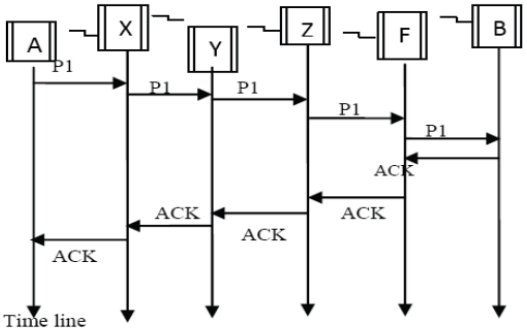


Fig. 2 End-to-End ACK IDS for MANETs

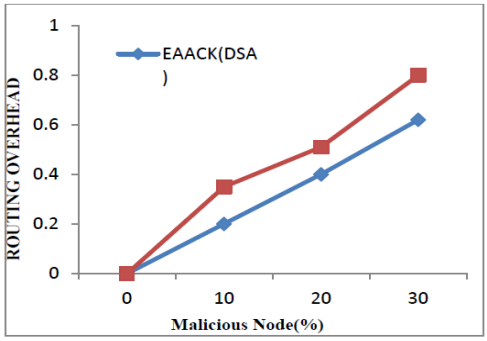


Fig 3 Routing overhead

III. PROPOSED SYSTEM

Secure IDS architecture (EAACK) was introduced on basis of security attributes and various algorithms, like RSA and DSA. EAACK is crafted to overcome three drawbacks of Watchdog IDS, namely, 1) Receiver collision, 2) Limited transmission power, 3) False misbehavior. Receiver collisions*:* As shown in Fig. 3, after node X sends Packet 1 to node Y, it tries to overhear if node Y forwarded this packet to node Z; meanwhile, node F is forwarding Packet 2 to node Z. In such case, node X overhears that node Y has successfully forwarded Packet 1 to node Z but failed to detect that node Z didn't get this packet because of collision between Packet 1 and Packet 2 at node Z.

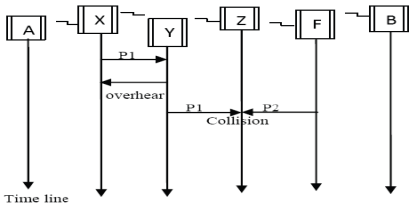


Fig. 4 Receiver collisions in MANETs

imited transmission power: Example of Limited power, shown in Fig. 5, in order to manage the battery resources in MANETs, node Y limits its transmission power so it is very strong to be overheard by node X after transmitting the packet (P1) to node Z , but too weak to reach node Z because of transmission power can be reduced

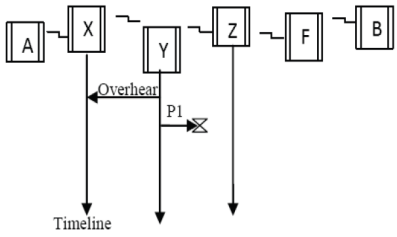
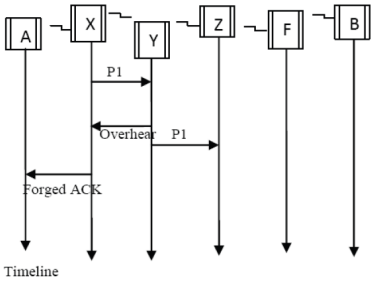


Fig. 5 Limited transmission power in MANETs

False misbehavior**:** Example of false misbehavior in MANETs, shown in Fig. 6, Even though node X and Y forwarded Packet 1 to node Z successfully, node X still inform node Y is behaving improper, as in the below figure. Due to the open medium system of MANETs, intruders can easily gain control over one or two nodes to attain this false misbehavior report attack. As mentioned earlier, TWOACK and AACK resolve two of these three weaknesses, namely, limited transmission power and receiver collision. But, both of them are endangered to the false misbehavior attack.



. Fig 6 False misbehavior in MANETs

IV. IMPLEMENTATIONS

A. *Secure Ids Description*

EAACK has three important fragments namely, ACK, secure ACK (S-ACK), and Misbehaviour Report Authentication (MRA). In order to differentiate different packet types in different strategies to include a 2-b packet header in the proposed method. As stated in DSR [7], there is 6 b guarded in the DSR header. But in this technique, use 2 b of the 6 b to flag various types of packets.

Data	ACK	S-ACK	MRA

Fig. 7 EAACK protocol in MANETs

In these secure IDS, there is a bi-directional link between nodes. Furthermore, for each transmission process, both source and destination nodes are not corrupted. All acknowledgment packets are required to be digitally signed and verified.

1) *ACK*: ACK is an end-to-end ACK technique. It aims to lower network overhead when no network wrongdoing is detected. Consider this case, first source node forwards an ACK data packet to the destination node D. Source and Destination along with all intermediate nodes are interactive and node D successfully receives packet, node D is required to return back an ACK acknowledgment packet to source but in a reverse order. Within estimated time, if source node receives packet, then the packet transmission from source to destination is correct. Else, the source node will change to S-ACK mode by forwarding a S-ACK data packet to look out for the misbehaving nodes in the path.
2) *S-ACK*: It is an improved version of the TWOACK IDS [6].For every three successive nodes in the path, the third node has to return back an S-ACK acknowledgment packet to the node, from where it started. The purpose of implementing S-ACK mode is to identify misbehaving nodes in the existence of receiver collision or limited transmission power.
3) *MRA*: Unlike the TWOACK technique, where the source node has confidence over the misbehavior report, it switches to MRA mode and guarantees this misbehaviour report. The MRA field is crafted to overcome the drawbacks of Watchdog as it fails to recognize misbehaving nodes. The false misbehaviour report can be produced by intruders to falsely report innocent nodes as corrupt. The core of MRA field is to verify whether or not the destination node has received the announced missing packet through another path. To start the MRA mode, the source node searches first its local knowledge base and gets for an alternative path to the destination. If there exists no path, the source calls for DSR routing technique to search another path. Because of Manet's architecture, it is easy to find out multiple paths. When the destination gets an MRA packet, it looks out in its local knowledge base and verifies if the reported packet is present. If it is already present, then we can say that this is a corrupted report and whoever produced this report is marked as intruder. Otherwise, the misbehaviour report is believed and taken for granted.
4) *Digital Signature:* As all techniques in EAACK are acknowledgment-based techniques. They all depend on ACK packets to find misbehaviours in the system. Thus, it is predominant to ensure that all acknowledgment packets in the proposed method are secured and trusted. Otherwise, if the intruders are smart enough to forge ACK packets. To overcome this problem, we need to implement digital signature.

B. Secure Ids In Dsa And Rsa

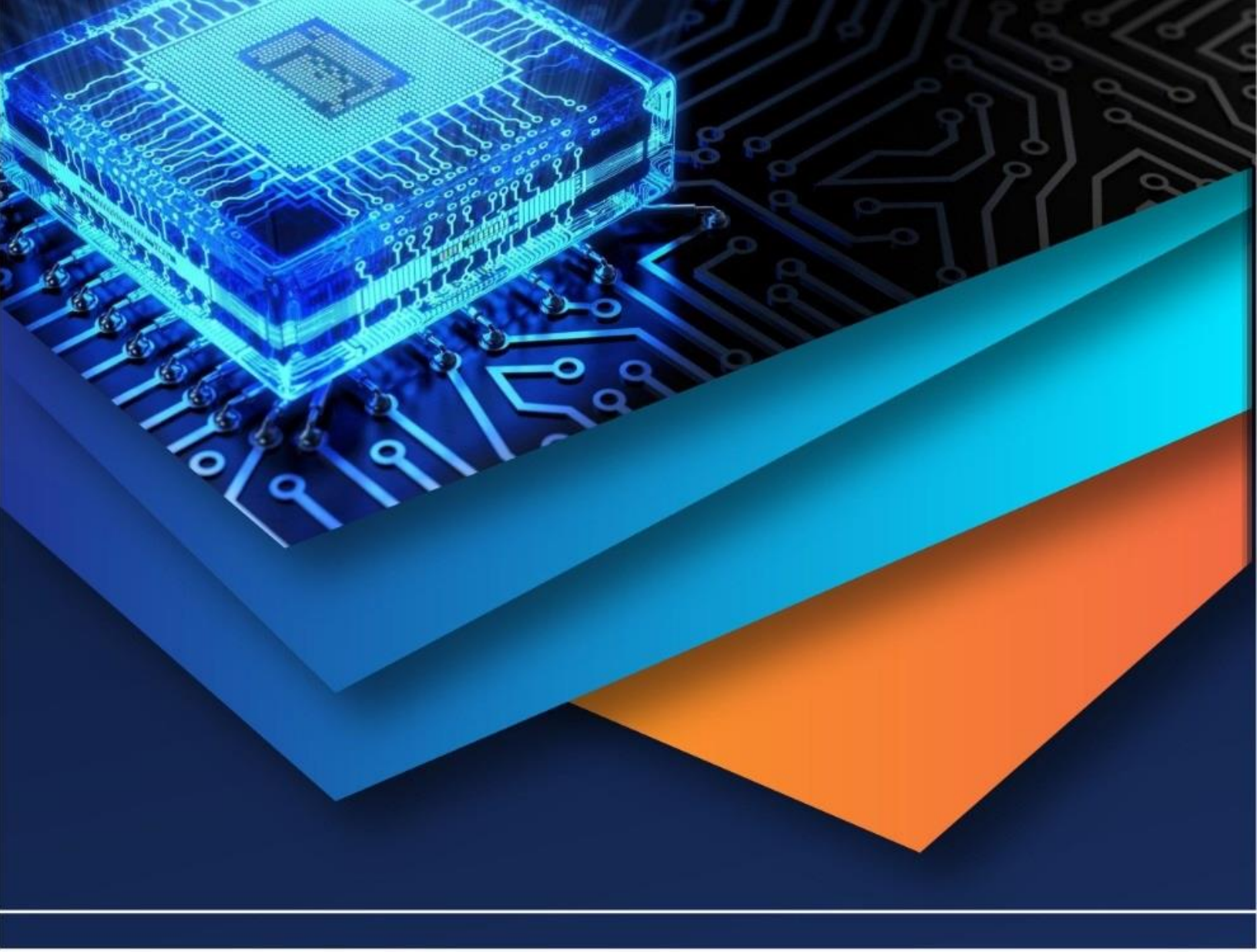
The signature dimensions of DSA are too smaller than the RSA. So the DSA scheme always produces slightly less network overhead than RSA does. It is good to see that the Routing Overhead differences between RSA and DSA schemes vary with different numbers of attacking nodes [15]. Assume that this is due to the effect, that more attacking nodes require more ack packets, thus increasing the ratio of digital signature in the entire network overhead. In this view, we find DSA as a wiser digital signature technique in MANETs [1].The logic is that data communications in MANETs consume more battery. Although the DSA technique needs more calculation to verify than RSA, considering the trade off between battery power and performance, DSA is still preferable.

V. CONCLUSIONS

Here, we represent a relative study of secure system for detecting attacker nodes and attacks. As the properties of MANETs reside, prevention techniques alone are not sufficient to control the whole network distribution. In this scenario detection should be concentrated as another part before an intruder can damage the entire network architecture. We study about secure detection technique named EAACK protocol uniquely crafted for MANETs and in future it is required compare against other popular mechanisms. Security is major part in MANETS; hybrid cryptography architecture will tackle the issue in an efficient manner. This way we can better preserve battery and memory space of mobile nodes.

REFERENCES

[1] EAACK – A Secure Intrusion Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and Tarek R. Sheltami, Member, IEEE
[2] Investigating Intrusion and Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes Marjan Kuchaki Rafsan,Ali Movaghar and Faroukh Koroupi,World Academic of Science Engineering and Technology 44 2008
[3] D. Johnson and D. Maltz, “Dynamic Source Routing in ad hoc wireless networks,” in Mobile computing. Norwell, MA: Kluwer, 1996,ch. 5, pp. 153–181.
[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proc. 6th Annu. Int.Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.
[5] “A study of different types of attacks on multicast in mobile ad hoc networks” Hoang Lan Nguyen, Uyen Trang Nguyen, Elsevier AdHoc Networks(2008) 32-46.
[6] D. Johnson and D. Maltz, “Dynamic Source Routing in ad hoc wireless networks,” in Mobile computing. Norwell, MA: Kluwer, 1996,ch. 5, pp. 153–181.
[7] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, “Video transmission enhancement in presence of misbehaving nodes In MANETs,” Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.
[8] K. Stanoevska-Slabeva and M. Heitmann, “Impact of mobile ad-hoc networks on the mobile value system,” in Proc. 2nd Conf. m-Bus., Vienna, Austria, Jun. 2010
[9] A. Tabesh and L. G. Frechette, “A low-power stand- alone adaptive circuit for harvesting energy from a piezoelectric micro power generator,” IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.
[10]“Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol”Ahmed M. Abdulla, Imane A. Saroitb, Amira Kotbb, Ali H. Afsaric a* 2010 Published by Elsevier Ltd.
[11] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, “Security in mobile ad hoc networks:Challenges and solutions” (2004). IEEE Wireless Communications. 11 (1), pp. 38-47.
[12] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehaviour in MANETs,” IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.
[13] “ Security Issues in Mobile Adhoc Networks-A Survey” Wenjia Li and Anupam Joshi University of Maryland, Baltimore Country.
[14] M. Zapata and N. Asokan, “Securing ad hoc routing protocols,” in Proc.ACM Workshop Wireless Secur., 2002, pp. 1–10.
[15] R. Akbani, T. Korkmaz, and G. V. S. Raju, “Mobile Ad hoc Network Security,” in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY