International Journal of Research in Advent Technology, Vol.6, No.12, December 2018
E-ISSN: 2321-9637
Available online at www.ijrat.org

Experimental Results of - An Efficient Approach for Secure AOMDV Routing protocol in Adversarial Environment

Pravin R Satav[1], Dr. Pradeep M. Jawandhiya[2]
[1]*Research Scholar S. G. B. A. U. Amravati ,Lecturer in Computer Engineering, Government Polytechnic Arvi*
[2]*Principal,Pankaj Ladhhad College of Engineering, Buldhana, Maharashtra*
Emails:- prsatav@gmail.com, pmjawandhiya@gmail.com

Abstract- MANET has several security issues and these are overcome by the many solutions. But there are some limitations are not overcome. Several routing algorithms presently working for MANET are suffers from black hole attack. The performance of the network will be degraded in presence of an attack. There will be more than one paths are available on the network, amongst these paths some paths are with malicious node and some are without malicious nodes. For selecting an alternate path without malicious node, AODV routing algorithms has to initiate new route discovery process but there are many more chances that the malicious node took part in this process and the issue of selecting secure path is not solved. This route discovery process may decrease the battery power significantly. If an attack is detected in the network then there should be some automated mechanism which will choose the alternate path automatically which will be reliable and secure. This will promote the use of multipath routing algorithm for routing purpose. As the there are many multipath routing algorithms are discovered for MANET. AOMDV multipath routing algorithm is used to achieve & solve the black hole attack problem by selecting an alternate route

1. INTRODUCTION

The most common problem of every network is to achieve reliability without any overhead and at a reduced cost. Intermediate neighbor's nodes in a network that are used in transferring the packets to destination sometimes cannot be trusted. That means nodes may misbehave either by dropping the packets intentionally or by sending the packets through other nodes those are not on the path to that destination. There were many solutions proposed but had weaknesses such as routing overhead, which in turn creates cost overhead. So, there is a need to examine the nodes that are misbehaving in mobile ad hoc networks and to avoid such problems and prevent the network from being attacked. Due to the misbehavior of nodes, network performance can be degraded to a bad level. There may be serious attacks prone to the network because of these misbehaving will be blackhole nodes. Gradually network providers are under a serious threat and users cannot find reliability and efficiency in the network. This is the reason for detecting misbehavior of nodes in the networks is one of the important challenges.

2. LITERATURE SURVEY

In [1] proposed a technique for detecting as well as defending against a cooperative black hole attack using True-link concept. True-link is a timing based countermeasure to the cooperative black hole attack. The author shows the performance of MANET decreases for an end to- end delay, normalized routing overhead and increases throughput and packet delivery ratio.

In [2], Proposed a security and performance issues of MANET. A novel cluster oriented concept is proposed to enhance security and efficiency of the network. The proposed strategy ensures the optimum performance of MANET in presence of black hole attack.

In [3], Proposed method can detect and isolate black hole and gray hole attack that is if the attacker is dropping the packets but if the attacker modifies the data packets without dropping the packets then this proposed method cannot detect this kind of attacks so we can extend the proposed methodology by using cryptographic hash function to detect and isolate packet modification attacks.

In [4]Proposed Ad-hoc On-demand Multipath Secure Routing (AOMSR) a Blackhole node detection system for mobile Ad-hoc network using a Permutation-Based Acknowledgment (PBACK). This technique uses Ad-hoc Distant Vector Routing (AODV) protocol to achieve this goal. AODV is used because it is a simple and efficient routing protocol designed specifically for use in the multi-hop wireless ad-hoc network. This mechanism solves the blackhole node problem using a lesser number of broadcast messages, as compared to other proposed and practiced techniques so far.

Discovery of a malicious node in the network, by intrusion detection system (IDS), is proposed [5]. In this system, authors assigned the unique identification

code to the malicious node present in the network and circulate this ID code to the all the nodes present in the network. This ID node will be blacklisted from the routing process. This methodology identifies and produces the assumption against misbehavior in routing through the malicious attack. The author created a network with black hole attack. For validating the results of the proposed technique, proposed IDS scheme is applied and calculated the performance of the network. This calculated performance of proposed technique is compared with the performance result after applying the existing AOMDV routing algorithm on this network and found that the performance of the network in both situations is same but the malicious activities of a malicious node are suspended and recover the 95 % of data as compared to the normal routing protocol. They suggested future work to apply this scheme to another attack and also analyze the effect of an attack on energy consumption of mobile nodes.

SDTP [6] is based on link-disjoint multipath routing protocol with key management. This proposed innovative protocol aasures the guarantee to protected data communication in ad hoc networks. The projected protocol ensures the truthfulness, privacy, approval and accessibility of data transmission in ad hoc networks. Ad hoc network uniqueness should be taken into consideration to be capable to propose efficient solutions. This approach takes advantage of multiple paths between nodes in MANETs to ensure the security.

SALR [7] Secure Adaptive Load-Balancing Routing protocol, is projected with the routing assessment is taken at each hop considering the unpredicted changes in the network. Multipath selection based on node strength is done at each hop to choose the most protected and least congested route. The system predicts the most excellent route slightly than running the obstruction recognition and security schemes constantly.

Trust-based Secured Adhoc On-demand Multipath Distance Vector (TS-AOMDV) [8] is a expansion of AOMDV. The projected TS-AOMDV deals with recognizing and separating the attacks such as black hole, gray hole, flooding attacks in MANET. Intrusion Detection System (IDS) and trust-based routing, helps for attack identification and isolation are carried out in two phases of routing namely as path detection and data forwarding phase. IDS make easy entire routing protection by examining both data packets and control packets that are concerned in the route recognition and the data forwarding phases. TS-AOMDV provides enhanced routing performance and security in MANET.

Authors [9**]** had done the comparative analysis impact of blackhole attack on network and to present the study of existing methods for preventing the blackhole attack in MANET. These methods have benefits like higher packet delivery or support multiple black hole attack at the same time. All of these methodologies have some or the opposite drawbacks, either it might be having higher overhead, higher packet loss, doesn't support cooperative black hole attack or increased end to end delay. Primarily based on the above performance comparisons, it can be concluded that Black Hole attack affects network negatively. Thus there is a desire for perfect detection and elimination of black-hole mechanism that relies on cluster organization of network. This supports cooperative black hole attack and additionally offers way to facilities the server node to overcome the failure. Thus providing security for Black hole attack and Efficient in detection and prevention are the future need for Ad hoc networks.

Authors [10] considerers the black-hole attack is one of the most well-known active attacks that degrade the performance and reliability of the network as a result of dropping all incoming packets by the malicious node. Black-hole node aims to fool every node in the network that wants to communicate with another node by pretending that it always has the best path to the destination node. Authors propose a new lightweight technique that uses timers and baiting in order to detect and isolate single and cooperative black-hole attacks. During the dynamic topology changing the suggested technique enables the MANET nodes to detect and isolate the black-hole nodes in the network. The results of the suggested technique in terms of Throughput, End-to-End Delay, and Packet Delivery Ratio are very close to the native AODV without black holes. As a future work, aim is to enhance the proposed model in order to increase the Throughput and Packet Delivery Ratio also to decrease the End-to-End Delay.

Authors [11] have proposed a protocol called as Mitigating Black Hole effects through Detection and Prevention (MBDP-AODV) based on a dynamic threshold value of the destination sequence number. In order to validate the efficiency of proposed protocol, the NS-2.35 simulator is used. The simulation results show that proposed protocol performs better as compared with existing one under black hole attack. From the simulation results, it has been found that our proposed protocol performs well as compared with the existing one in term of packet delivery rate and average throughput under black hole attack. It has also been found that the when the threshold value of K = 3, it performs slightly better as compared when the value of K = 4 under black hole attack due to the fast calculation of dynamic destination sequence number based threshold value. Moreover, with the increase in malicious node percentage, the performance of MBDP-AODV decreases. The limitation of this protocol is that it cannot detect smart gray hole attack due to its participation in route discovery process. As a future

work, planning to extend this approach for dealing with smart gray hole attack.

Authors [12] looks at utilizing the inherent trust relationship among the nodes in a MANET by formulating a trust model to recognize the trustworthiness of a node. This trust model makes use of intrusion detection to detect, identify and mitigate Black hole attacks. The proposed mechanism is able to provide a substantial improvement in the affected network in terms of throughput and PDF, although it experiences higher end to end delays.

3. METHODOLOGY DESCRIPTION

The main objective of the proposed system is to inspect all the nodes in a network through their reliability value where all nodes are marked as reliable or malicious on their behaviors. When route discovery starts it will check the nodes trustworthiness if nodes are trusted then the route is established with these node and mark these routes as a reliable routes. If there is route with malicious node i.e with not trusted node then that route is marked as a unreliable. For marking route is reliable or unreliable we modified the routing table structure of the AOMDV routing protocol. Finally, the proposed method efficiently identifies blackhole nodes are present or absent on route by their trustiness.

Existing conventional methods create an extra overhead to the network and consume more time and cost but could not provide an efficient way of detecting the blackhole misbehaving node. This algorithm improves the efficiency of the network and this is done in a lower cost.

While developing, a proposed approach route reliability parameter is added. While source node start route discovery between sources to the destination, this proposed approach will categories the paths as a reliable or unreliable. Routing table structure of AOMDV contains various parameters like destination nodes IP address, destination sequence number, advertisement hop count, path list, expiration route. The path list contains information on the path with its hop-count and IP addresses. Path list consists of the combination of next hop IP and its count.

4. PERFORMANCE METRICS

a. End to End delay

The source will generate a packet at some time interval. This packet travels through various nodes present in the path. It is not necessary that the communication path is always ready or available to carry the source nodes packets. Each node will take some time interval for receiving the packet and transmitting the packet. Sometimes delay takes place because about the discovery of route, queuing, intermediate link failure, packet retransmissions, etc., while calculating the delay. End-to-end delay is the average time required for successful transmission of the packet to the destination. While calculating end-to-end delay by abstracting the time at which the first packet was sent by sender node from the time at which first data packet is reached to the destination node. End to end delay can be graphically shown as an average end to end delay versus a number of nodes. End to End delay is inversely proportionate to the number of nodes. Routing protocol perform better when the end to end delay is less.

$$\text{Average E\_to\_E delay} = \frac{\sum \text{time spent to deliver packets for each destination}}{\text{Number of packets received by the all destination}}$$

b. Throughput

This parameter measures, how the data is consistently transferred to the sink node by the network. These metrics calculate the total number of packets delivered per second, means the quantity number of messages which are delivered per second. This nothing but the average rate of a number of packets received successfully to the destination from the source node. Every network developer expects the higher level of throughput. But there are some aspects which will affect the throughput are untrustworthy communication, dynamic topology, bandwidth and limited energy. Throughput generally depends on several of factors of networks such as scheduling policies, power control, routing approaches, packet collision, , obstacle between nodes, acknowledgment and network topology. Presence of malicious node in the network decreases the throughput because the malicious blackhole node discards some of the packets [Lineo Mejaele et.al 2016].

$$\text{Throguhput} = \text{Number of packets delivered} / (\text{stopTime} - \text{startTime})$$

c. Packet Delivery Ratio

In MANET source node will transmit the packets to the destination amongst multiple hops. While sending these packets, the source is expecting that all packets sent by him must be reached to its destination node. Packet dropping in MANET is due to so many reasons are listed below

- Un stability network
- Link breakage
- Crowded traffic
- The overflow of the transmission queue
- Due to energy constraints
- Presence of Malicious node.

The source node can check how many packets are reached to the destination node. Checking the ratio of a number of packets reached to the destination node out of the numbers of the packets sent by the source node is known as packet delivery ratio. A generalized expression of calculation of packet delivery ratio is as

Packet Delivery Ratio

$$= \frac{\sum_{i=0}^{n} \text{Recived Packets}}{\sum_{i=0}^{n} \text{Packets sent}} \text{ X } 100$$

Packet delivery ratio plays a very important role in network processing capability and data transfer capability. Reliability, effectiveness, integrity, and correctness of the routing protocol are depending on this PDR. Performance of the protocol is inversely proportional to the PDR.

5. SIMULATION AND PERFORMANCE ANALYSIS

Network Simulator-2.35 to simulate our proposed scheme.

6.1 Simulation Environment.

Table 1 employs the simulation setup. To test the performance of our mechanism, a simulation scenario with the support of the network simulator *ns-2* [106] is used. Each mobile host has an omni-directional antenna having unity gain with a nominal radio range of 250 m. The random waypoint model is selected as a mobility model in a rectangular field (1000 x 500 meters) with a nodes' speed uniformly between 0 and a maximum value of 10 $m.s-1$. Nodes remain stationary for a specified period called the "pause time". In the simulation work, we are considering the proposed ad hoc on demand vector routing (AODVM) protocol and ad hoc on demand vector routing (AODVM) protocol under blackhole node. The total simulation time is 10 seconds. The detailed simulation parameters are mentioned in table 1. To evaluate the performance of the proposed protocol, the following metrics are used.

Table 1.Simulation parameters.

Parameter	Value
Simulator	NS-2(Version 2.35)
Simulation Time	10 S
Number of mobile nodes	05,10,15,20,25,30,35,40,50
Maximum Speed	20 Meters/second
Topology	500 * 500 meters
Node Placement Strategy	Random
Mobility Model	Random Way Point
Routing protocol	AODV, SBHAODV,CBHAODV SBHAOMDV,CBHAOMDV PAOMDV
Traffic	Constant Bit Rate

Simultion result and analysis

a. Comparative Analysis of end to end delay with single & multipath routing protocol.

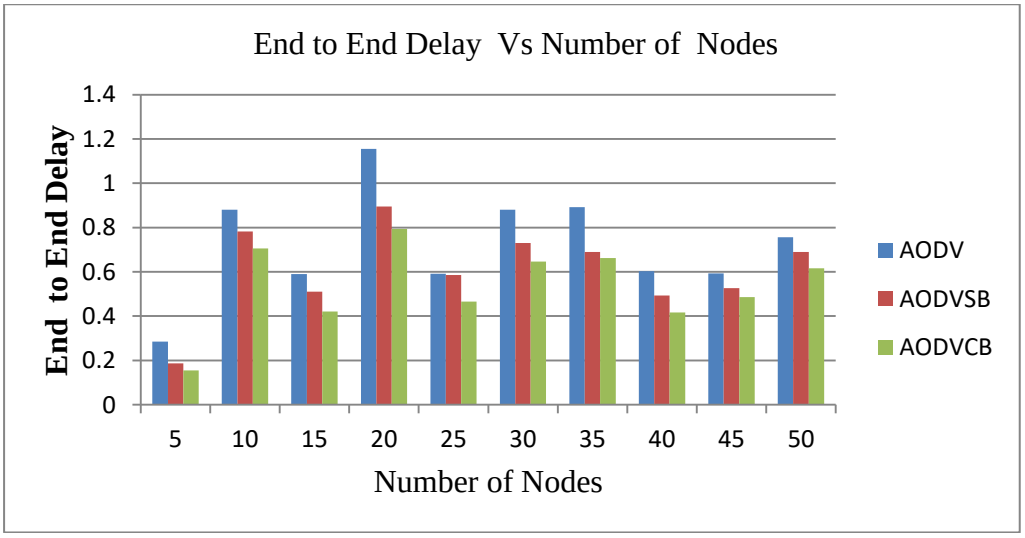

Fig1:- End to End Delay vs Number of nodes of AODV Routing protocol without Mobility

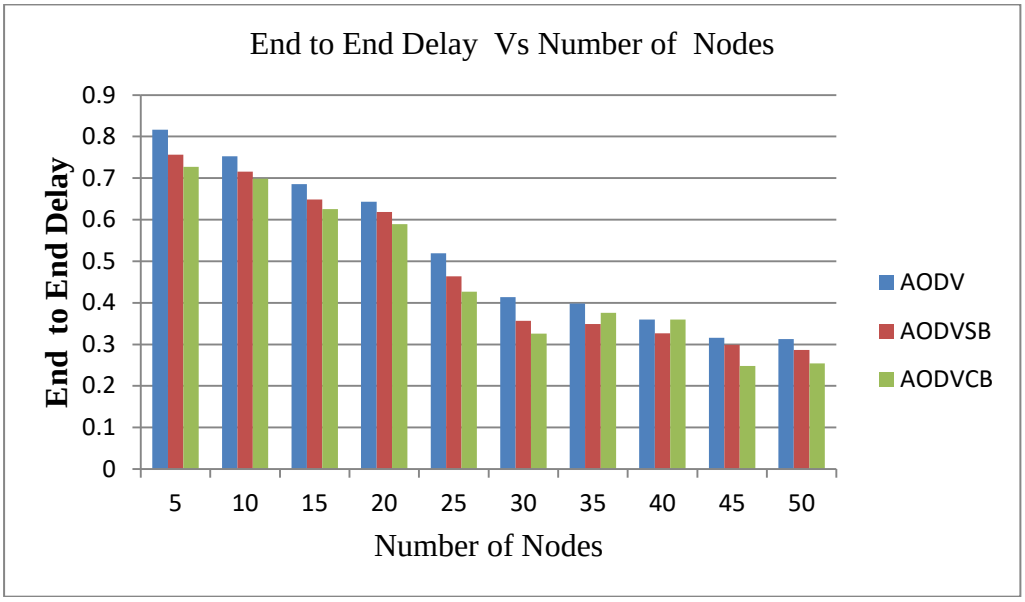

Fig 2. End to End Delay vs Number of nodes of AODV Routing protocol with Mobility

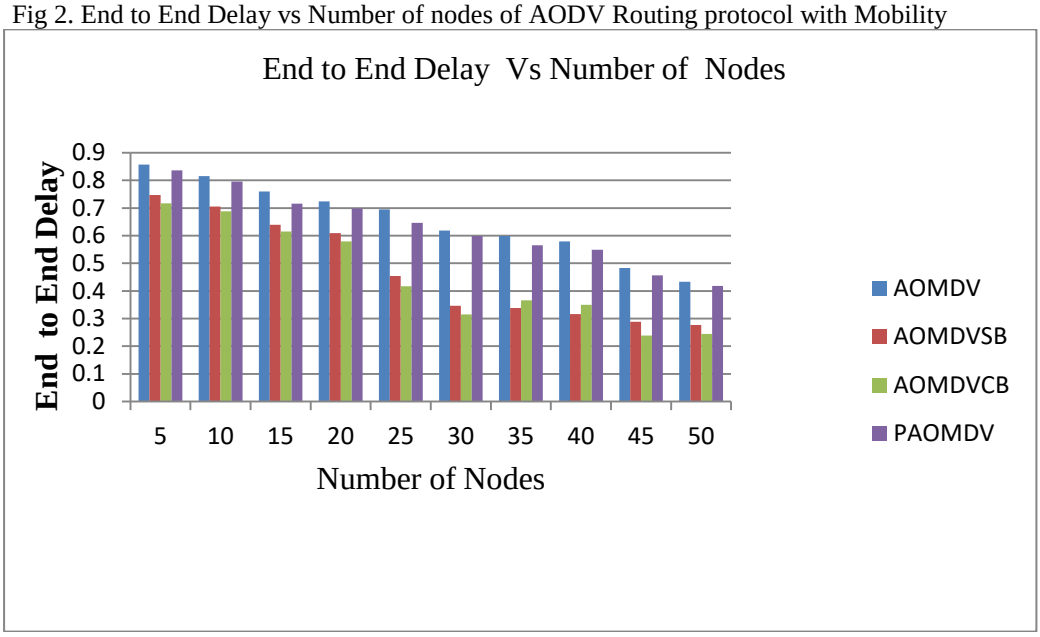

Fig 3. End to End Delay vs Number of nodes of AOMDV Routing protocol an Proposed approach without mobility

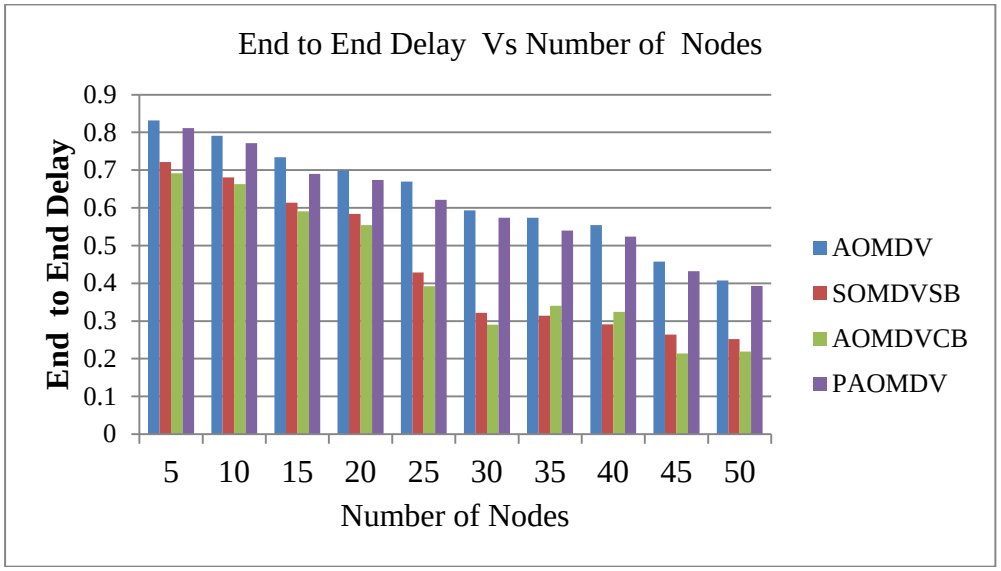

Fig 4 End to End Delay vs Number of nodes of AOMDV Routing protocol and Proposed approach with mobility.

b. Comparative Analysis of Throughput with single & multipath routing protocol.

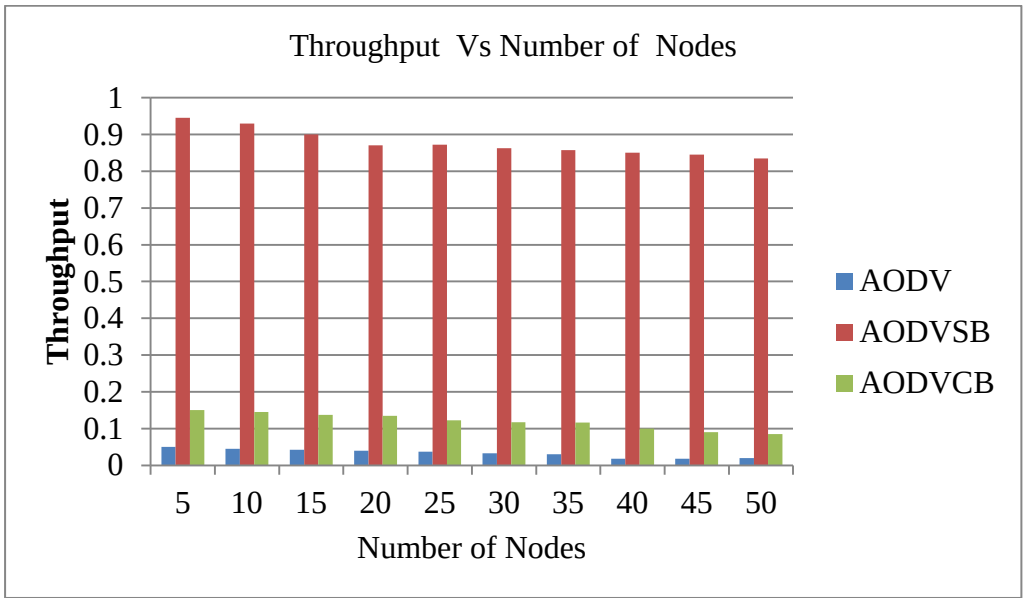

Fig 5 Throughput vs Number of nodes of AODV Routing protocol without mobility

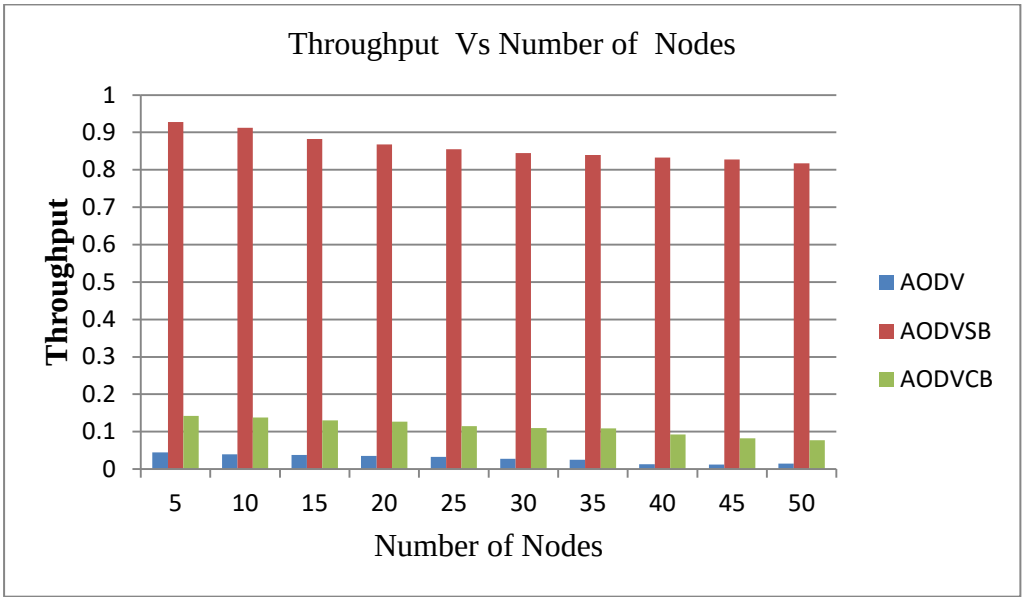

Fig 6 Throughput vs Number of nodes of AODV Routing protocol with mobility

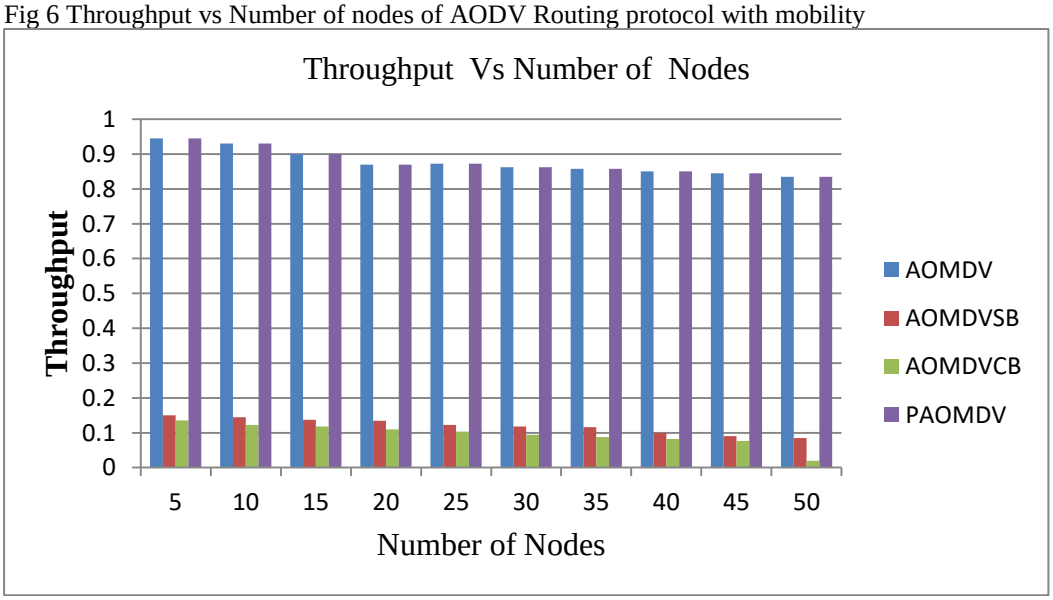

Fig7 Throughput vs Number of nodes of AOMDV Routing protocol & Proposed Algorithm without mobility

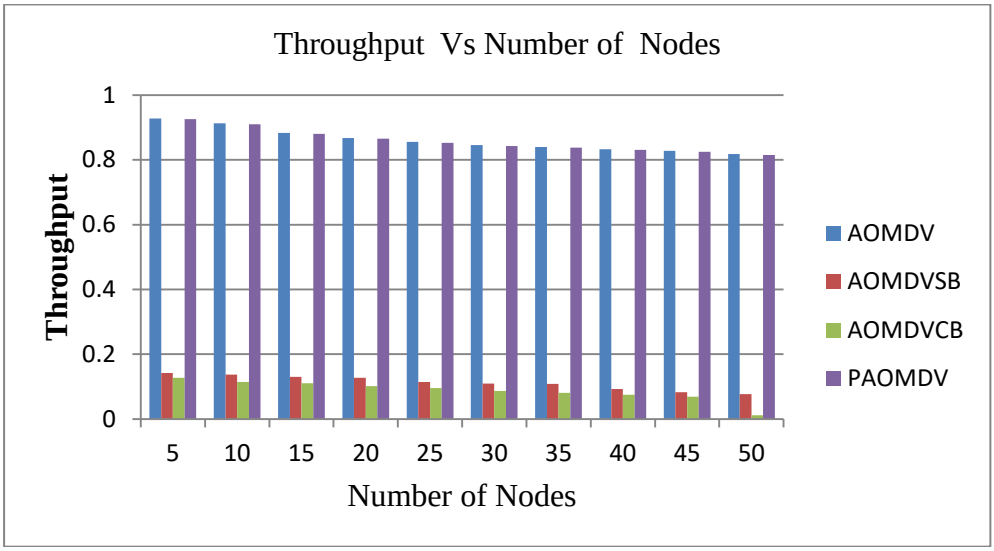

Fig 8 Throughput vs Number of nodes of AOMDV Routing protocol & Proposed Algorithm with mobility

c. Comparative Analysis of PDR with single & multipath routing protocol.

Blackhole nodes presence is one major security threat in MANETs that can affect the performance of the underlying protocols. These simulation results, shows that the presence of Blackhole node/s in network, how it can affect network performance. Presence of black hole node in the network absorbs all packets only and these are not delivered to the destination node. Because of this type of behavior the PDR and throughput becomes zero in presence of blackhole attack in the network [A.A.Chavana et.al 2016]. Simulation results illustrate that network with AODV routing protocol has on average 2.75 % data loss and if a there is blackhole node is present in such network then data loss is increased to 90.38 %. Network with normal behavior founds 2.75 % data loss and presence of the blackhole node will increases this data loss by 87.63 %. In this proposed work, options for detecting the blackhole misbehaviors are proposed as entails route discovery, contact chances into nodes and assignment constraints imposed on nodes. With higher energy, the node is able to contribute more cooperation as well as more packet delivery ratio. It is necessary that the security scheme adopted to face the blackhole behavior of a node have to enforce the execution of both the packet forwarding and the AOMDV functions.

Figure 9 to 12 presents the Packet Delivery Ratio (PDR) of proposed modified AOMDV routing protocols with one black node and varying node velocity. In a moderate density network, when there is blackhole node in the network, network shows a lower packet delivery ratio as blackhole node in active mode. On the other hand, with increasing node velocity PDR of network achieves moderate performance in the presence of blackhole node. The PDR of proposed AODVM is improved between 70% to 80% in all cases, it shows once blackhole node detected, performance of network improved.

Selection secure route for communication achieves noticeable improvement in the PDR. PDR is affected by various parameters like presence of malicious node in network mobility of nodes, end to end delay and queue overflow.

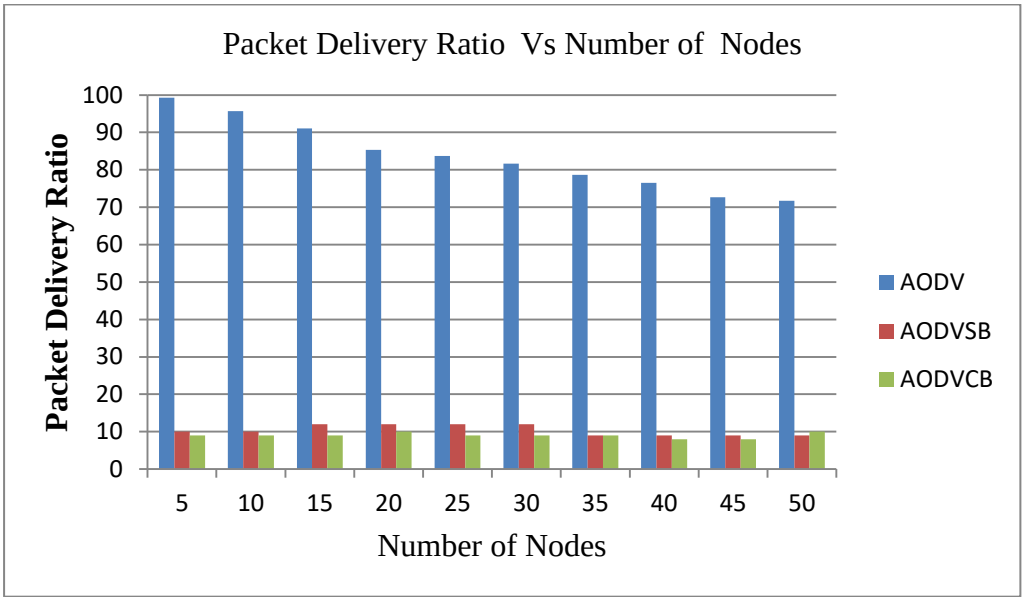

Fig.9 Packet Delivery Ratio VS Number of nodes of AODV Routing protocol without mobility

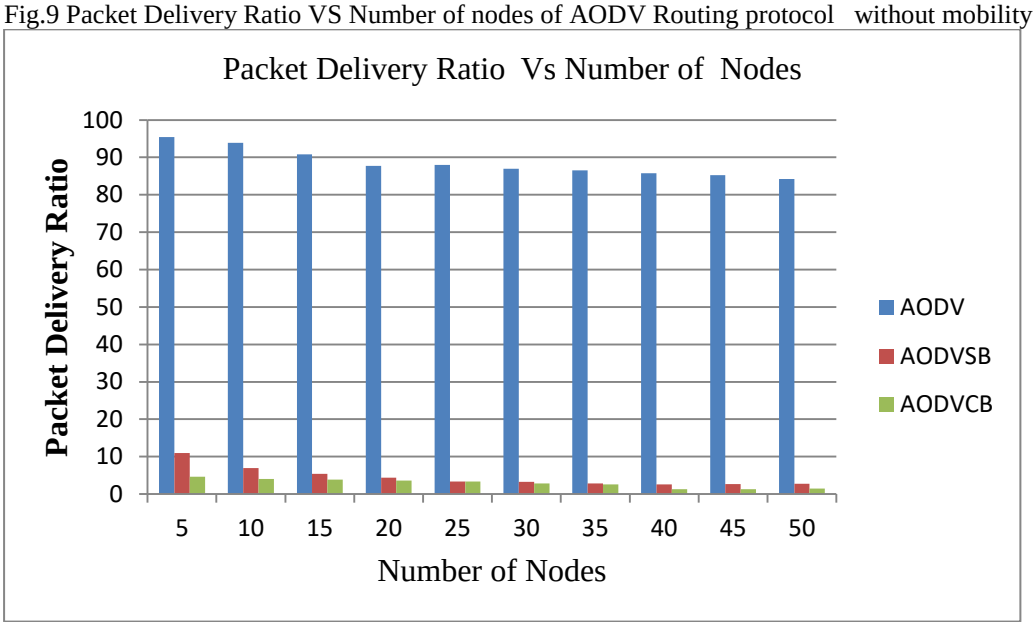

Fig.10 Packet Delivery Ratio VS Number of nodes of AODV Routing protocol with mobility

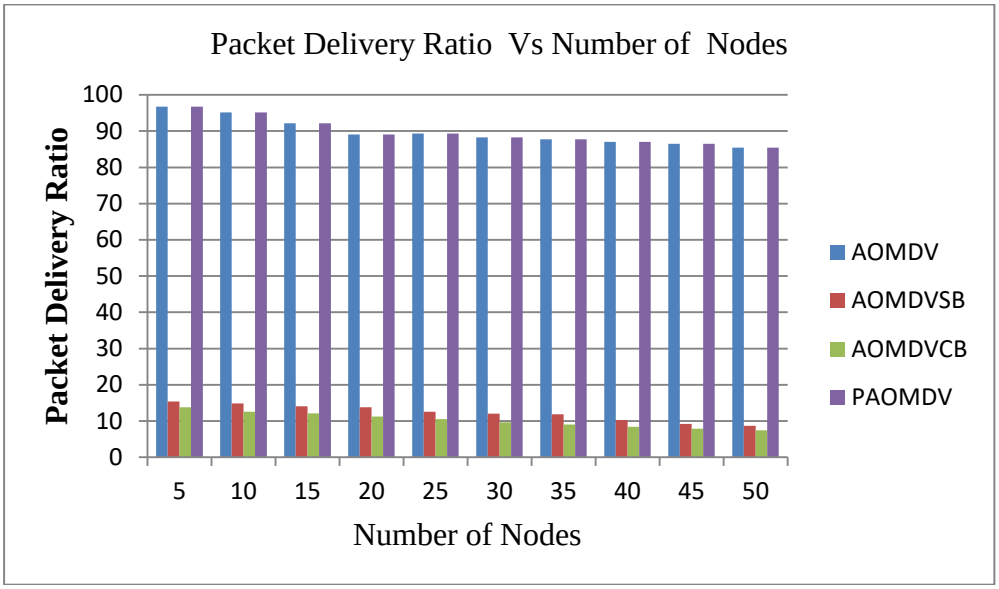

Fig.11 Packet Delivery Ratio Vs Number of nodes of AOMDV Routing protocol and Proposed approach without mobility

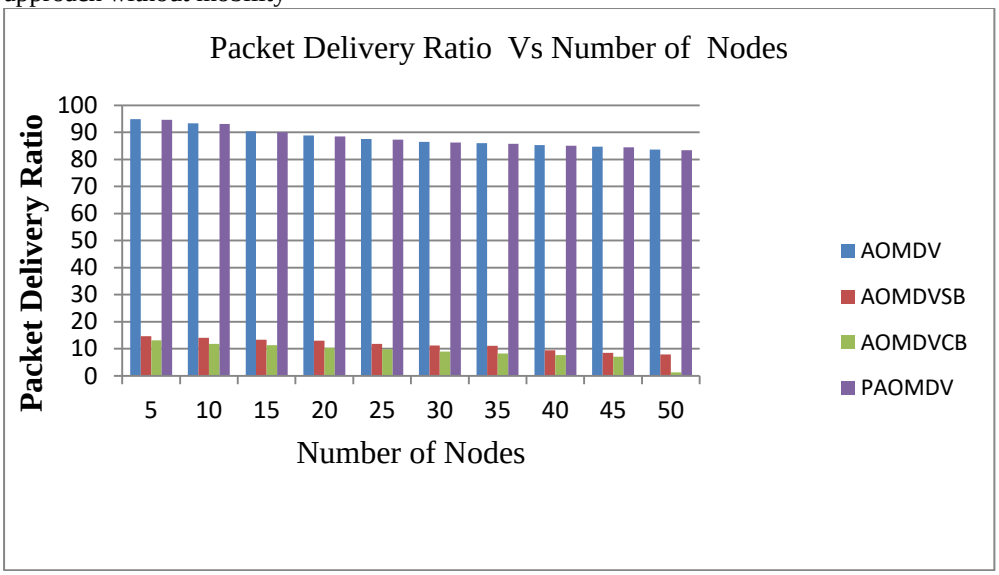

Fig.12 Packet Delivery Ratio Vs Number of nodes of AOMDV Routing protocol and proposed approach with mobility

Table 4.7**:** Comparison Table

Sr. No	Comparison Metric	Limitation of Previous Approach	Merits of Proposed Approach
1	Detection of Different Types of Blackhole Attacks	Various detection schemes proposed are not able to handle collaborative blackhole attacks.	The proposed approach can handle single and collaborative blackhole attacks by selecting an alternate path.
2	Requirement of Extra Memory / Database	Proposed DRI and cross-checking schemes have need of an additional database for accumulating the past routing experiences at each node.	Multipath AOMDV protocol is used. AOMDV stores multiple link disjoint and node disjoint paths towards the destination hence extra memory is not required to proposed approach.

3	Burden on Intermediate Nodes	Intermediate nodes are overburdened due to their involvement for assuring the trustworthiness of the network. This overburden consumes more energy.	For proper functioning of the network, proposed approach will selects the alternate path hence participation of intermediate nodes is required very less for the proper functioning of the scheme. Thus this proposed scheme reduces the overburden of intermediate nodes. Only sender and destination node is responsible for the proper functioning of approach
4	Increase in Performance Metrics like Packet Delivery Ratio, Throughput etc.	Proposed schemes improve in throughput and packet delivery ratio significantly. Throughput is improved by 10 to 20 % and by 50 to 60 % in packet delivery ratio is improved.	Results shows that the packet delivery ratio and throughput were nearer to the original values of the network those were obtained in absence of blackhole nodes in the network.
5	Decrease in the performance metric such as end to end delay		In proposed approach, not necessarily selects the optimal path for delivery of packets selects only secured path hence there is significant increase in end to end delay.

6. CONCLUSION

AOMDV is a multipath routing algorithm is generally used routing protocol for mobile ad hoc networks but this protocol will selects alternate path only when intial path is failure due to any reason. In this chapter, we present how the performance will be improved for the reliable data transmission in MANET by selecting the alternate path and trust based scheme on the AOMDV protocol with detection of single and collaborative black hole nodes. Proposed AOMDV is able to provide reliable communication. This scheme selects the best alternate node disjoint / link disjoint route based on the non-presence of any malicious node in that path. But, normal AOMDV selects alternate path after failure of exiting path but proposed approach will detect the blackhole nodes initially and AOMDV will selects only secured the alternate path for entire communication. The results proved that the detection of single and collaborative nodes in AOMDV based MANET using proposed scheme provides better performance in presence of the blackhole attack.

REFERENCES

[1]. [G.Wahane et.al 2014],Gayatri Wahane, Ashok M. Kanthe, Dina Simunic, "Technique for Detection of Cooperative Black Hole Attack using True-link in Mobile Ad-hoc Networks" IEEE-2014, MIPRO 2014, 26-30 May 2014, Opatija, Croatia, PP-1428-1435.

[2]. [J.Sayner et.al 2014],Jitendra Sayner, Vinit Gupta,"Clustering of Mobile Ad Hoc Networks: An Approach for Black Hole Prevention",in IEEE-14 International Conference on Issues and Challenges in Intelligent Computing Techniques pp 361-365.

[3]. [S.Uyyala et.al 2014],Shivani Uyyala, Dinesh Naik, "Anomaly based Intrusion detection of Packet Dropping Attacks in Mobile Ad-hoc Networks" in IEEE-14 (ICCICCT). PP-1137-1140.

[4]. [D.Dave et.al 2014],Dhaval Dave, Pravnav Dave,"An Effective Black Hole Attack Detection Mechanism using Permutation Based Acknowledgement in MANET", in IEEE-14 International Conference on Advances in Computing, Communications and Informatics (ICACCI).PP-1690-1696.

[5]. [S. Shrivastava et.al 2015], S. Shrivastava, C. Agrawal, A. Jain, "An IDS scheme against black hole attack to secure AOMDV routing in MANET," Int. J. on AdHoc Networking Systems (IJANS), vol.5, no.1, 10.5121/ijans.2015.5101, 2015.

[6]. [Mohommamd faisal et.al 2015], Mohommad faisal Haasn Mathkoot, "SDTP: Secure Data Transmission Protocol in Ad hoc Networks based on Link disjoint Multipath Routing Web Applications and Networking (WSWAN)", 2015 2nd World Symposium

[7]. [Lata.B.T. et.al 2015]Lata B.T and others "SALR: Secure Adaptive Load-Balancing Routing in Service Oriented Wireless Sensor Networks". in Signal Processing, Informatics, Communication and Energy Systems (SPICES), 2015 IEEE International Conference..

[8]. [Abrar et.al 2016], Abrar Omar Alkhamisi, Seyed M Buhari, "Trusted Secure Adhoc On-Demand Multipath Distance Vector Routing in MANET", in 2016 IEEE 30th International Conference on Advanced Information Networking and Applications.PP212-219.

[9]. Marco Mezzavilla, Giorgio Quer_, Michele Zorzi " On the Effects of Cognitive Mobility Prediction in Wireless Multi–hop Ad Hoc Networks" , IEEE ICC 2014 - Cognitive Radio and Networks Symposium, 978-1-4799-2003-7/14.

[10]. Karmveer Singh,Vidhi Sharma "Performance Analysis of MANET with Reactive and Proactive Routing Protocols and Mobility Models " ISSN: 2321-Vol. 2 Issue V, May 2014.

[11]. David Palma, Marilia Curado "Towards Scalable Routing for Wireless Multi-hop Networks" , IEEE, 978-1-4799-0913-1/14 2014.

[12]. Evripidis Paraskevas, Kyriakos Manousakis, Subir Das and John S. Baras "Multi-Metric Energy Efficient Routing in Mobile Ad-Hoc Networks " , IEEE , 2014 Military Communications Conference 978-1-4799-6770-4/14

[13]. AdwanYasin and Mahmoud Abu Zant, "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique," Wireless Communications and Mobile Computing, vol. 2018, Article ID 9812135, 10 pages, 2018. https://doi.org /10.1155 /2018 /9812135.[3]

[14]. Gurung, S. & Chauhan, S, "A dynamic threshold based approach for mitigating black-hole attack in MANET," Wireless Network November 2018, Volume 24, Issue 8, pp 2957–2971. https://doi.org/10.1007/s11276-017-1514-1.[4]

[15]. Biswaraj Sen et.al, "Mitigating Black Hole Attacks in MANETs Using a Trust-Based Threshold," International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 7 (2018) pp. 5458-5463 © Research India Publications. http://www.ripublication.com.[5]

[16]. [Lineo Mejaele et.al 2016],Lineo Mejaele and Elisha Oketch Ochola, "Effect of Varying Node Mobility in the Analysis of Black Hole Attack on MANET Reactive Routing Protocols "in 2016 Information Security for South Africa (ISSA),on 17-18 Aug. 2016at Johannesburg, South AfricaDOI: 10.1109/ISSA.2016.7802930 pp-62-68.

[17]. The Network Simulator - NS-2. (http://www.isi.ed/nsnam/ns/index.html