iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 5 **Issue:** I **Month of publication:** January 2017

**DOI:**

www.ijraset.com

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

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

# A Black hole Detection Algorithm in MANETS Using MAC Scheme

Manju Taya[1], Pankaj Gupta[2]
[1]Research Scholar, [2]Assistant Professor
Department Computer Sc Glaxy Institute of Technology and Management Kurukshetra University Kurukshetra

***Abstract:*** ***Unattended installation of sensor nodes in the environment causes many security threats in the Ad-hoc networks. The security of the DSR and AODV protocol is threaded bydifferent types of attacks. Mobile Adhoc Networks (MANETs) are dynamic in nature. Any nodes can join and leave the network at any time. Hence any type of intruders can attack the communication at any time, especially the routing mechanism between the nodes. In this study, we study and enhance the security of MANET by encrypting the data using RSA before transmission and performing the key exchange among nodes by Diffie Hellman key exchange algorithm. The proposed work involves these algorithms and improves the security and possibility of attacks on network as any intruder doesn't have these mechanisms when present in mobile Adhoc network. In our research AODV routing protocol is used to detect which node sends the reply after getting the request packet. This work will lead to minimum delay of packets in simulation results. The results confirm that the introduction concepts adds minimal overhead in time but enhances the security manifolds.With the help of RSA, a scheme is proposed which performs encryption and decryption. The key idea in the algorithm is that the source node calculates KEYfor encryption in RREP and then it matches the calculated KEY with KEY of the node which generates RREQ.***

***Index Terms—BlackHole, Manet, MAC, RREQ, RREP, AODV.***

## I. INTRODUCTION

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, PDAs and handheld digital devices, has impelled a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society[4]. Mobile ad hoc network got outstanding success as well as tremendous attention due to its self-maintenance and self-configuration properties or behaviour. At early stage most people focused on its friendly and cooperative environment and due to this way many different problems came into being; security is one of the primary concerns in order to provide secure communication between different nodes in a mobile ad hoc network environment.

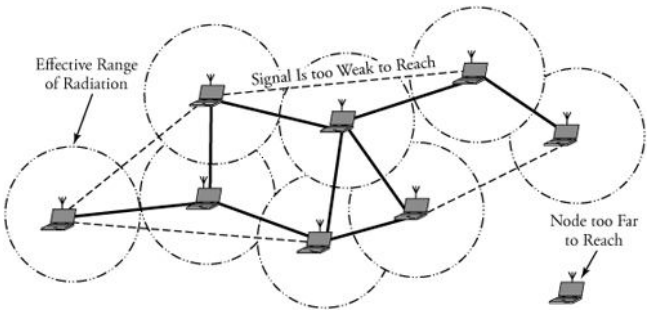



Fig. 1: MANET Architecture

### *A. Interception Attacks on Manets*

Attackers might launch the interception attacks to get an unauthorized access to the routing messages that are not intentionally sent to them. This kind of attack jeopardizes the integrity of the packets because such packets might be modified before being forwarded to the next hop [35].

Wormhole attacks: In the wormhole attacks, a compromised node in the ad hoc networks colludes with external attacker to create a shortcut in the networks. By creating this shortcut, they could trick the source node to win in the route discovery process and later launch the interception attacks. Packets from these two colluding attackers are usually transmitted using wired connection to create

the fastest route from source to the destination node. In addition, if the wormhole nodes consistently maintain the bogus routes, they could permanently deny other routes from being established. As a result, the intermediate nodes reside along that denied routes are unable to participate in the network operations.

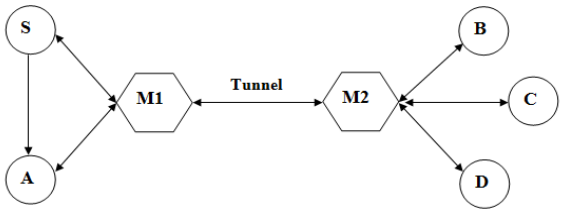



Figure 2: An example of wormhole attack

Here, $M_1$ and $M_2$ are two malicious nodes which link through a private connection. Every packet that $M_1$ receives from the network is forwarded through "wormhole" to node $M_2$,and vice versa. This attack disrupts routing protocols by short circuiting the normal flow of routing packets. Such a type of attack is difficult to detect in a network, and may severely damages the communication among the nodes. Such an attack can be prevented by using packet leashes, which authenticate the timing information in the packets to detect faked packets in the network.

*B. Black Hole Attacks*

In this attack, malicious nodes trick all their neighboring nodes to attract all the routing packets to them. As in the wormhole attacks, malicious nodes could launch the black hole attacks by advertising themselves to the neighboring nodes as having the most optimal route to the requested destinations. However, unlike in the wormhole attacks where multiple attackers colluded to attack one neighboring node, in the black hole attacks, only one attacker is involved and it threatens all its neighboring nodes.

*C. Routing packet analysis attacks*

Since no disruptive action occurs, routing packet analysis could be classified as one of the passive attacks against the ad hoc networks. One way to launch this attack is by exploiting the promiscuous mode employed in the ad hoc network. In a promiscuous mode, if node A is the neighbor of both nodes B and C at a particular time, node A can always hear the transmissions between node B and node C. By exploiting this nature, node A is able to analyze the overheard packets transmitted between node B and node C. Besides, malicious nodes could also launch this attack by exploiting the nature in a multi hop routing. In multi hop routing, packets need to be forwarded through several intermediate nodes before reaching the actual destination. Malicious nodes might exploit this opportunity by locating themselves in any location along the route to participate in the message forwarding process and later launch the routing packet analysis attacks.

## II. RELATED RESEARCH

Juan-Carlos Ruiz*et. al.* [35] described that Ad hoc networks exploit the processing storage and wireless communication capabilities of mobile devices to create spontaneous and low-cost self-configuring networks. A first step towards that ambitious goal was to study how central elements of ad hoc networks their routing protocols behave in absence but also in presence of malicious faults or attacks. Black holes were simple but effective denial of service attacks in today's ad hoc networks. This paper described how to inject such attacks in ad hoc networks relying on proactive routing protocols.

Mohammad Al-Shurman*et. al.* [34] provided a solution for single black hole node detection. In the proposed method each intermediate node to send backs the next hop information when it sends back an RREP message. When the source node receives the reply message it does not send the data packets right away but extracts the next hop information from the reply packet and then sends a further request to the next hop to verify that it has a route to the intermediate node who sends back the Further reply FRP message and that it has a route to the destination node. Limitation of this proposal was that it would not be able to identify that NHN works cooperatively with IN and sends back false FRP. DjamelDjenouri*et. al.* [30] suggested a non-cooperative game framework for the defense of nodes in WSN. In this framework three different schemes have been applied to finding the most vulnerable node in WSN and protected it. The first scheme an attack defense problem was approached as two players non zero non-cooperative game between the attacker and the sensor network. The second scheme used the Markov Decision Process (MDP) to find the most vulnerable sensor node whereas the third scheme applied node's traffic as an intuitive metric to use it as an indicator for protected the node. The authors claimed that the evaluation of their schemes reveals its effectiveness of successful defence against attacks.

This study required an experimental investigation to prove the concepts of the three used schemes. Another limitation of this work was that the strategy on when the MDP should be applied and when the theoretic game framework should be used to gain high success detection was not determined.

D. Ben Khedher*et. al* [27] suggested that node failures and message losses were frequent in MANETs. This paper proposed a novel overlay-based architecture for MANET applications to ensure that if a node failed all the other nodes would be notified. Nodes form a self-organizing overlay network that was overlaid on the physical network. In an overlay network a set of nodes called detectors periodically sense each other's heartbeat messages. Every detector also sensed the heartbeat messages of a set of nodes. If a detector did not heard from a node after a timeout possibly due to node failure or message loss it identifies the failure of the node according to a set of failure detection rules and then reports the failure to all the other nodes. A simulation was done to demonstrate scalability and to compute the number of non-failed nodes declared as failed. Finally the author described a use case for recovery in a conferencing situation in MANETs. K. Sivakumar and Dr. G. Selvaraj(2013)analyzed the security problems in MANET and present a few promising research directions. On the prevention side, various key and trust management schemes have been developed to prevent external attacks from outsiders, and various secure MANET routing protocols have been proposed to prevent internal attacks originated from within the MANET system. On the intrusion detection side, a new intrusion detection framework has been studied especially for MANET. Both prevention and detection methods will work together to address the security concerns in MANET.

## III. PROBLEM DEFINED

In the different researches discussed above, the authors used various routing algorithms for smooth exchange of information between mobile nodes. Generally we imply security on all the nodes of the network. But this causes wastage of time and cost. Static security architectures cannot cope with rapidly changing security environment, including: physical parameters, threats, network dynamics, and mission goals.

To find out the shortest path and then imply the security in multicast routing in order to save time.

To hide the source or the destination of a packet, or simply the amount of traffic between a given pair of nodes.

To encrypt data so that attackers cannot destroy the data.

Following are a few objectives of proposed system:

To compute single-source shortest paths in the network for different destination nodes.

To provide security between the two nodes which are communicating instead of whole network thereby increasing the performance.

To provide security between nodes for Key Exchange.

To apply encryption and decryption by using cryptographic scheme such as RSA.

## IV. PROPOSED METHODOLOGY

Here the Flow chart of the proposed work is presented. As we know the flow chart is the graphical representation of the algorithmic

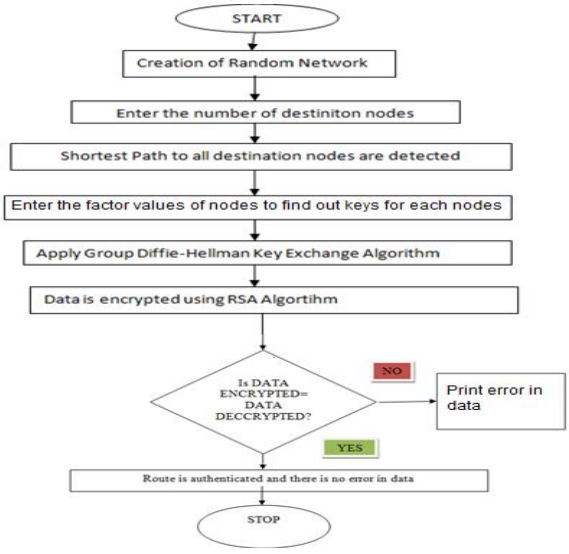



Figure 3: Flowchart of Proposed Work

In this research, Message Authentication Code (MAC) based black hole attack detection and reaction scheme is proposed that can be used to guard against black hole nodes in MANETs. The nodes can try to attack the network by conducting malicious transactions, or spreading viruses and worms, or attacking known vulnerabilities. The proposed scheme tries to predict the future behaviour of a node by observing its past behavior. It is believed that the proposed scheme will have a positive impact in malicious node detection and prevention for wireless mobile ad hoc networks.

## V. IMPLEMENTATION RESULTS

The research methodology generated by the author is programmed using MATLAB R2012 tool. The simulation parameters used to initialize the network are given in table below:

| | |
|---|---|
| Simulation Time | 100 seconds |
| Environment Size | 100 x 100 |
| Packet Size | 512 bytes |
| Traffic type | CBR |
| Packet rate | 4 packets/second |
| Mobility model | Random Waypoint model |
| CBR sources | 10 |
| Maximum Speed | 20 m/s |
| Pause Time | 0, 35, 70, 100 |
| Protocol | DSR |
| Number of nodes | 60 |

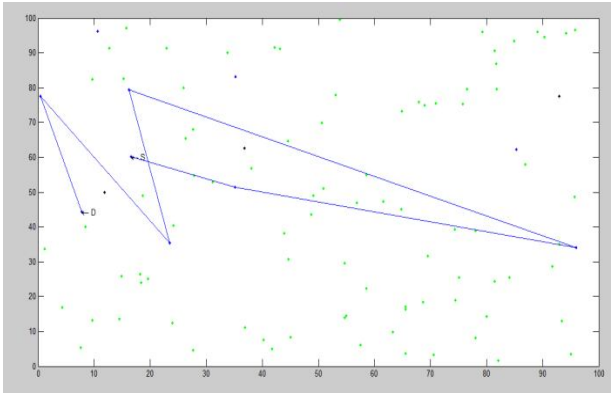


Figure 4: Transfer of Packet from Source to destination

In figure 4 an artificial MANET simulator is created so as to detect the attacks which are performed during the data transmission takes place between the networks. In this simulator random number of nodes is generated at the time of implementation. The green colour dots are nodes in the networks which contain some value of energy such as E0 = 0.005 and the transmitter state energy ETX = 50*0.000000001 and receiver state energy ERX = 50*0.000000001. The transmission process is based on the most preferable

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

available node among the nearest node to the sender node. The data is transmitted with in the network by choosing the available node in the network. Sometimes it may occur the most nearest accurate node is consumed in other process so it is not necessary to choose the specific node rather to shift to some other most preferable node. There is not preferred algorithm to select the node for transmission of data packets. In this system while transmission energy is lost at each step which leads to dead nodes in the network. The energy of each node is reduced with each round during the process of transmission of data packets. The selection process of nodes takes place such as if initially a node is selected from the nearest neighbours of source node and the selected node is busy in transferring data to some other node so randomly some other node is selected from the nearest neighbour of that node. In figure 5 the path presented is created by selecting the required nodes and according to this path data is transferred within the network. As the data is transmitted and the number of rounds increases the energy is reduced and the nodes are dead. At final stage the red coloured cross are dead nodes with zero energy. These nodes could not be further entertained in the network for further transmission process. The black coloured dots depict black hole attack which occurs when a malicious node act as an intermediate node and destroys the data packets. The blue colour dots represents the grayhole attack in which the attacker misleads the network by agreeing to forward the packets in the network. As soon as it receive the packets from the neighbouring node, the attacker drop the packets. The remaining green coloured dots are the left over nodes in the network which are not utilised in the data transmission process.

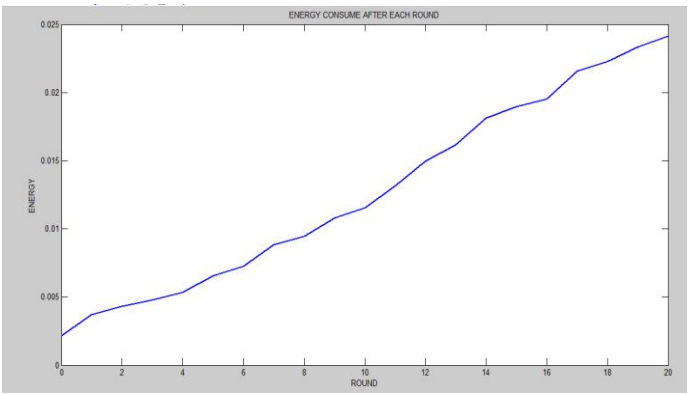



Figure 5: Energy consumption each round

The amount of energy consumed in each round is increased as the system iterates. In figure 3.4 there is a large increment in the amount of energy consumed after each round. The pointer shows a great increment starting from 1st round to 200 rounds. As the energy is lost after each round, it indirectly shows the energy consumption of the system after each round.

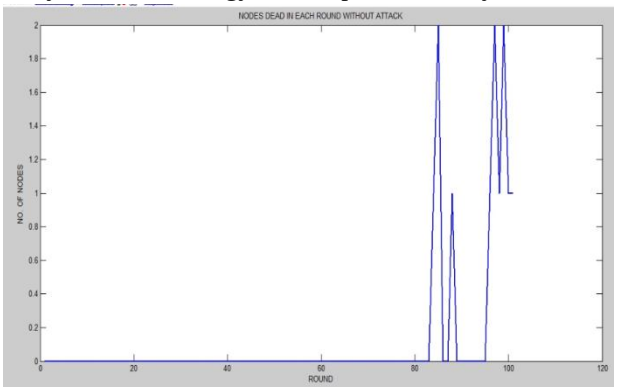



Figure 6 Graph for dead nodes in each round without attack

In figure 6 the graphical analysis of number of dead nodes found in each round without attack is performed in the system is presented here. While iteration takes place before attack is performed in the system, the nodes involved loose there energy with lesser speed and the number of dead nodes are also less in the end of the system in comparison to the system with attack. As the number of rounds increases there is a great increase in the number of dead nodes to be formed. There is a large decrease in the amount of energy of nodes after 80 rounds which leads to the increase in the number of dead nodes of the system.

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

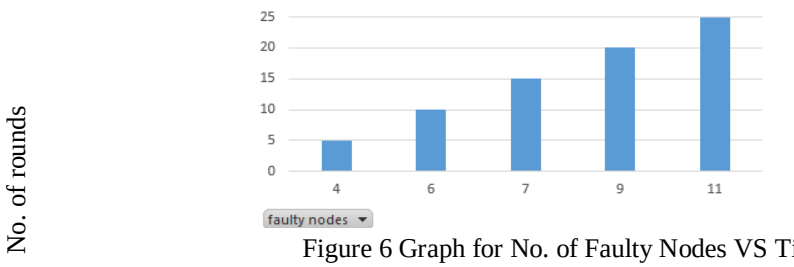


Figure 6 Graph for No. of Faulty Nodes VS Time

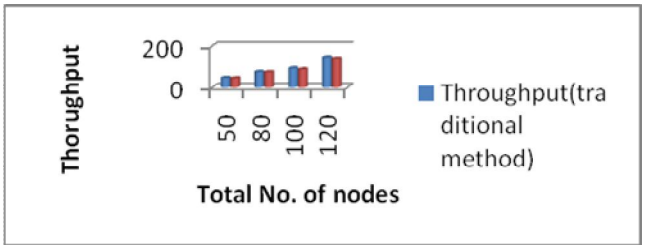


Fig. 7: Throughput by two techniques

## VI. CONCLUSION

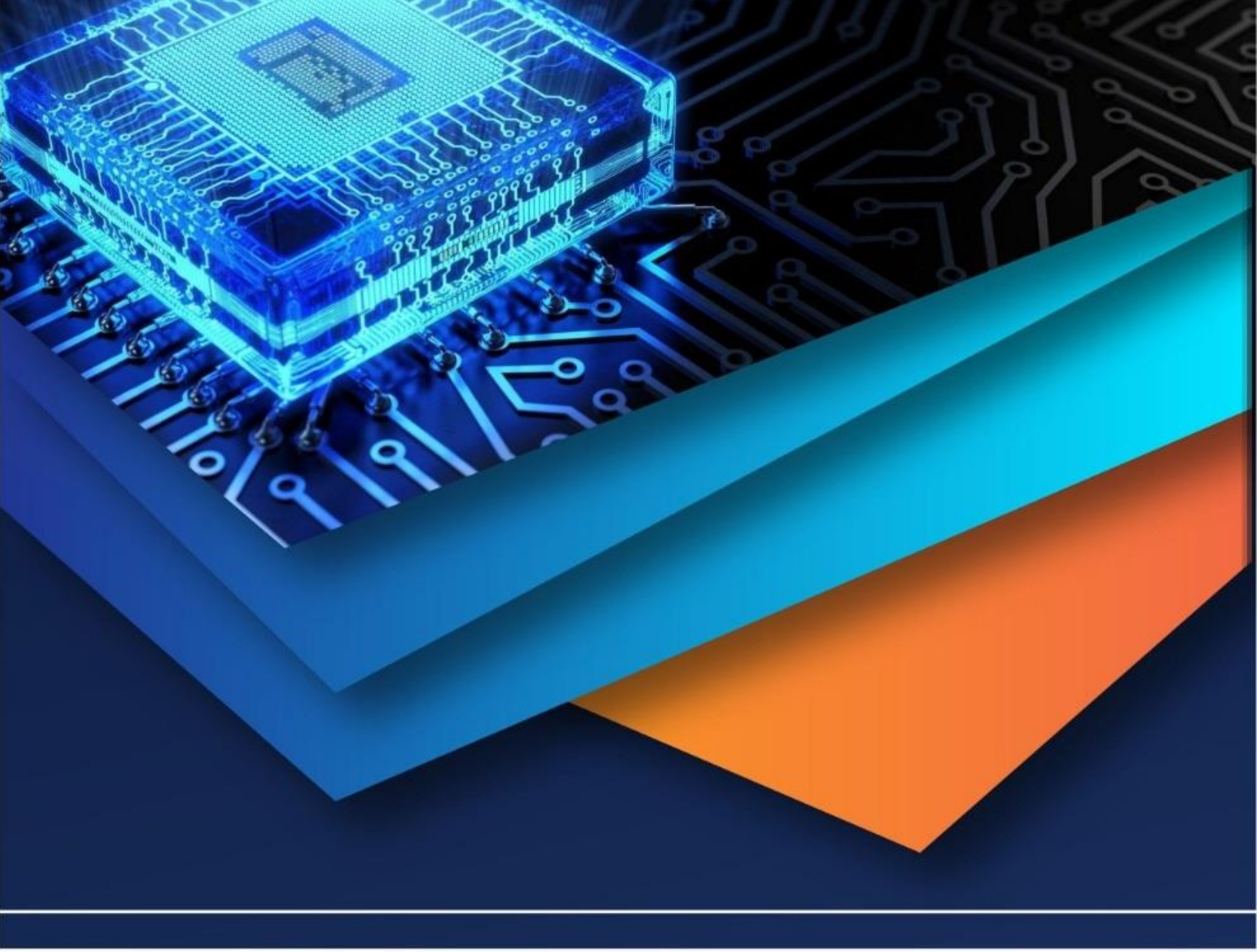
In this research, Message Authentication Code (MAC) based black hole attack detection and reaction scheme is proposed that can be used to guard against black hole nodes in MANETs. The nodes can try to attack the network by conducting malicious transactions, or spreading viruses and worms, or attacking known vulnerabilities. The proposed scheme tries to predict the future behaviour of a node by observing its past behaviour. In this thesis, we have overviewed the challenges and solutions of the security threats in mobile ad hoc networks. As shown in the graphs and the Black Hole attacks are more vulnerable than other attacks because the packet drop ratio is high for Black Hole attacks compared to other attacks. When compared to the amount of energy consumption in the system, it is more in the case of any attack performed in the system rather than without attacked system. Thus from the simulation results one can observe that Black Hole attacks causes more damage to MANET compared to other attacks. With the help of MAC, a scheme is proposed which requires time synchronization. The key idea in the algorithm is that the source node calculates MAC of RREP and then it matches the calculated MAC with MAC of the node which generates RREP

## VII. ACKNOWLEDGMENT

I owe my special thanks to Mr. ABC for all his guidance and support without which this research was not possible. I also thank my parents and the almighty for their blessings. And also special thanks to all my friends for all the moral support.

## REFERENCES

[1] K. Sivakumar And Dr. G. Selvaraj, “Overview Of Various Attacks In Manet And Countermeasures For Attacks”, International Journal Of Computer Science And Management Research, ISSN 2278-733x ,Vol 2 , January 2013.
[2] Gagandeep, Aashima And Pawan Kumar, “ Analysis Of Different Security Attacks In Manets On Protocol Stack A-Review”, IJEAT, ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.
[3] B.Persis Urbana Ivy, PurshotamMandiwa and Mukesh Kumar, “A modified RSA cryptosystem based on ‘n’ prime numbers”, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume1 Issue 2 ,Page No. 63-66, Nov 2012.
[4] Ajit Singh, Tamanna, SahilBatra And PriyankaGoyal , “Mobile Ad Hoc Networks: Challenges, Applications & Their Routing Protocols”, Int. J. Of Recent Trends In Engineering And Technology, Vol. 4, No. 2, Nov 2010.
[5] PriyankaGoyal,VintiParmar,Rahul Rishi, “Manet: Vulnerabilities, Challenges, Attacks, Application”, Ijcem .Vol.11.January2011.
[6] SatyendraNathMandal, Kumarjit Banerjee, BiswajitMaiti and J. Palchaudhury, “Modified Trail division for Implementation of RSA Algorithm with Large Integers”, Int. J. Advanced Networking and Applications Volume: 01, Issue: 04, Pages: 210-216 , 2009.
[7] Shuhui Yang And Jie Wu, “New Technologies Of Multicasting In Manet”, Department Of Computer Science And Engineering, Florida Atlantic University, Boca Raton, Fl 33431,2009.
[8] T. Nirmal Raj, S. Saranya, S. Arul Murugan, G. Bhuvaneswari.” Secured Multi Path Routing With Trust Establishment Using Mobile Ad Hoc Networks”, International Journal Of Scientific & Engineering Research, Volume 3, Issue 1, ISSN 2229-5518, January -2012 .
[9] TanuPreet Singh, Neha And Vikrant Das, “ Multicast Routing Protocols In Manets”, International Journal Of Advanced Research In Computer Science And Software Engineering,ISSN: 2277 128x,Volume 2, Issue 1, January 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY