Prevention and Detection of black hole attack using Trust Based Routing in MANETs

[*]Pranjul Sarathe, [#]Mr. Neeraj Shrivastava

[*,#]Dep. Of CSE, IES IPS Academy, Indore, India. [*]pranjulsarathe@gmail.com,

[#]neeraj0209@gmail.com

ABSTRACT: MANET has gained an esteemed popularity in networking. It is having dynamic nature of random network topology. Security issues are very important in such networks. Black hole attack create most crucial condition in network by which network performance degrade. We have proposed trust mechanism based on trust value, we have recommended a formula to find trust value of each nodes and find a trusted route to communicate from source to destination, and used modified version of AODV routing protocol(MTAODV). If nodes maintain trust value base on our trust method then node is trusted and start communicate between Source to Destination , otherwise discard the route. We also have a simulating tool in form of Network Simulator (NS2.35) and simulation parameters that include Throughput, PDR, E2E Delay and energy.

KEYWORDS: MANET,AODV, MTAODV, Black-hole, Cooperative Black hole .

I. INTRODUCTION

MANETs is an important property is that it can be fastly simulated, and very comfortable for different applications like that: Nodes monitoring, making wireless structure of mobile nodes, it is a self-arranged type of network therefore simulate very easily and fastly and in economical way. A challenging task that comes in MANETs is the analysis of simulating environment of mobile nodes which describes the final analysis of simulating process because in transmission and reception of data a particular time remain most important in MANETs [1].

A wireless network consists of tiny and strongest network of mobile nodes which receives more attention to make nodes of wireless network and has been consider as a faultless MANET's group of mobile networking nodes consists which communicate with each of one another node without the necessity of main authority. In this network of mobile nodes, every wireless node may work as wireless node, making group of nodes whenever receive data packets from adjacent nodes and then transmit to corresponding mobile node[2].

In MANETs, acceptance can be stated as "Proximity of the approximate analysis in middle of entities that take part in routing process". for ex: any company, goodness, aloneness while Quality of Service trust being obtained based on capacity, responsible, experience and number of packets forwarding, etc. This routing is very important and useful for highly aggressive environmental conditions when different nodes functioning to reach their target. Process of Routing Protocol based on this research has been suggested as a key for analysis and abundance with security caused by malicious nodes in Mobile Ad-hoc Networks[3].

In this research article, we presenting an ideal approach and operative trust – based safe routing procedure. Suggested processes choose and transmitted nodes by a studying and analysis to develop an optimal location for dynamic situation. The given solution depend on the trust mechanism which give better performance and safe connection to data transmission and avg. energy capacity[4].

The remaining part of this paper can be described as follows: Section two consists of work related to this articles which published by different authors in past. Section three describes the suggested method for safe and Quality of Service process. Section fourth showing some analysis and results for the benefit of suggested method on 2 different methods in form of necessary metrics. In the end conclusion of this complete analysis. These following measurements and analysis of Routing process in this paper analyze functioning of MANETs[5].

II. REVIEW OF RELATED WORK

V. K. Saurabh et al. [6] in proposed approach nodes are divided into clusters and each will have cluster head and also some check-points are also deployed in the network which will check that no. of packets sent are equal to no. of packets received and proposed approach provided better results related to modified AODV approach.

V. Rishiwal et al. [7] analyzed the performance of network in both homogeneous and heterogeneous MANET(H-MANET), heterogeneity has been introduced in

 DOI : 10.35291/2454-9150.2019.0358

terms of different initial energy and used parameters are PDR, throughput, energy, delay. and the simulation has done in NS-2.

R. Prasad and Shivashankar [8] analyzed and compared the different IDS(intrusion detection system) such as- signature based approach, anomaly based, reputation based approach, behavior based, traffic based and multi-trust based approach, basically IDS is based on security goals like- authentication, integrity, non-repudiation and confidentiality.

L. Prashar and R. K. Kapur [9] analyzed the performance **o**f routing protocols are –proactive routing protocol, reactive routing protocol and hybrid routing protocol under the different types of routing attacks such as- black-hole attack and wormhole attack in MANET and the used parameters are-packet delivery ratio, end-to-end delay and throughput.

G. Vaseer et al. [10] proposed a distributed trust based security mechanism to prevent multiple attacks like- probe, DOS, vampire, in which they used watcher nodes to determine trust of other nodes and performed method based on three steps: route discovery state, steady state and execution state and report above 95% accuracy in data transmission.

III. THE PROPOSED TRUST BASED MECHANISM IN MOBILE AD-HOC NETWORK

The secure level esteem figuring depends on the parameters appeared in the table 3.1. The check field portrays around two criteria achievement and disappointment which depicts whether the communicate was an effective transmission or a disappointment. RREQ and RREP are the course request and course answer separately which is traded between nodes in the system. Information alludes to the payload transmitted by the node in the directing way.

Table 3.1 Secure Value Calculation Parameters

COMMUNICATION TYPE	RREQ	RREP	DATA IN MAX QUEUE SIZE(1000)
SUCCESS	RREQS	RREPS	DATAS
FAILURE	RREQF	RREPF	DATAF

The parameter RREQS is characterized as the course ask for achievement rate which is computed in view of number of neighboring nodes who have effectively gotten from the source node which has communicate it, REEQF characterized as the course ask for not a win rate which is ascertain base on number of neighboring nodes which have not gotten the inquiry ask for, RREPS is characterizes as the course answer achievement rate which is figured as fruitful answers gotten by the source node which has sent the RREQ and RREPF is characterized as the course answer disappointment rate which is figured in view of the quantity of neighboring nodes which have not sent the answers for the question asks forgot. Facts is characterized as the information achievement rate computed in view of effectively transmitted information and DATAF is characterized as information disappointment rate ascertained in light of information which have neglected to achieve goal. Nonetheless, it is perceived that for each system there will be least information misfortune because of different limitations.

$$RRR = (RREQS - RREQF) / (RREQS+RREQF) \quad \ldots\ldots \ldots\ldots (1)$$

$$RPR = (RREPS - RREPF) / (RREPS + RREPF) \quad \ldots\ldots\ldots\ldots . (2)$$

$$RDR = (DATAS - DATAF) / (DATAS +DATAF) \quad \ldots\ldots\ldots\ldots\ldots (3)$$

Where RRR, RPR and RDR are middle of the route esteems that are utilized to ascertain the nodes Request rate, Reply rate and Data transmission rate. The estimations of RRR, RPR and RDR are standardized to fall in scope of -1 to +1. On the off chance that the qualities fall past the standardized range then it obviously demonstrates that the disappointment rate of the node is expanded and means that the comparing node may not be able for directing.

$$TV = (RRR + RPR + RDR) /3 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

Where, TV is the secure esteem and T (RREQ), T (RREP) and T (DATA) are time factorial at which course request, course reaction and information are sent by the node in a specific order. Aside from the previously mentioned standardized range, utilizing the above equation the secure esteem (TV) is figured for every node amid steering and is checked against the edge esteem (extend - 1 to +1).

Table 3.2 Threshold Comparison

SECURE VALUE	ACTION	NODE BEHAVIOR
0 - 0.4	Block	Untrusted node
0.4 - 0.7	Allow	trusted nodes
0.7 – 1	Allow	Most trusted nodes

I. **Untrusted:** The depended node of the system is delegated Unreliable node. These nodes have least secure esteem.

II. **Trusted:** These are the nodes which have the secure level among the Most Reliable and Unreliable. Implies a node is Reliable to its neighbor implies it has sent a few bundles through that node.

III. **Most trusted:** The nodes with higher secure esteems are considered as most solid node.

This node might be the best node for some other transmission between some other source and goal in a similar system. MTAODV checks each node with its secure an incentive to make itself extreme and in charge of

 DOI : 10.35291/2454-9150.2019.0358

valuable and capable directing and furthermore to ensure security in MANET.

3.1 Process of Proposed Work

Input: Network consist random nodes.

Output: Route search and attack on network.

Procedure:

1. We are having a network which consist random nodes. Total number of nodes is 20, 40, 60, 80 and 100.
2. A data packet is require sending from source to destination and for this it will generate a route request (RREQ) and waits for route reply (RREP).
3. When it receives multiple reply then it will decide the best route using trust value, sequence number and hop count.
4. Based on the secure on neighbor and appropriate threshold values the nodes can be categorized in to the following.

- **Un-Secured:** The Un-Secured is the un-trusted. Un-secured nodes are those nodes which are having low trust value. When a new node enters into the network then this relationship with all other neighbor nodes is negligible that time it is treated as Un-Secured node.
- **Secured:** Secured nodes are those nodes which are having secure level in between un-trusted and most trusted. A node is considered as Secured when it received some packets through that node.
- **Most-Secured:** Most-Secured are most trusted nodes which are having highest trust value value. Here high secure level means neighbors had received or transfer many packets successfully through this node.

5. The result of secure estimation function is the Secure-status of all of neighbors as Most- Secured, Secured Un-Secured.
6. When it detects black-hole behavior and packet lost problem it will classify nodes on the basis of their reliability.
7. For the purpose of detection of black hole nodes behavior, corresponding secure table is maintained. This table keeps record of secure status of every node with its neighbors.
8. Working of the table --

This table 4.2 is as taken as reference whenever any node receives the packet. When a new node joins the network it is considered as Un-Secured. Hence, probability of attack is more in Un-Secured then Most-Secured. In case Most-Secured node is not available then we will choose secured node but never choose un-Secured node for the route.

Input: As input it requires values of RREQS, RREQF, RREPS, RREPF, DATAS and DATAF.

Where,

RREQS = RREQS is route request success rate which shows the rate of successfully broadcast requests.

RREQF = RREQF is route request failure rate which is based on neighboring node not received request.

RREPS = RREPS is the success rate of route reply calculated as route reply received by source node.

RREPF = RREPF is the failure rate of route reply

DATAS = DATAS is the success rate of data received.

DATAF = DATAF is the failure rate of data.

Output: Secure value

3.2 Flow Chart of Proposed Work

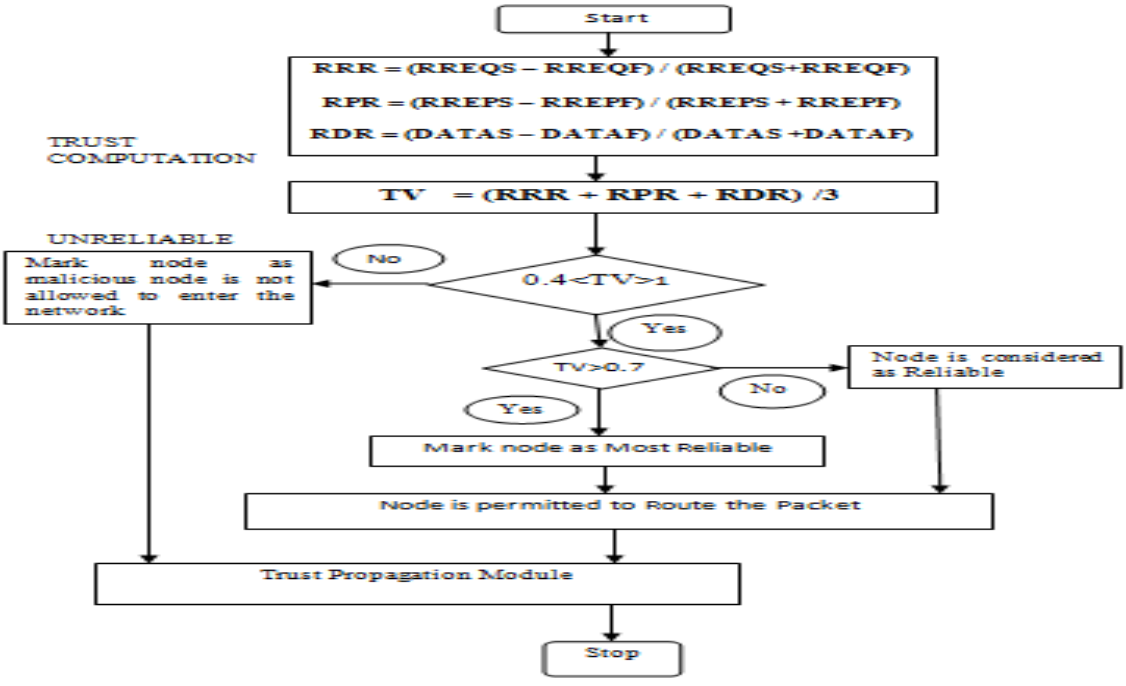


Figure: 3.1 Flow Chart of Proposed Method

 DOI : 10.35291/2454-9150.2019.0358

3.3 Prove Proposed Secure Based Method using Mathematical Calculation

For the specimen arrange appeared in figure 4.2, the way chose is S->E->F->D. For instance, Node F has seven neighbors and for this node the secure esteem figuring is to be finished.

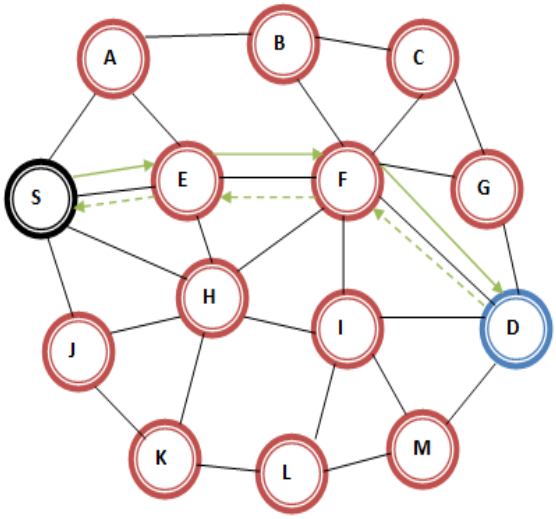


Figure 3.2 Sample Network to Implement MTAODV

For node E the secure esteem estimation table is given in table 2 which contains the accomplishment and disappointment rate of course demand, answer and information.

Table 3.3 Secure value calculation for Node E

	COMMUNICATION TYPE	RREQ	RREP	DATA IN MAX QUEUE SIZE(1000)
R				
R	SUCCESS	10	10	950
R	FAILURE	0	0	50

= (7 - 0) / (7 +0) = 1
RPR = (7 - 0) / (7 +0) = 1
RDR = (950-50) / (950+50) = 0.9

The estimations of RRR, RPR and RDR are falling inside the standardized range settled - 1 to +1. In this manner the secure esteem is ascertained for the node F.

Television = (1 +1 +0.9) / 3 = 0.96 (which is more than 0.6) in this manner making this node a most solid node for directing, this secure estimation is accomplished for all nodes in the steering way to screen nodes conduct. On the off chance that the disappointment rate builds it consequently influences the RRR, RPR and RDR esteems in this manner making them drop past the standardized principles along these lines resulting in secure esteem not as much as the edge.

Table 3.4: Simulation Parameters

Parameters	value
Simulation	ns 2.35
Routing protocol	AODV, BAODV , MTAODV
Scenario size	1000*1000 m^2
No. of nodes	20, 40, 60, 80, 100
Misbehaving nodes	0-40%
Simulation time	240s
Traffic type	CBR / UDP
Pause time	5s
Mobility	4-20 m /s

 DOI : 10.35291/2454-9150.2019.0358

IV. IMPLEMENTATION AND RESULT

4.1 Result Analysis Scenario: - Black Hole Attacks

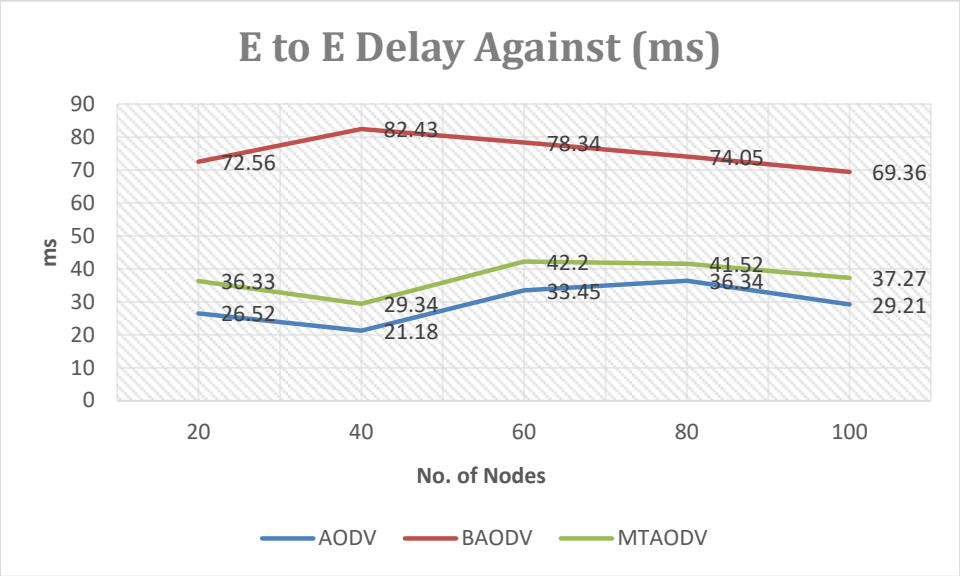
1. End to End Delay: End to End delay of MTAODV is better than Black Hole attack AODV (BAODV). This delay is average delay of data sent to destination. We have shown the result on 20, 30 and 40 number of nodes and used AODV, BAODV and MTAODV for comparison, we found that MTAODV is far better than BAODV.

E to E Delay = (Arrive time - Send time) / Number of Send Messages

EED = Total EED / No. of Packets Sent

Table 4.1 End to End Delay Against AODV, BAODV and MTAODV

E to E Delay Against (ms)			
No. of Nodes	**AODV**	**BAODV**	**MTAODV**
20	**26.52**	**72.56**	36.33
40	**21.18**	**82.43**	29.34
60	**33.45**	**78.34**	42.2
80	**36.34**	**74.05**	41.52
100	**29.21**	**69.36**	37.27



Graph 4.1 End To End Delay for Scenario of Black Hole Attacks

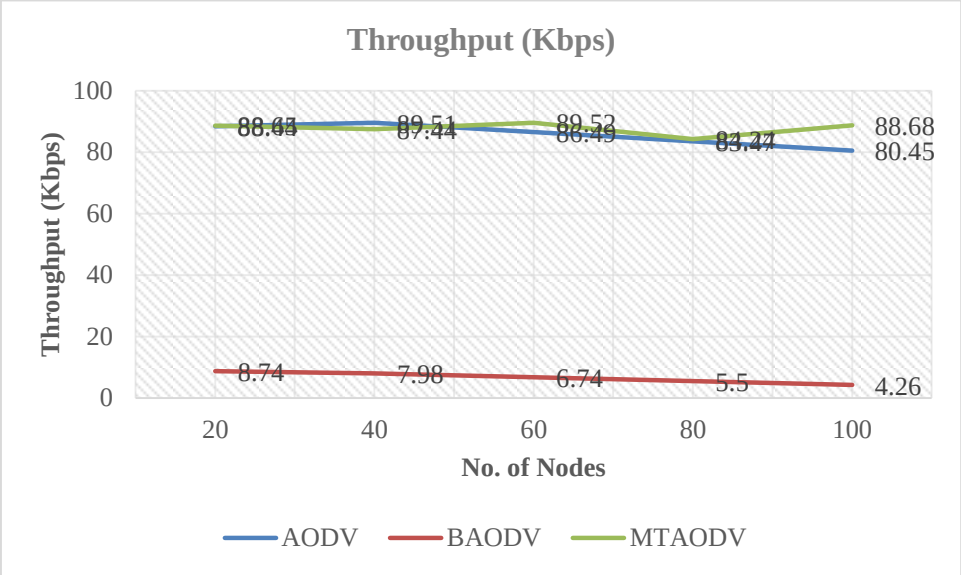
2. Throughputs: Throughput of MTAODV is better than Black Hole attack AODV (BAODV). So the performances of our network rise than other in case of MTAODV.

Throughput = (No. of Packets ∗ Packet Size) / Total Time

Table 4.2 Throughput against AODV, BAODV and MTAODV

Throughput (Kbps)			
No. of Nodes	**AODV**	**BAODV**	**MTAODV**
20	**88.44**	**8.74**	88.65
40	**89.51**	**7.98**	87.44
60	**86.49**	**6.74**	89.52
80	**83.47**	**5.5**	84.24
100	**80.45**	**4.26**	88.68

 DOI : 10.35291/2454-9150.2019.0358



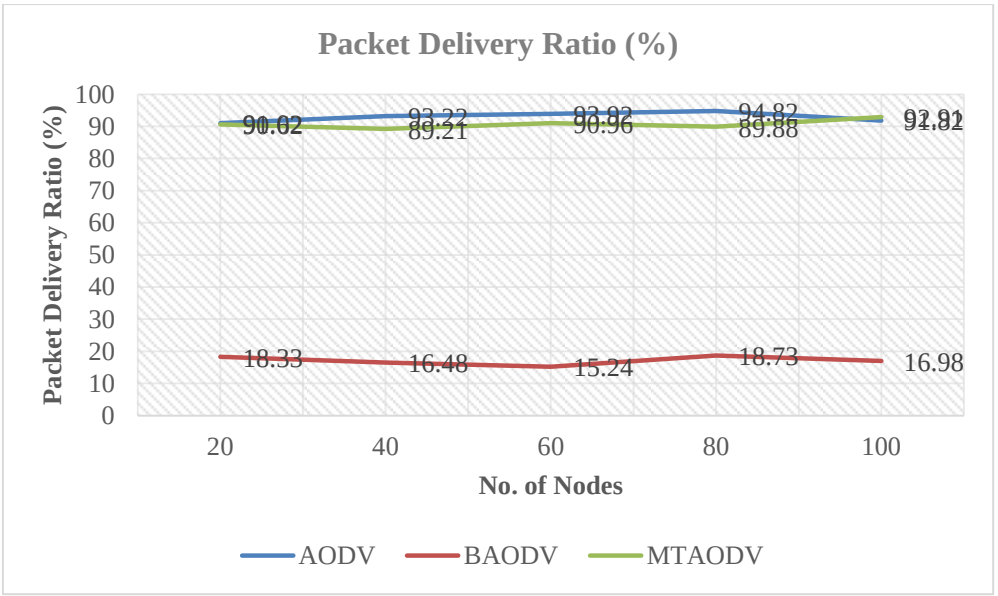
Graph 4.2 Throughputs for Scenario of Black Hole Attacks

3. Packet Delivery Ratio: Packet Delivery Ratio: PDR of MTAODV is better as compared to Black Hole attack AODV. It is a ratio of number of packet received to the no of packet send. We have compared the result of our method with AODV and BAODV on different no of nodes. Finally we found that our method is far better than BAODV and also compared with AODV.

PDR = No of Packet Received / No of Send Packets

Table 4.3 Packet Delivery Ratio against AODV, BAODV and MTAODV

Packet Delivery Ratio (%)			
No. of Nodes	**AODV**	**BAODV**	**MTAODV**
20	**91.02**	**18.33**	90.62
40	**93.22**	**16.48**	89.21
60	**93.92**	**15.24**	90.96
80	**94.82**	**18.73**	89.88
100	**91.82**	**16.98**	92.91



Graph 4.3 Packet Delivery Ratios for Scenario of Black Hole Attacks

 DOI : 10.35291/2454-9150.2019.0358

4. Energy (%): Energy of AODV is better than Black hole attack AODV (BAODV) and MTAODV. Show table 5.4 and graph 5.5 Energy against AODV, BAODV and MTAODV.

Table 4.4 Energy against AODV, BAODV and MTAODV

No. of Nodes	AODV	BAODV	MTAODV
20	98.45	62.85	96.66
40	96.85	58.76	92.34
60	97.43	54.83	94.22
80	92.85	42.85	90.75
100	89.67	39.73	94.45

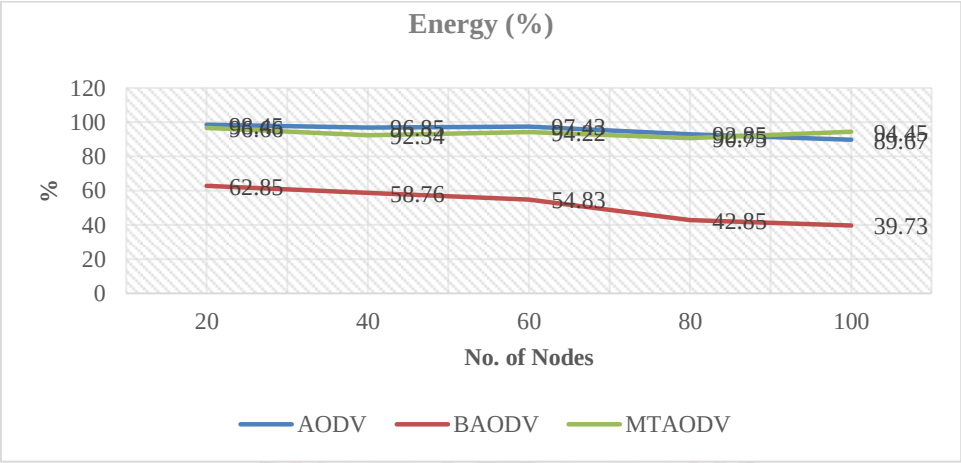
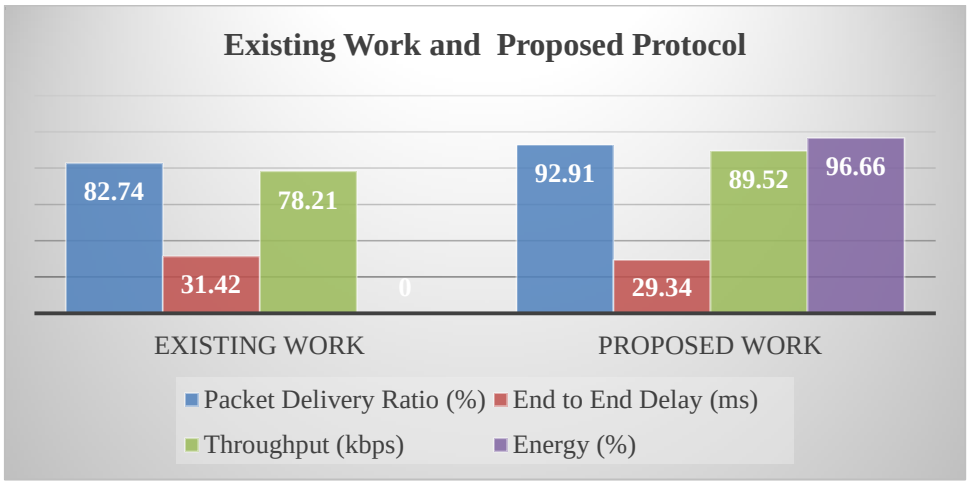


Figure 4.4 Energy against AODV, BAODV and MTAODV

4.2. Comparison between Existing and Proposed Protocol

Table 4.5 Comparisons between Existing and Proposed Protocol

	Existing Work	Proposed Work
Network Parameters	MTAODV	MTAODV
Packet Delivery Ratio (%)	92.8571	92.91
End to End Delay (ms)	1.54601	29.34
Throughput (kbps)	142.629	89.52
Energy (%)	NA	96.66



Graph 4.5 Comparisons between Existing and Proposed Protocol

 DOI : 10.35291/2454-9150.2019.0358

V. CONCLUSION

The detection and prevention of black hole attack in the network exists as a challenging task. In this work analyzed the effect of black hole attack in the performance of AODV protocol and prevent the black hole from the network using MTAODV protocol. Analyzing the results of PDR shows the Packet Delivery Ratio of Normal AODV, AODV under black hole attack, MTAODV under black hole attack; we found that there is 10-12% increase in PDR for MTAODV. This clearly shows that there is a significant benefit when the solution against Black hole attacks is applied. results of Throughput shows the Throughput of MTAODV under black hole attack, is significant rise of 8-12% in MTAODV against normal AODV under Black-Hole Attack. the results of End-to-End Delay has 20-22% decreased for Secure AODV compared to normal AODV. Remaining amount of energy has been increased 5-7% .

REFERENCES

[1] Shweta Shah, Madhu Sharma and Ashish Jain, " wormhole attacks in Mobile Ad-hoc Networks", IEEE International Symposium on Collasal Data Analysis and Networking, March 2018.

[2] Drake Xavier Dzurovcak ; Shuhui Yang , "Performance Analysis of Routing Protocols in Delay Tolerant Networks" , IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) , 2017, pp.1-7.

[3] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang and Arjun Agrawal " Detection and Removal of cooperative blackhole & grayhole attacks in MANET" International Conference on System Engineering and Technology, 2012.

[4] Sakshi Jain and Dr. Ajay Khuteta "Detecting and Overcoming Black-hole Attack in Mobile Ad-hoc Network", IEEE International Conference On Green Computing and Internet of Things, pp. 225-229, ISSN: 978-1-4673-7910, Jan. 2015.

[5] S.R. Deshmukh, P.N. Chatur and N.B. Bhople "AODV-Based Secure Routing Against Black-hole Attack in MANET", IEEE International Conference On Recent Trends in Electronics, Information & Technology, pp. 1960-1964, ISSN:978-1-5090-0774, May 2016.

[6] Vidya Kumar Saurabh**,** Roopesh Sharma and Ravikant Itare "Cluster-based Technique for detection and prevention of Black-hole Attack in MANET"IEEE International conference of Electronics, communication and Aerospace Technology(ICECA) April 2017.

[7] Vinay Rishiwal, Sandeep Kumar Agarwal and Mano Yadav "Performance of AODV Protocol for H-MANET" IEEE International Conference on Advances in Computing, Communication and Automation(ICACCA)" Sep. 2016.

[9] Prasad P Rajendra and Shivshankar "Multitier energy system on secure intrusion detection system in MANET" IEEE International Conference on Recent Trends in Electronics, information & Communication Technology(RTEICT)" May 2017.

[9] Lakshit Prashar and Raj Kamal Kapur "Performance Analysis of Routing Protocol under Different Types of Attacks in MANETs" IEEE International Conference on Reliability Infocom Technologies and Optimization (ICRITO)" December 2016.

[10] Gurveen Vaseer, Garima Ghai and Dhruva Ghai "Distributed Trust-Based Multiple Attack Prevention for secure MANETs" IEEE International Conference on Smart Electronic System(SES)" Dec. 2018.

[11] Ankit D Patel and Kartik Chawda " Black hole and grayhole attacks in MANET", IEEE International Conference on Information Communication and Embedded System(ICICES), Feb. 2014.

 DOI : 10.35291/2454-9150.2019.0358