iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5330

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Implementation: Detection of Blackhole Mechanism on MANET

Mr. Vishwajith M V[1], Pratik Sanjel[2], Pranish Pokharel[3], Kshetiz Pokhrel[4]
[1]*Assistant professor Information Science & Engineering Department, NHCE, Bangalore, India*
[2, 3, 4] *Student, BE, Information Science & Engineering Department, NHCE, Bangalore, India*[2]

Abstract: A mobile ad hoc network (MANET) is a collection of autonomous nodes that communicate with each other by forming a multi-hop radio network and maintaining connections in a decentralized manner. Protecting the network layer of a MANET from malicious attacks is an important and challenging security issue, since most of the routing protocols for MANETs are vulnerable to various types of attacks. Ad hoc on-demand distance vector routing (AODV) is a very popular routing algorithm. However, it is vulnerable to the well-known black hole attack, where a malicious node falsely advertises good paths to a destination node during the route discovery process but drops all packets in the data forwarding phase. This attack becomes more severe when a group of malicious nodes cooperate each other.The proposed mechanism does not apply any cryptographic primitives on the routing messages. Instead, it protects the network by detecting and reacting to malicious activities of the nodes. Simulation results show that the scheme has a significantly high detection rate with moderate network traffic overhead and computation overhead in the nodes. Keywords: Mobile ad hoc network (MANET), blackhole, packet dropping attack, malicious node, routing misbehavior,

I. INTRODUCTION

Wireless network is the network of mobile computer nodes or stations that are not physically wired. The main advantage of this is communicating is keep in contact with rest of the world while being mobile.

The disadvantages are their limited bandwidth, memory, processing capabilities and open medium. Two basic system models are fixed backbone wireless system and Wireless Mobile Ad hoc Network (MANET).

An intermediate node is used to carry out data from sender to destination. Each node is a router and a host in MANET. Despite the major issues in the node mobiity and bandwidth constraints and error prone wireless channel, resource constrained nodes, and dynamic changing of the network topology various routing protocols have been designed to enhance the network performance i.e Proactive(table driven) and reactive(on demand) routing protocols.

In this paper we mainly focus AODV protocol. Cryptographic technique can be used to detect the malicious node but it is expensive as well as also the integrity and the authenticity cannot guarantee on finding the malicious node

A. AODV as Routing Protocol

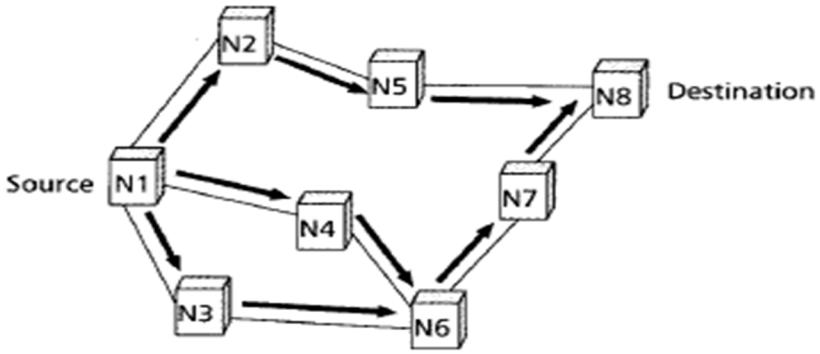
AODV (Ad hoc On-Demand Distance Vector) is a reactive routing protocol To send data to a given destination , the source node trace the node ids and the position of the node from the routing table.

If it finds a route towards this destination ,it uses it immediately, else it launches a route search route , which consists in broadcasting, by the source node , a route request (RREQ) message towards neighbors. When RREQ is received by an intermediate node, this last consults it routing table to find a fresh route (the route is fresh If the sequence number of this route is larger than that of RREQ) towards the requested destination in RREQ.

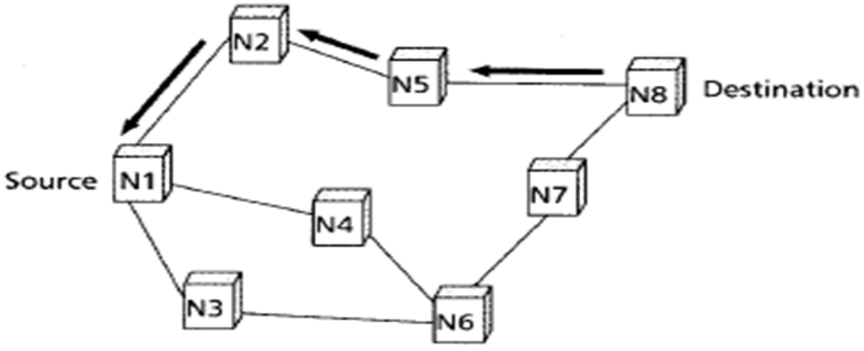
If such a route is found, a route reply (RREP) message is sent through the preestablished reverse route (established when RREQ pass through intermediate nodes) towards the source S . If the intermediate node does not find a fresh route, it updated its routing table and sends RREQ to these neighbors. This process is reiterated until RREQ reaches the destination node D.

The destination node sends RREP to S by using the pre-established reverse route. If the source finds out the malicious node than it choose the alternative path for sending the packets.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com



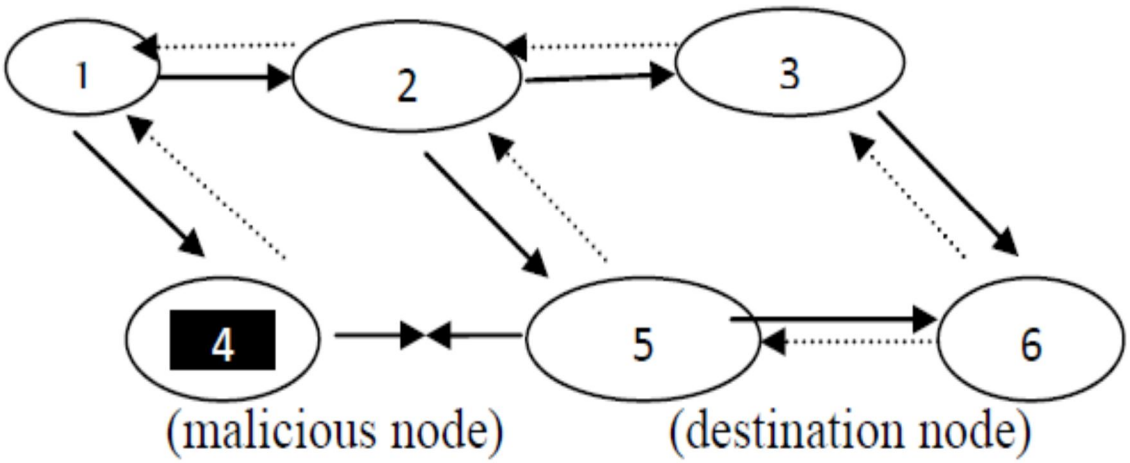
(a) Propagation of the RREQ



(b) Path of the RREP to the source

B. Black Hole Attack

In this attack, the malicious node advertise itself to have the shortest route for the communication and transferring of packets, and thus drops the packets without forwarding them to the neighbouring nodes. Black hole attack is one of the possible attack and most common attack in MANET. It can be said as the Denial of Service. In this attack, a node generates a RREQ message and passes it to its neighbours; a malicious node advertises that it has the best path to the destination node during the process of route discovery. As soon as it receives the RREQ message from the source node, it immediately sends back a fake RREP message to it. The source node receives the RREP message and starts sending the packet to it. When source node starts sending packets to the destination by using this route, the malicious node drops all packets instead of forwarding it. In other words it can be said that it "swallows" the data packet.



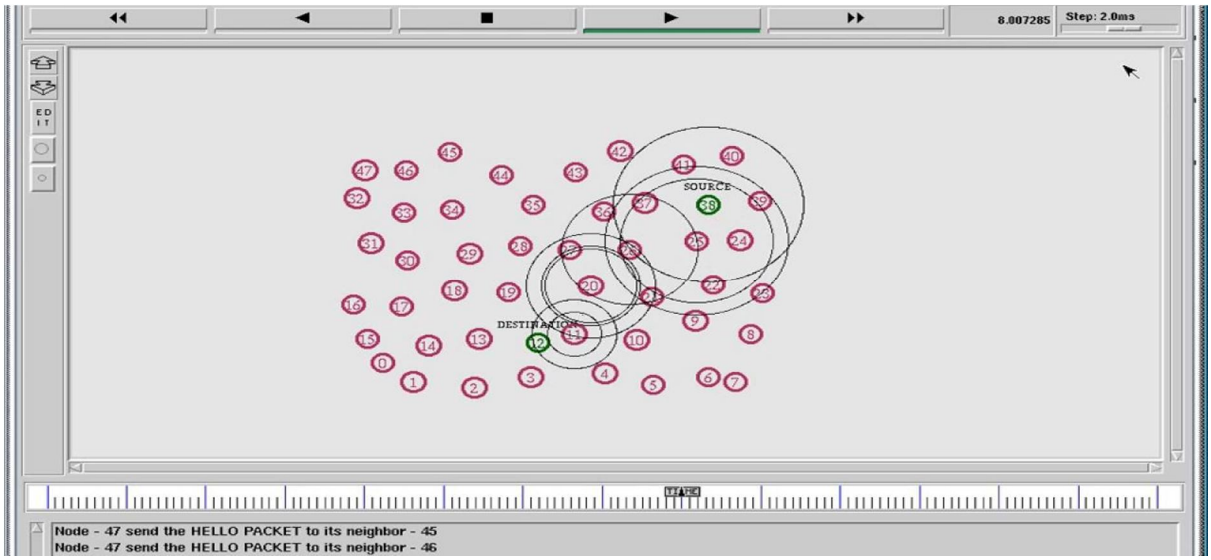
In the above figure, there are 6 nodes out of which node 1 is the source node which generates the RREQ message in order to find the fresh route to send a packet to the destination node i.e. node 6. The intermediate nodes of node 1 are node 2 and node 4. Both the nodes get the RREQ message generated by the node 1. Node 4, being the malicious node, sends the RREP message back to the node 1 advertising that it has the best path to the destination node, node 6. After receiving the RREP message from node 4, node 1 started sending the packet to the node 4. But node 4 will not forward it; it discards all the messages just making it the denial of service.

C. Implementation

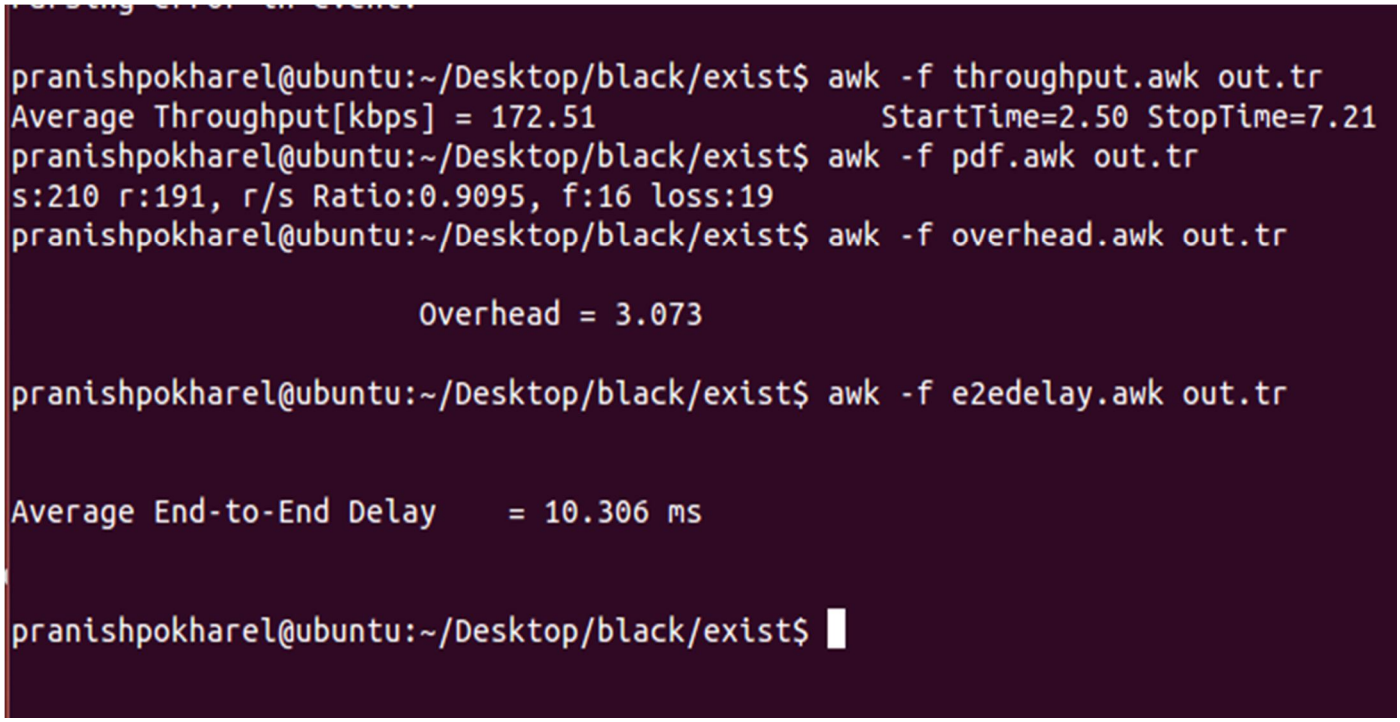
NS Network Simulator, It is an event driven network simulator program,which includes many network objects such as protocols applications and traffic source behar. Implementing new protocol In Implementation of a New Manet Unicast Routing Protocol in NS-2 is described. To implement our contribution we have used the details explained in this paper. In our work, we have used the nodes that exhibit black hole behavior in wireless ad-hoc network that use AODV protocol. Since the nodes behave as a Black Hole, they have to use a new routing protocol that can participate in the AODV messaging. All routing protocols in NS are installed in the directory of "ns-2.34".We start with duplicating aodv folder in the folder ns-allinone-2.34/ns-2.34. Then we rename all the files in the folder as blackdv instead of aodv eg aodv.cc as baodv.cc., aodv.h as baodv.h and so on. Then we change all classes, functions, exists, variables and constants from aodv to black names in all the files in the directory. NS2 network simulation for the black hole ,TCl(Tool command language) language is used. Tcl is a high-level, general-purpose, interpreted, dynamic programming language. It was designed with the goal of being very simple but powerful. Changes need to be done in ns2 ,We made changes at 3 places

class AODV

```
#define MY_ROUTE_TIMEOUT       10                    // 100 seconds
#define ACTIVE_ROUTE_TIMEOUT   10                          // 50 seconds
#define REV_ROUTE_LIFE         6                           // 5  seconds
#define BCAST_ID_SAVE          6                     // 3 seconds
// No. of time to do network-wide search before timing out for
// MAX_RREQ_TIMEOUT sec.
#define RREQ_RETRIES           3
// timeout after doing network-wide search RREQ_RETRIES times
#define MAX_RREQ_TIMEOUT   10.0 //sec
Various constants used for the expanding ring search */
#define TTL_START     5
#define TTL_THRESHOLD 7
#define TTL_INCREMENT 2
// This should be somewhat related to arp timeout
#define NODE_TRAVERSAL_TIME     0.03          // 30 ms
#define LOCAL_REPAIR_WAIT_TIME  0.15 //sec
```



In this black hole attack we have compare 4 parameter and how they are different before and now.
Such as the throughput, overhead, pdf (packet delivery ratio), energy.
-Packet Delivery Ratio (PDR): It defines Ratio Between number of packet sent from source to destination and number of packet actually received at destination.
-PDR = (Total number of packet sent by source / number of packet received by destination)
-End to End Delay (E2E Delay): It is the time slice between sending time at source and receiving time at destination. It includes transmission delay, process queue delay and propagation delay.
Throughput: Throughput defines the rate of successful packet delivery over a communication channel. Energy.energy defines as how much the energy are consumed while delivering the data from source to destination. In this implementation we have done both the existing and as well as proposed system and we compared all the four parameter in both the existing as well as proposed system in this existing system. Existing system based on sensing the wireless channel. As well as this approach assigns a max trust value to all its neighboring nodes. A node will not do any further communication with those neighbor having trust value is less than min trust value. First of all we start with the node deployment ,then after some time the node start mobility and starts move there are total 32 node out of them there are 2 source node, as well as 2 of them are destination node also there is malicious node but here we have assign the node number 13 as the malicous node and node 5,6 as source and 18 and 20 as destination. After the mobility of the node the source starts for the route search and send the rep request for all the node for the shortest path to send the packet to the destination. after some time the malicous node also send the rep to the source then the source start to send the packet to the destination from the path of the malicious node, when the malicious node gets the packet if will not forward the data and keeps the data with itself then, after sometime the source knew that the data has been consumed by the malicious then it search for the alternative path and send the packet to the destination. After the compeltation of the packet from source to the destination then we start to calculate the parameter.
For, throught put the command :=awk –f throughput.awk out.tr
Overhead-= awk –f overhead.awk out.tr
Pdf-= awk –f pdf.awk out.tr
(the out,tr is the trace file where all the node are trace.)



And for the energy we have calculate for all the node. so its has been done at the last but for other parameter it can calculate for one node also.
Energy-+awk –f a.awk out.tr

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

```
pranishpokharel@ubuntu:~/Desktop/black/exist$ awk -f a.awk out.tr
node 0 1.67463
node 1 2.32433
node 2 0.911514
node 3 2.17704
node 4 0.85904
node 5 3.37409
node 6 0.945507
node 7 0.955496
node 8 0.995581
node 9 3.1551
node 10 1.74475
node 11 2.23604
node 12 1.47237
node 13 1.26982
node 14 1.55204
node 15 1.04591
node 16 2.37317
node 17 0.853865
node 18 2.5505
node 19 0.832884
node 20 0.851444
node 21 0.772087
node 22 0.637596
node 23 1.10058
node 24 0.857001
node 25 0.946279
node 26 0.923937
node 27 0.634349
node 28 0.659475
node 29 0.59983
node 30 0.407237
node 31 0.575959
node 32 0.449327
node 33 0.183255
node 34 0.211084
node 35 0.408354
+===========+
average energy 3.98671
pranishpokharel@ubuntu:~/Desktop/black/exist$
```

In the propsed system we have add the command on the mac layer such as for the antenna we have increased its capacity .but the process are the same and we agan=in start the calculating the data of the parameter.

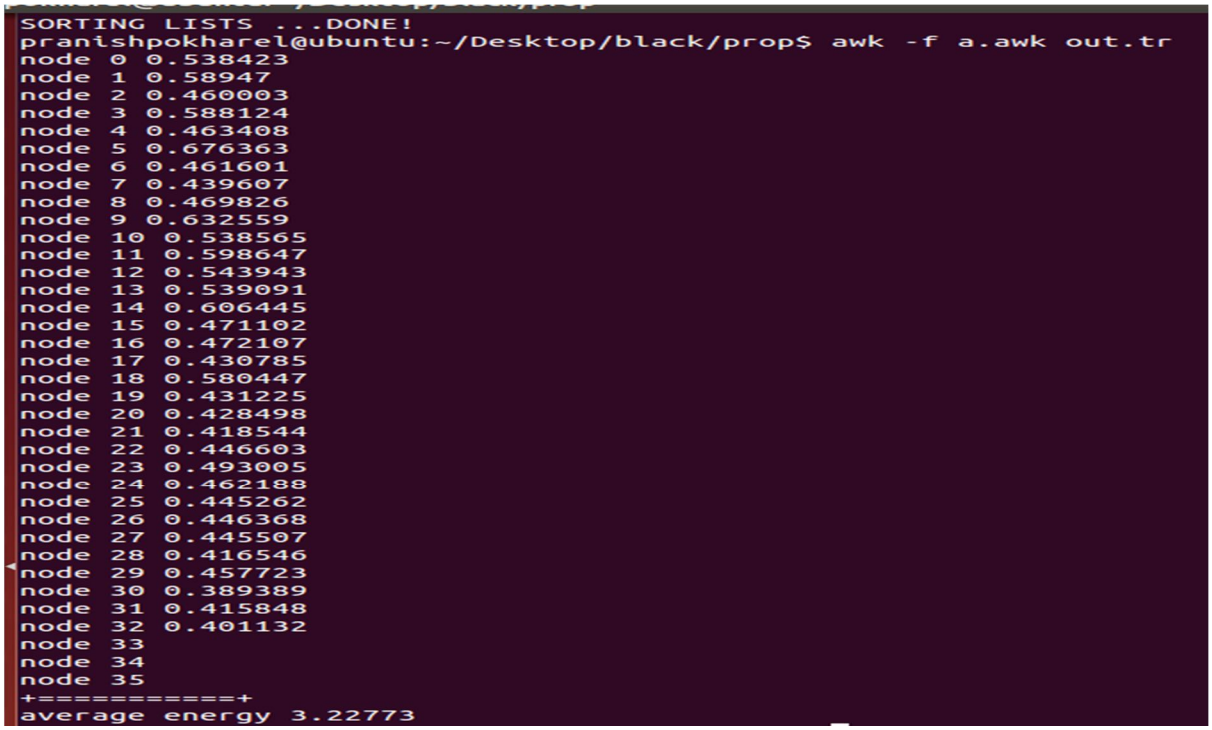
```
pranishpokharel@ubuntu:~/Desktop/black/prop$ ns main.tcl
num_nodes is set 36
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
Loading connection pattern...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 897.9
SORTING LISTS ...DONE!
pranishpokharel@ubuntu:~/Desktop/black/prop$ awk -f throughput.awk out.tr
Average Throughput[kbps] = 184.68                StartTime=2.50 StopTime=7.20
pranishpokharel@ubuntu:~/Desktop/black/prop$ awk -f pdf.awk out.tr
s:228 r:204, r/s Ratio:0.8947, f:17 loss:24
pranishpokharel@ubuntu:~/Desktop/black/prop$ awk -f overhead.awk out.tr

                      Overhead = 2.946

pranishpokharel@ubuntu:~/Desktop/black/prop$ awk -f e2edelay.awk out.tr


Average End-to-End Delay    = 1.14808 ms
```

We can see that the throughout has been increased,the overhead has been decresed and the packet deliver ratio has been increased .



Aslo the engery consumed has been decreased.

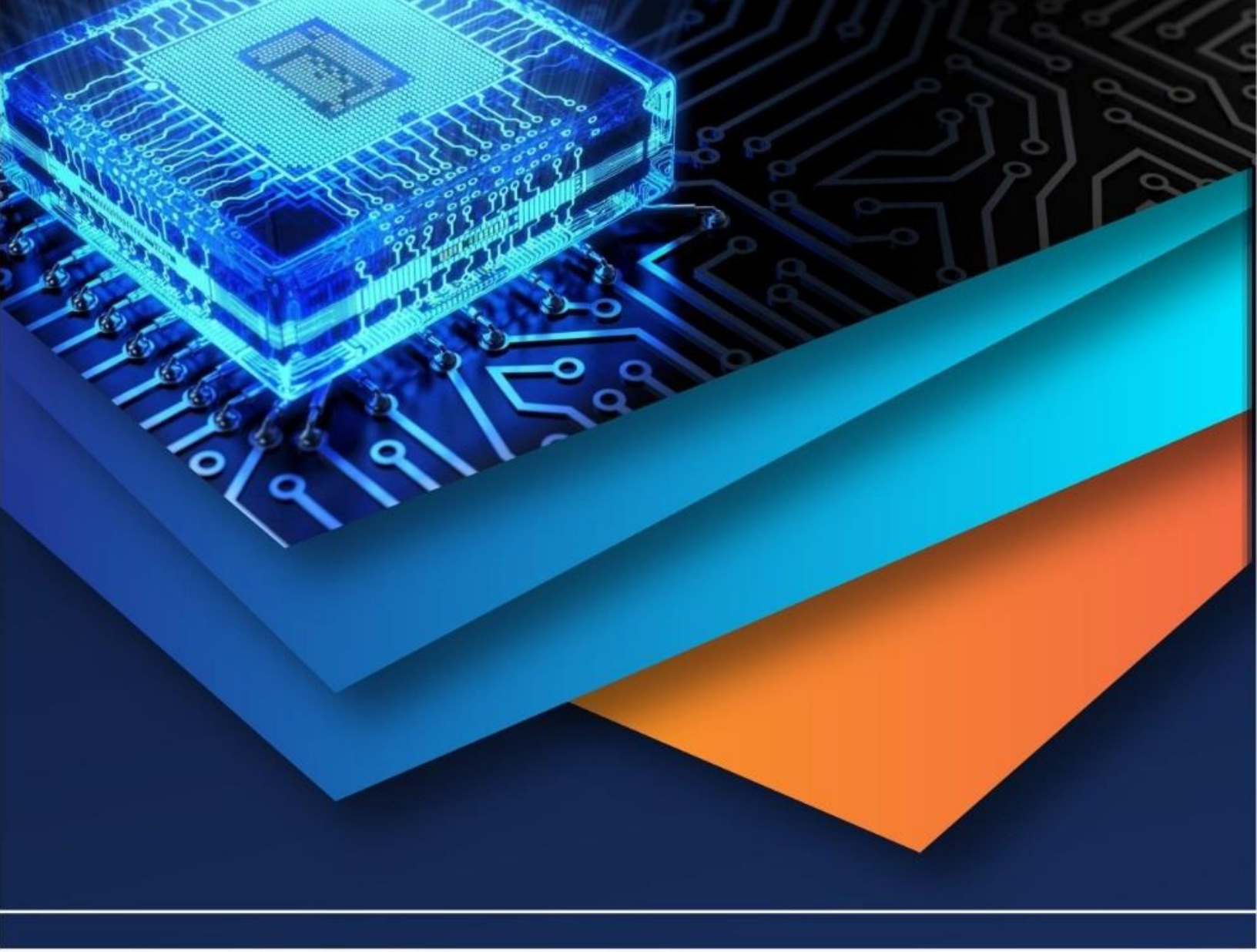
Parameter	Existing	Proposed
Througtput	172.51	184.68
Overhead	3.073	2.96
Packet deliver ratio(pdr)	.09095	.8085
End to end delay	10.360ms	1.1406ms
Energy	3.98	3.20

II. CONCLUSION

In this survey paper, the reactive detection method eliminates the routing overhead problem from the event-driven way is founded, as well as it suffered from some packet loss in the beginning of routing procedure. Therefore, hybrid detection method is recommended which combined the advantages of proactive routing with reactive routing is the tendency to future research direction. However, we also discover that the attacker's misbehavior action as the key factor. The attackers are able to avoid the detection mechanism, no matter what kinds of routing detection used. Accordingly, some key encryption methods or hash-based methods are exploited to solve this problem. The black hole problem is still an active research area. This paper will benefit more researchers to realize the current status rapidly.

REFERENCES

[1] M. A. Abdelshafy and P. J. King. Analysis of security attacks on AODV routing. In 8th International Conference for Internet Technology and Secured Transactions (ICITST), pages 290–295, London, UK, Dec 2013.
[2] M. A. Abdelshafy and P. J. King. AODV & SAODV under attack:performance comparison. In ADHOC-NOW 2014, LNCS 8487, pages 318–331, Benidorm, Spain, Jun 2014.
[3] N. Choudhary and L. Tharani. Preventing black hole attack in AODV using timer-based detection mechanism. In International Conference on Signal Processing And Communication Engineering Systems (SPACES), pages 1–4, Jan 2015
[4] P. Joshi. Security issues in routing protocols in MANETs at network layer. Procedia Computer Science, 3:954–960, 2011.
[5] S. Lee, B. Han, and M. Shin. Robust routing in wireless ad hoc networks. In International Conference on Parallel Processing Workshops, pages 73–78, 2002.
[6] P. Papadimitratos and Z. J. Haas. Secure link state routing for mobile ad hoc networks. In Symposium on Applications and the Internet Workshops, pages 379–383. IEEE Computer Society, 2003.
[7] M. Patel and S. Sharma. Detection of malicious attack in MANET a behavioral approach. In IEEE 3rd International on Advance Computing Conference (IACC), pages 388–393, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY