www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 2 February , 2014 Page No. 3884-3890

Detection and Prevention of Black Hole Attack To Improve Network Performance By Using Fidelity and ECARP Algorithms

Pankaj Solanki, Deepak Shuhkla
IES, IPSA, Indore,
RGPV Bhopal, Bhopal
Pankaj.s1027@gmail.com
Deepakactive@gmail.com

Abstract—**MANET is a next generation communication network and can be defined by self.Due to its characteristics that is keptattracting for academic research and development.Due their ad hoc nature and dynamic topology, performance and security is a key problem in MANET. In search of secure, efficient and effective algorithm, a simulation is prepared in this paper. This paper describes the detailed analysis and implementation of the proposed work. After implementation, the performance of the designed system is evaluated. according to given results system isadoptable at the performance as well as security point of view.**

***Keywords**—MANET, security, performance, improvement, simulation.*

I. Introduction

MANET is a new generation communication network, which is much promising due to their characteristics. These characteristics are also providing a definition of the MANET. MANET is defined using independent mobility, infrastructure less network topology which is self-configuring. But due to their ad hoc nature of network infrastructure and topology that is a point of attraction for academic research as well as communication engineers. Due to their dynamic topology nodes are independently moving in any direction and able to communicate with any node in the network, but sometimes it is quite complicated for security and performance issues.

The proposed work investigates about blackhole attacks over MANET. The black hole attack is one of the most frequent attacks which are deployed in MANET. There are various techniques and methods are available to detect and prevent a black hole attack, but most of them are not much efficient during performance measurements.Thus a hybrid approach is required to develop to detect and prevent with efficient and reliable communication. The proposed networking system is simulated using NS3 network simulator. After implementation of the proposed technique, network is successfully able to detect and prevent black hole attack.

There are two major issues in MANET performance and security. So required to design a new communication system where security and performance are both available. The MANET suffers from many security issue because of limited hardware resources like limited battery power, comparatively less processing speed, transmission is received by every device nearby weather it is part of network or not and many more, because of this deficiencies the wireless devices are highly venerable toward Blackhole attack.many solutions are proposed to avoid the attack, majority of the solutions degrade performance in terms of delay and throughput so to provide an approach which take care of both security and performance, Which includes the following objectives to be achieved after completion of the study.

1. The main objective of this work is to avoid black hole efficiently.
2. Implements black hole with AODV in a scenario.
3. Upgrade AODV with security algorithm to detect and avoid attackers.
4. Upgrade AODV with proposed enhancement to improve performance.
5. Compare the results of existing routing protocol and enhanced routing protocol to verify that, proposed approach is efficient and secure.

The given section provides an overview of the proposed study and in next section describes the background work and their descriptive study.

II Background

In search of efficient and secure method for detection and prevention of the black hole attack some previously designed and technique are studied, some of them are provided in this section.

MANET is an autonomous collection of mobile nodes forming a dynamic network and communicating over wireless links. As MANETs are gaining popularity, their need to support real time and multimedia applications is rising as well. Therefore a QoS estimation work is organized by ***[Mandeep 2013]*** according to author such applications have Quality of Service (QoS) requirements like bandwidth, end-to-end delay, jitter and energy. Consequently, it becomes very necessary for MANETs to have an efficient routing and QoS mechanism to support these applications. This paper [1] presentsan overview of the QoS routing protocols along with their strengths and weaknesses. A comparative study of the QoS routing protocols is done and in addition, the current issues and future challenges that are involved. It is found that there are a number of unsolved challenges that need to be addressed to design QoS routing protocols for mobile ad-hoc networks. These are maximization of accuracy of QoS routing protocols, minimization of control overhead, route maintenance, resource reservation, cross layer design, power consumption as well as robustness and security. Solving the existing QoS routing issues require the design and development of new QoS routing protocols in MANETs which will allow future ad-hoc networks to meet user expectations.

The dynamic topology of MANET poses a real challenge in the design of a MANET routing protocol. A paper given by ***[Nurul 2010]*** considers the problem from a different perspective, using a simulation model the combined effect of node density and packet length; node density and mobility on the performance of a typical 802.11 MANET is investigated.[2] Based on the QoS (end-to-end delay, throughput), routing load and packet retransmissions, this paper systematically analyzes the performance of four diverse MANET routing protocols with the different simulation model and configurations, and drew more complete conclusions.

The security of the AODV protocol is compromised by a particular type of attack called ‘Black Hole’ attack. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. ***[Latha 2008]*** proposes an approach to combat the Black hole attack [3] is to make use of a ‘Fidelity Table’ where in every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a ‘Black hole’ and is eliminated. Simulation shows that given protocol provides better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead.

Mobile Ad hoc Networks shows unexpected behaviour with multiple data streams under heavy traffic load such as multimedia data when it is sent to common destination. The main reason for packet loss in mobile ad hoc networks is due to congestion. to control losses in MANET ***[Basavaraju 2006]*** provide an study according to the current design, the routing protocols are not congestion adaptive. The way in which the congestion is handled results in longer delay and more packet loss. When a new route is needed the routing protocols take significant overhead. In this paper author propose an adaptive congestion control algorithm, which out-performs even during constrained situation. For analyzing the performance they have chosen four popular routing protocols such as AODV, DSR, DSDV and TORA. The proposed congestion control routing protocol outperforms all the other routing protocols during heavy traffic loads. They strongly argue that routing should not only be aware of but also be adaptive to network congestion. But in case of proactive protocol scenario does have impact on the performance In normal cases AODV better then DSR using packet delivery ratio and average delay. But in constraint situation of many CBR sources leading to same destination, DSR works better than AODV and DSDV. In this paper author have considered die non-congested route, which yields good results in constraint environment. The performance of AODV and DSDV was improved by using local proactive mechanisms which are quick reactive to local route repairs to overcome the problem of congestion. The future work can extend to other scenarios by changing the traffic load and network density.

This paper describes the detection, prevention of black hole attack with improved performance. Thus first required to understand how the black hole is deployed in MANET.A Black hole is formed during the week routing infrastructure. When a malicious node joins the network this problem arises. This node falsely replies for route requests without having an active route to the destination and exploits the Routing Protocol to advertise itself as having a good and valid path to a destination node. Actually in AODV routing for find the path between source and sink RREQ packets are flood and all the path replies with RREP packets if malicious node RREP is arrive first then the requester node suppose the provided information is correct and reply with the data packets. [5]

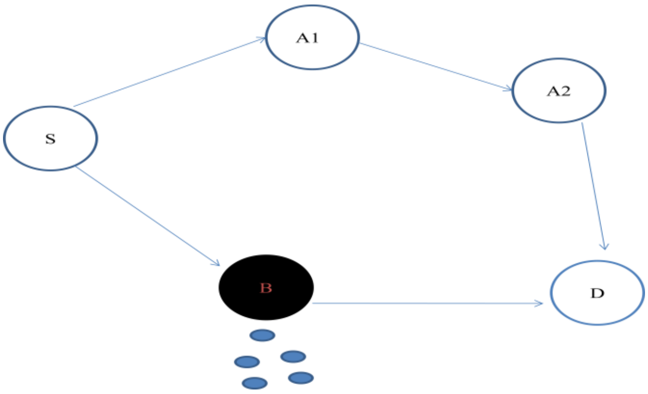


Fig. 1 shows black hole attack

As shown in Fig1, a malicious node tries to become an element of an active route which is reply first, if there is a chance and it has bad intention of disrupting data packets being sent to the destination node or obstructing the route discovery process.

This section describes the background works that are studied during investigation of security and performance related works that are provided previously. in next section we describes how the proposed system is working and implementing.

III. Proposed System

MANET is a new kind of technology where no fix and centralized authority is available to keep track the security and management of network. Therefore, that is frequently faces issues of performance due to mobility and security due to its ad hoc nature. In MANET wifi enabled devices are simulating co-operative behaviour by which communication becomes possible. There are various methods are available for detection and prevention of the black hole attack these methods are simulates effective approaches to detect and prevent the attacks more accurately. In order to detect and prevent the attack the attacker nodes are not responding any packet during attack formation is observed and identified as the malicious node. In our observations some most frequent techniques are

1. **Routing Protocol improvement:**verious authors proposed and implement routing protocol based security to improve security against any individual attack i.e. black hole and flooding attacks.
2. **Certificate based:** some authors are provides certificate based authentication schemes for detecting and preventing an individual kinds of attack mostly used for wormhole detection and DoS attacks.
3. **Cross layer:** some of them are promoting cross layer authentication based schemes, that is an enhanced and more promising method but sometimes this technique is not much effective for different attacks.
4. **Clustered architecture based:** some authors are supporting the clustered architecture of MANET and providing security on different level, on observation that is more feasible and efficient approach, but this domain is also limited with a limited number of attacks.

Due to study found that, most of the methods are uses this property and a similar effort, and in [3] author is able to detect a black hole attack in network.and proposed method in [4] is efficient for congestion control.

In this proposed work trying to improve the problem identified in submission [3] for delay, by which this method becomes more effective and efficient.In order to find the solution objective the below given steps are involved for finding an optimum way of implementation.

Finding path from source to destination: Source node sends RREQ to all neighbours and all the nodes that received the acknowledgement forward it to their neighbours with this limited broadcast RREQ travels until the destination node is found or a node which have latest path to destination, freshness of path is decided by sequence number. The nodes with fresh enough path send a RREP to the source. Source will receive RREP until specified time and store all the path is a table than select best path on basis of average fidelity level of the paths. Path with highest fidelity is selected if a more than one path tie for it than path with lowest hope count is selected.

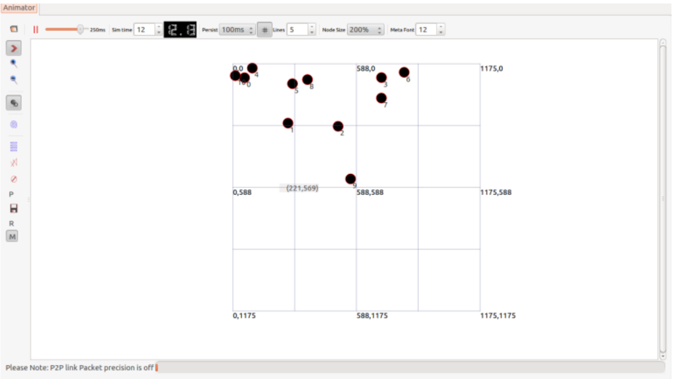
Transmitting data from source to destination: After route is decided source starts sending data to destination via the specified route it suffers from frequent delay because it has to wait for acknowledgement here the solution is to divert traffic to other route if possible for this a variable is introduced called congestion level Cl its value is decided by number of packet buffered divided by total buffer size if the value of Cl is less than a particular threshold value than data is transmitted via second best path from the table in which all the path are stored. This provides a hike in performance and also keeps it safe from any packet dropping attack.

Detection and Elimination of Black hole attack : When a node is dropping data packet, and acknowledgement is not received. then source have to decrement fidelity level of node which replied to RREQ packet by RREP and the node next to it which claimed to have link to destination node. Fidelity levels also have to be exchanged periodically, when fidelity levels of any node drop to zero than this node is considered as attacker and have to be eliminated from network. The information about node with zero fidelity level needs to be told to every other node so it is also broadcasted by source node so that in future every node can avoid attacker.

To implement the desired simulation using ns3 network simulator the below given simulation parameters are required.

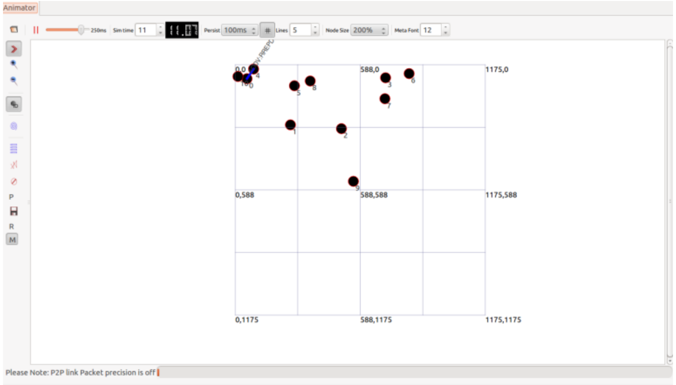
Network parameters	**Parameter values**
Simulation size	1000X1000
Loss model	RangePropagationLossModel
routing protocol	AODV
Simulation time	500ms
Number of node	10
Channel	wifiChannel
Traffic	UDP
Mobility	RandomWalk2dMobilityModel

Network scenarios by which the system is define, which is given by two screens. the provided scenario is described as.



Please Note: P2P link Packet precision is off

Figure 2 shows first network Scenario



Please Note: P2P link Packet precision is off

Fig 3 shows after preventing black hole

Scenario 1: in first scenario normal network with wifi nodes are provided and black hole attack is deployed over the network which is given using the fig 2.

Scenario 2: in this simualtion the proposed approach of detection and prevention is applied over network and performance is estimated which is given using fig 3.

IV. IMPLEMENTATION AND RESULTS

This section of the presented document provides the results and the performance of the designed algorithm.

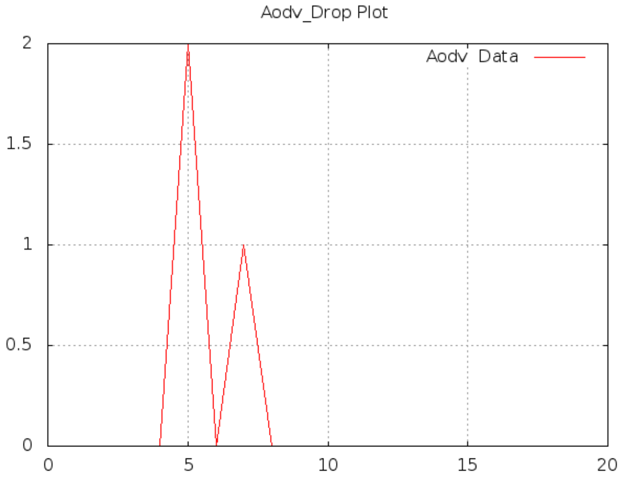


Fig 4 shows the PDR normal conditions

Packet drop ratio

Provides the number of packets drop during communication sessions, which is evaluated using the below given formula.

$$packetdropratio = \frac{totaldroppackets}{totalsentpackets}$$

To obtain the PDR we implement the ADOV routing protocol using NS3 simulator in MANET environment. After forming attack, we evaluate the packet drop ratio in same simulation scenario.After analysis we found that during attack packet drop ratio increases in each session.

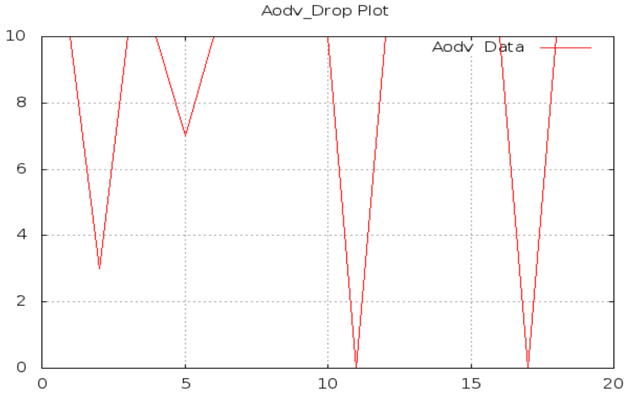


Fig 5 PDR during the attack conditions

After implementation of the proposed method, we found the effective results and packet drop is again calculated during attack conditions.

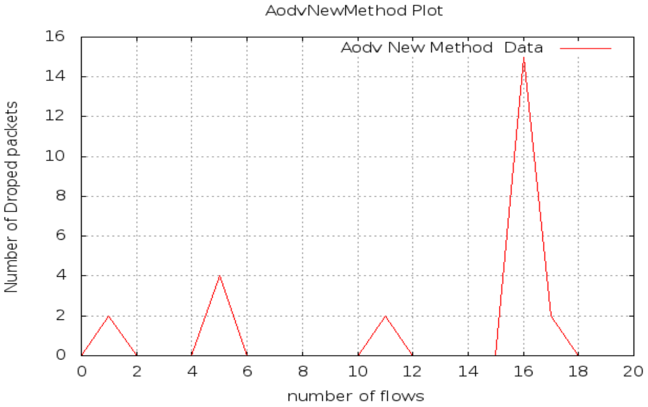


Fig 6 shows the PDR after preventing the attack

After evaluation of packet drop ratio we found that the PDR is effectively improved using the proposed technique.

PACKET DELIVERY RATIO

Provides information about the performance of any routing protocols, where PDR is estimated using the formula given

$$packet\ delivery\ ratio = \frac{total\ delivered\ packets}{total\ sent\ packets}$$

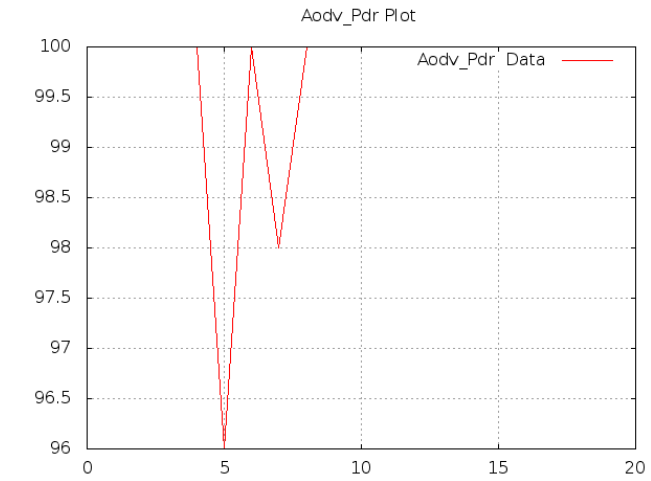


Fig 7 shows the packet delivery ratio

Simple AODV routing is implemented in MANET environment and estimated packet delivery ratio is given using figure 7.

After that we apply the attack on the same implemented network scenario and got the performance of network data delivery, but the no packets are delivered at the target node and we get the below given using fig 8.

END-TO-END DELAY

Refers to the time taken for a packet to be transmitted across a network from source to destination

$$D_{end2end} = N\left[D_{trans} + D_{prop} + D_{proc}\right]$$

$D_{end2end}$= end-to-end delay

D_{trans}= transmission delay

D_{prop}= propagation delay

D_{proc}= processing delay

Where

$$N = number\ of\ links(Number\ of\ routers + 1)$$

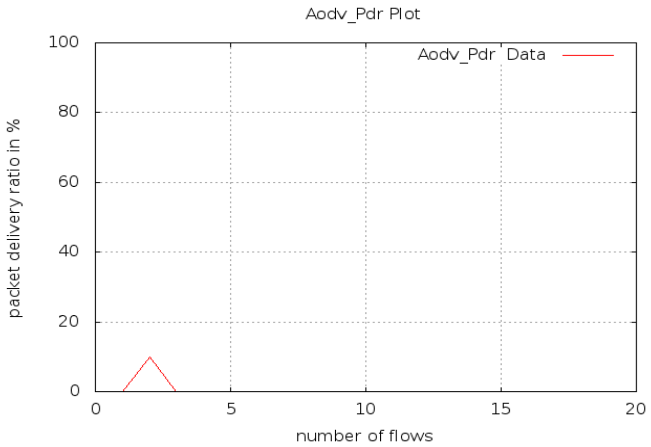


Fig 8 shows the Packet delivery ratio during attack

in normal condition of AODV implementation, performance is evaluated which is given by the below given performance graph.

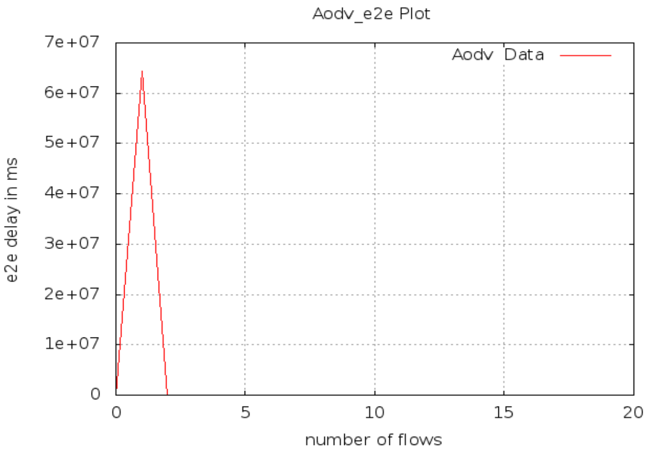


Fig 9 shows the end to end delay of the system

Our main aim is to improve the end to end delay after implementation of proposed technique results are improved. the improved end to end delay is given using figure 10,11 and 12.

Network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bit/s or bps, and sometimes in data packets per second or data packets per time slot.

The ADOV routing protocol is used for implementation.Throughput is given using below given performance graph, in addition of during attack condition and after prevention of network throughput is provided below. When attack is formed the network throughput is becomes zero.

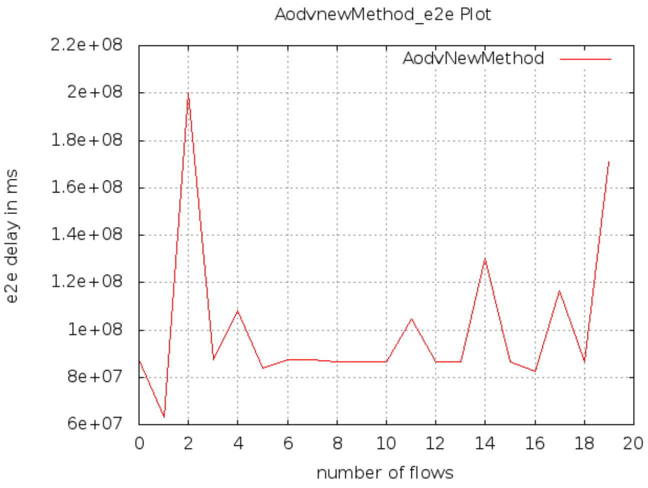


Fig 10 shows the end to end delay

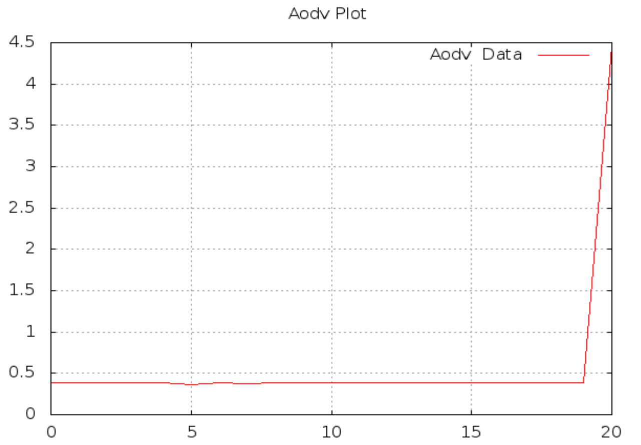


Fig 11 throughput of network in normal conditions

After implementing the proposed technique the throughput of the network is improved and provides the efficient results.In next section provides the conclusion and future extension of the proposed work.

V. CONCLUSION AND FUTURE WORK

In this section of the paper we conclude our study around MANET, we found that most frequent attack is a black hole in MANET. To find a solution for that various algorithms are available. But to resolve security and performance issues some improvements on the routing technique is implemented. And following facts are observed.

1. We found a routing protocol which is providing security and similar efficient AODV routing protocol.
2. We study about two different applications and their combination, which make useful for routing security issues.
3. We study about routing and their aspects additionally we learn about congestion control mechanisms.
4. Design and implement a security algorithm for detection and prevention of black hole attack.

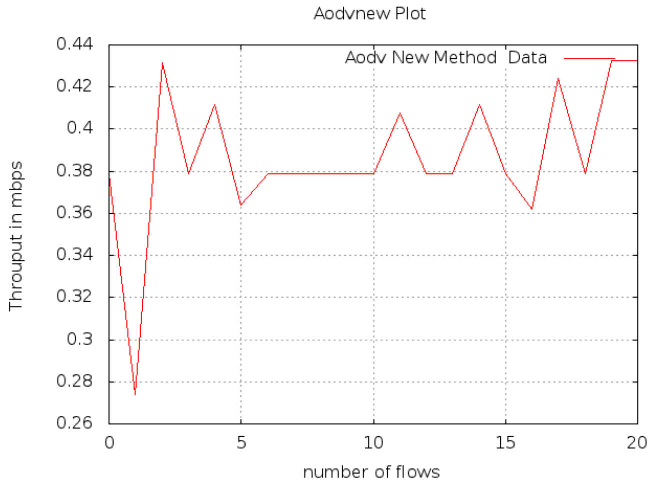


Fig 12 shows the throughput after prevention

Implementation of proposed technique is quite effective for network and able to detect and prevent attack. Additionally the performance of the network is improved effectively.the summaryof performance is given using summary table.

Parameters	Performance	Remark
Packet delivery ratio	Improved	High performance
Packet drop	Decreases	Improved performance
End to end delay	Improved	That is main objective and successfully reduces the end to end delay
Throughput	Improved	High performance

The proposed protocol can able to refine two major issues,security and performance, into one place, but this concept is able to detect only one attack and effective for black hole and in some cases of DOS attacks. In future a framework for security is required, where more than one attacks are handeled.

VI. ACKNOWLEDGMENT

With due respect I would like to inform, that the article which I had proposed is prepared for academic scenario, that is not feasible for industrial research purpose the references which I had taken from listed here, one or not only references there are many other references which I had taken from real world and from daily life aspects. so it is vary through to remember all those references.

VII. REFERENCES

[1] A Review of QoS Routing Protocols in MANETs, Mandeep Kaur Gulati, Krishan Kumar, 978-1-4673-2907-1/13/$31.00 ©2013 IEEE

[2] A Study of MANET Routing Protocols: Joint Node Density, Packet Length and Mobility, Nurul I. Sarkar, Wilford G. Lol, 2010 - ieeexplore.ieee.org

[3] Prevention of Co-operative Black Hole Attack inMANET,Latha Tamilselvan,Dr. V Sankaranarayanan,JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008

[4] ECARP: An Efficient Congestion Adaptive Routing Protocol for Mobile Ad hoc Networks, T G Basavaraju and: Subir Kumar Sarkar, C Puttamadappa and M A Gautham, 2006 6th International Conference on ITS Telecommunications Proceedings

[5] DIFFERENT SECURITY ISSUES OVER MANET, PRATIK GITE & SANJAY THAKUR, ISSN 2249-6831 Vol. 3, Issue 1, Mar 2013, 233-238 © TJPRC Pvt. Ltd.

[6] TRUST Level Evaluation for Communication Paths In MANET BY Using Attribute Certificates Shinichiro Inoue, Masakuni Ishii, Naofumi Sugaya, Takeshi Yatagai, Iwao Sasase Dept. of Information and Computer Science, Keio University japan 978-1-4244-7057-0/10/$26.00 ©2010 IEEE

[7] BLACK Hole Attack Prevention Based on Authentication Mechanism. Junhai Luo, Mingyu Fan, and Danxia Ye University of Electronic Science and Technology of China, Chengdu, China, 1-4244-2424-5/08/$20.00 ©2008 IEEE

[8] Detection and Prevention of Black hole Attack in MANET Using ACO(Ant Colony Optimization(ACO). Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi Dept. Of Computer Science and Engineering,Visvesvaraya Technological University,Belgaum,Karnataka,India Manuscript revised May 20, 2012

[9] Luke Klein-Berndt, ―A Quick Guide to AODV Routing

[10] Dr.M.S.Aswal, ParamjeetRawat and Tarun Kumar "Threats and Vulnerabilities in Wireless Mesh Networks", International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009

[11] Risk-Aware Mitigation for MANET Routing Attacks,Ziming Zhao, Hongxin Hu, Gail-JoonAhn,IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012