International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Confidence-based Security System for Routing Protocol in Mobile Ad-hoc Networks

S. J. Patil, L. S. Admuthe, M. R. Patil

Abstract*: A mobile ad-hoc network (MANET) is an infrastructure-less network of wireless nodes. The network topology may change quickly with respect to time, due to node mobility. The network is a disintegrated network, activities such as delivering messages by determining the topology essential to be implemented by the nodes themselves i.e., the routing activity will be unified into mobile nodes. Due to the lack of centralized administration in multihop routing and open environment, MANET's are susceptible to attacks by compromised nodes; hence, to provide security also energy efficiency is a crucial issue. So as to decrease the hazards of malicious nodes and resolve energy consumption issues, a simple confidence-based protocol is built to evaluate neighbor's behaviour using forwarding factors. The reactive Ad-hoc on-demand multipath distance vector routing protocol (AOMDV), is extended and confidence-based Ad-hoc on-demand distance vector (CBAOMDV) protocol, is implemented for MANET. This implemented protocol is able to find multiple routes in one route discovery. These routes are calculated by confidence values and hop counts. From there, the shortest path is selected which fulfills the requirements of data packets for reliability on confidence. Several experimentations have been directed to relate AOMDV and CBAOMDV protocols and the outcomes show that CBAOMDV advances throughput, packet delivery ratio, normalized routing load, and average energy consumption.

Keywords: AOMDV, CBAOMDV, MANETs, Security.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is normally defined as a network that has many autonomous nodes, often composed of mobile devices or other mobile pieces, that can arrange themselves in several ways and operate without firm top-down network administration. Nodes out of range with each other need in-between nodes to forward their communications. Due to multi-hop routing and open working atmosphere, MANETs are susceptible to attacks by malicious nodes, such as modifying attacks and selective forwarding attacks, along with the energy efficiency issue of network. Therefore, a significant problem in a MANET is dependable packet routing. To ensure properties such as privacy, reliability, etc. using encryption and authentication tools, secure routing protocols have been established [1], [2]. However, central trusted third party required by those protocols, which is unfeasible for MANET's [3]. As in society, one person will trust another to accomplish, but the previous cannot give assurance to the latter's behavior [4]. Thus, the concept of confidence level is introduced into a computing network to measure uncertainty and about another's future behavior for a certain action. The confidence level can be derived from direct communications as well as from indirect recommendations. In centralized models, trust values are maintained through an authorized third party or a common central node. This goes counter to the nature of MANETs. While, in distributed models, trust values are assigned to every node. To evaluate trust from various facets and screen out the bad evaluations many investigators [5], [6], [7], [8] are encouraging the use of scores and prefer to intricate rating aggregation algorithms. Pirzada and McDonald [9] proposed the aggregation mechanism, where nodes calculate trust according to multiple observed events. A number of trust models [10], [11], [12], [13] based on sharing recommendation information have been developed to establish reputation peer-to-peer systems. The nodes in a MANET usually have restricted resources, like bandwidth and energy; hence reactive routing protocols attract more interests of researchers. To formulate a loop-free and single path routing protocol, AODV [14] combines the use of destination sequence numbers in DSDV [15] with the on-demand route detection technique in DSR [16]. AOMDV [17] is proposed to discover link-disjoint and multiple loop-free paths. Experiments show remarkable improvement in the end-to-end delay in AOMDV. Pirzada et al. [18] assessed the performance of trust-based reactive routing protocols (trusted AODV, DSR, and TORA) by changing the number of malicious nodes. The outcomes show that each trusted routing protocol has the individual significance that makes it appropriate for application in a particular atmosphere. Especially at higher traffic loads AODV protocol sustains a stable throughput and outperforms on DSR and TORA. Therefore, the present work is focused on the confidence-based model to evaluate neighbor's behaviors. The packet forwarding factor was used to evaluate neighbours behaviors. There are two main inspirations related to confidence level organization in MANETs. At first, confidence assessment helps to differentiate between good and malevolent nodes. One node can remember other nodes' behaviors by creating a confidence history. Good entities avoid working with suspect ones by using this data. Secondly, confidence level management proposes an estimation of one's forthcoming behavior and improves network performance.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
S. J. Patil*, Department of Electronics Engineering, DKTE'S Textile & Engineering Institute, Ichalkaranji. Maharashtra, India.
L. S. Admuthe, Department of Electronics Engineering, DKTE'S Textile & Engineering Institute, Ichalkaranji. Maharashtra, India.
M. R. Patil, J.A.G.M. Institute of Technology, Jamkhandhi, Karnataka, India.

In this protocol, a node confidence level was denoted as a weighted summation of the forwarding factor of data packets and control packets. An average of node confidence was also computed as path confidence. Hence innovative routing protocol is put forwarded for MANETs, named as Confidence based Ad-hoc on-demand multipath distance vector(CBAOMDV). In this work, a communicator node can find many paths to a destination node in finding one route. An estimation vector made of hop count and confidence cost of every path. An end node will reply with the shortest tracks as nodes that satisfy the confidence necessities of data packets. Using the hop count, the shortest path will be carefully chosen as the forwarding path. Also, the energy module is included in the network, as the energy of the wireless node is a vital issue. Here the performance of AOMDV and CBAOMDV is compared. The experiment results presented in section V show that CBAOMDV improves packet delivery ratio, throughput, normalized routing load and most important average energy consumption.

II. CONFIDENCE BASED AND ENERGY-EFFICIENT PROTOCOL

A node can evaluate confidence level of neighbors by keep watching their behavior by keeping itself in promiscuous mode. It permits us to interpret all packets in the system that are related to that node.Energy consumption is a key factor while communication in Ad-Hoc network. Increased energy consumption may lead to a loss of communication link due to battery exhaust. Hence, initiation of new route discovery is necessary once again which may ultimately increase the control overheads. Therefore, an energy-efficient module is the need of today. It is assumed that all neighbors will obtain the packet appropriately which is broadcasted by one node. On the other hand, in case source and destination are away more than one hop, packets might be dropped by the middle nodes due to unpredicted grounds or malicious attacks. Confidence evaluation in a routing process is an assessment of forwarding behaviors of neighbors by a source. It is not considered as correct forwarding when a malicious node forwards a data packet later modifying data. If the correspondent node detects this unlawful change, the forwarding factor of the neighbor will decline.

A. Forwarding Factor

The number of packets forwarded appropriately to the number of packets to be forwarded is called forwarding factor.

$$FF(t) = \frac{Xc(t)}{Xa(t)} \quad (1)$$

Where Xc(t)- Count of correct forwarding
Xa(t)- Total count of all requesting before time t.

B. Node Confidence Level

In MANETs, Data packets caries main information and control packets are used for route update, route request, route reply, and route maintenance. The establishment of correct paths relies on the accurateness of control packets. Hence, FF(t) is separated into two fragments: control packet forwarding factor (CPF), and data packet forwarding factor (DPF). These are calculated using weighted summation of data and control packets as shown in formula 2. Confidence factors CPF(t) and DPF(t) are allotted weights so as to estimate the overall confidence cost of a node. The direct confidence in node i by node j is presented as Cij as shown below

$$Cij(t) = \alpha * CPFij(t) + \beta * DPFij(t) \quad (2)$$

Where, α and β (α; β ≥ 0 α+β = 1) are weights allocated to CPF and DPF, respectively. $CPF_{ij}(t)$ and $DPF_{ij}(t)$ signify control packet forwarding factor and data packet forwarding factor detected by node i for forwarding node j at time t, respectively.

Table- I: Weights of forwarding factor

Variable	Weights
α	0.4
β	0.6

During implementation, α is considered as 0.4 and β is considered 0.6 as shown in table I, it is known that data packets are more important than control packets so more weightage is given to data packets. After an individual interface, node i determines the authenticity of node j by correct forwardness. In the above condition, the confidence value Cij rises, else it declines. In this confidence-based protocol, confidence costs are restricted in an array from 0 to 1(i.e. 0 ≤ Cij ≤ 1). The confidence cost of 0 indicates complete disbelief whereas cost 1 gives complete trust. The confidence levels of nodes have been listed in Table II. In a lack of interaction, confidence cost is set to 1. A threshold h, is the black-list confidence threshold, for the detection of malicious nodes. In other words, if the confidence cost of a node is less than a black-list threshold (h), the node would be considered as a malevolent node.

Table- II: Confidence levels

Sr. No.	Confidence Level	Node type
1	[0. 0.45]	Malicious
2	[0.45, 0.8]	Suspicious
3	[0.8, 0.9]	Less confident
4	[0.9, 1]	Confident

C. Path Confidence

In this model, the confidence cost of a path P is equivalent to the average of the confidence cost of nodes along the path P, i.e.

$$Cp(t) = \frac{Cij(t)}{n} \; (Cij(t) \mid ni, nj \; \varepsilon \; P \; and \; ni \rightarrow nj) \quad (3)$$

Where ni and nj- Any two next nodes among the path P
ni→nj- nj is the next-hop node of ni
n -total number of nodes.

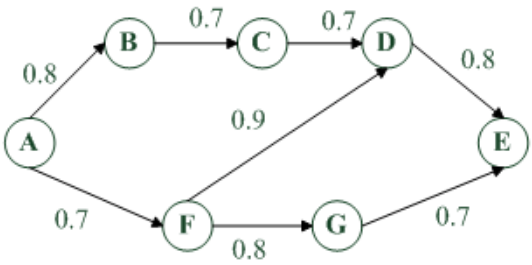

Fig. 1. Path Confidence Calculation

As shown in fig. 1 source node A finds two shortest paths to destination node E (A→F→G→E) and (A→F→D→E). The first path confidence level is 0.7, and the second path confidence is 0.8. If confidence requirements of the packet to be transmitted are 0.7, it will choose the second path, if the confidence level requirements of the packet to be transmitted are less than 0.7 the two paths will meet safety requirements. The source node can select both paths to send the data. More specifically it will select the shortest path to the destination.

III. CONFIDENCE BASED ON-DEMAND MULTIPATH ROUTING PROTOCOL

In this section the details of confidence level record list and entries in the routing table are discussed.

A. Confidence level record list

An information record list is introduced to store the confidence level. Each node maintains a confidence level record for every neighbor node to which packets have corresponded for forwarding. A confidence record exhibited in Table III. To record recent packets sent packet buffer issued. The oldest packet will be removed if it is not removed in time by using the rounded buffer.

Table- III: Confidence record structure

Node ID
Node Confidence
Xc and Xa for control packets
Xc and Xa for data packets
Packets Buffer

B. Entries in Routing Table

The routes to other neighbor nodes are stored in a routing table. An Ad-hoc network routing table consists of numerous routing entries maintained by each node. When a data packet is going to the end node, it denotes to the local routing table to discover the next hop. Once it reaches node X, it refers to node X's routing table for the next hop to the destination. This progression will repeat until it finds the destination. Only recent node interaction records will be maintained by the node due to the dynamic topology of a MANET. Table IV shows the structure of routing table entries for CBAOMDV.

Table-IV: Structure of routing table for CBAOMDV

Destination ID
Destination Sequence Number
(NextHop1, HopCount1, PathConfidenceValue1, Timeout1), (NextHop2, HopCount2, PathConfidenceValue2, Timeout2),

Several routes to the identical destination are set in ascending order of hop count. If two paths have the same hop count, the one with greater path confidence is preferred.

IV. PERFORMANCE EVALUATION

A. Simulation model and Parameters

To estimate the performance of the proposed CBAOMDV routing protocol the NS-2.35allinone simulator is used. In NS-2, the constant bit rate (CBR)produces the data in the network, and the User Datagram Protocol (UDP)constitutes the transport layer. Two Ray Ground model is suitable for long-distance communication, was used as a propagation model in the protocol. As shown in Table V the simulation model consists of 50 to 150 number of nodes within the square network area of 1000m x 1000m to transmit data packets of 512 bytes. The node communication range is about 250m, and it is capable of communicating directly with others within that range. The performance of the CBAOMDV is compared and evaluated with the existing AOMDV protocol. The simulation time considered was 100s. To get better results in various attributes like a number of node variation, node speed variation and number of malicious nodes are considered. The simulation parameters are summarized as follows:

Table-V: Parameters considered

Simulator	NS-2.35allinone
Area considered	1000 X 1000
Nodes variation	50, 75, 100, 125, 150.
Speed of the nodes	0, 5, 10, 15, 20, 25, 30m/s.
Malicious nodes	1, 2, 3, 4, 5
Traffic load	CBR
Transport layer protocol	UDP
MAC protocol	IEEE802.11
Simulation time	100s.

B. Assessment parameters

- Packet delivery ratio It is the ratio of data packets delivered to the destination nodes to those sent by the source nodes.
- Throughput
  It is the average rate of successful message delivery on a communication channel.
- Average Energy Consumed
  The average energy consumed in the network is the average energy consumed by all nodes.
- Normalized Routing Load
  It is the ratio of the number of control packets transmitted per data packet at the destination.
- Packets Dropped
  It is the total number of packets dropped in the network.

V. RESULTS AND DISCUSSION

In the present study, various performance matrices are analyzed for AOMDV, CBAOMDV and emphasized in graphical representations. Performance matrices like Packet delivery ratio, Number of packets dropped, Throughput, Normalized routing load, and Average energy consumption is considered. These performance matrices also correspond with various attributes like a number of node variation, node speed variation and number of malicious nodes as shown in table VI.

Table- VI: Performance matrices with various attributes variation

Parameters	**Nodes**	**Speed**	**Pause time**	**Malicious Nodes**
No. of nodes	50 to 150	4 m/s	25 s	Random
Node Speed	50	0 to 30 m/s	25 s	Random
No. of Malicious node	100	4 m/s	25 s	1,2,3,4,5

A. Varying Number of Nodes:

In this attribute, a number of nodes are varied between 50 to 150 with node speed 4m/s, pause time 25s, an area considered 1000x1000 m and simulation time 100s.Packet delivery ratio (PDR) has been evaluated by corresponding

node variation with a step size of 25 nodes which is presented in fig. 2. Results show that PDR was more in CBAOMDV as compared to AOMDV in every variation with respect to a number of nodes. PDR with reference to CBAOMDV was observed increasing up to 75 numbers of nodes. It gives the best result at 75 nodes and starts declining as the number of nodes was increased. However, it was observed far better than that of AOMDV.The results of throughput are shown in fig. 3 and it clearly indicated that the throughput of CBAOMDV was much better than AOMDV. However, along with an increase in the number of nodes, there was a reduction in throughput.

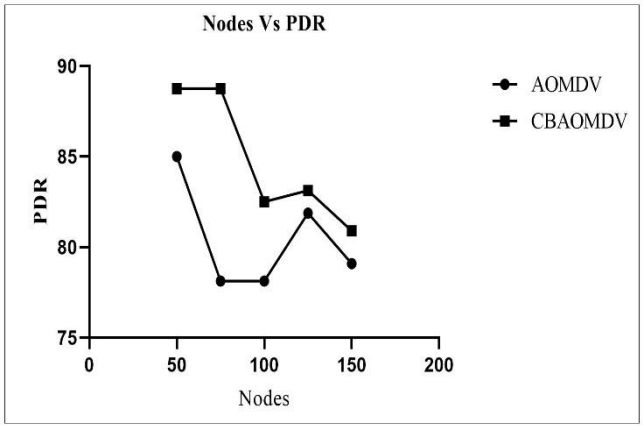

Fig. 2. Comparison of packet delivery ratio

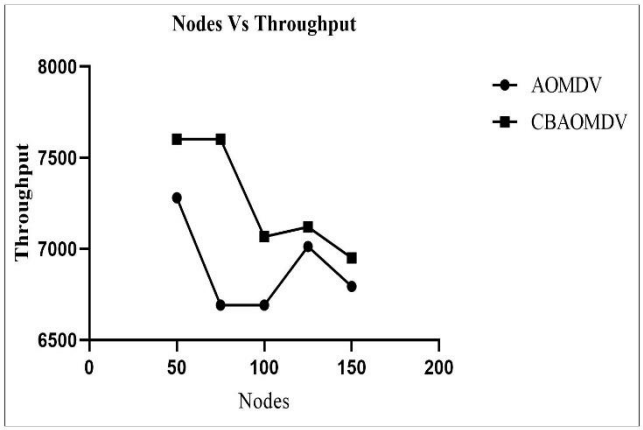

Fig. 3. Comparison of throughput

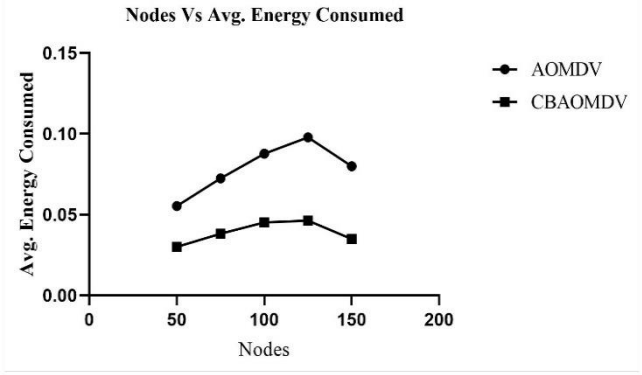

Fig. 4. Comparison of the average energy consumed

Energy consumption is a key factor while communication in Ad-Hoc network. Therefore, the energy-efficient module is the need of time. Here, in fig. 4 energy consumption of two protocols has been compared with reference to a number of nodes. The results revealed that AOMDV consumes more energy than that of CBAOMDV. Against the increase in the number of nodes, energy consumption was nearly constant.

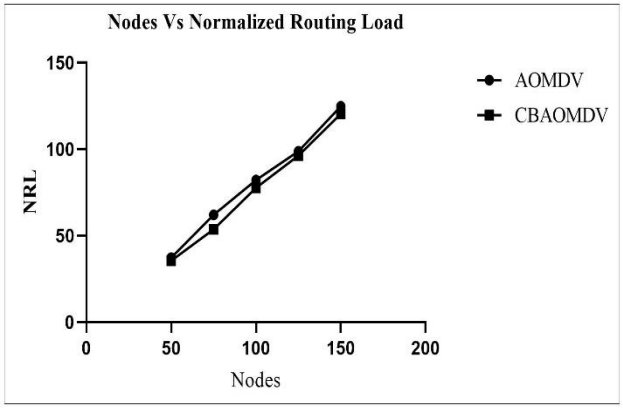

Fig. 5. Comparison of normalized routing load

Fig. 5 compares the normalized routing load and from this it can be concluded that normalized routing load was less than the AOMDV, and it increases with an increase in the a number of nodes.

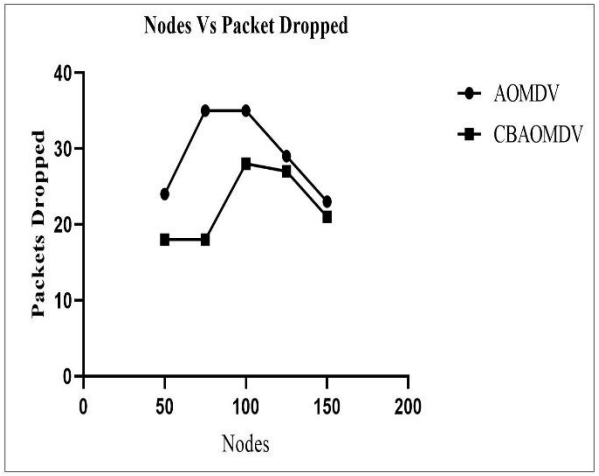

Fig. 6. Comparison of packet dropped.

The total number of packets dropped against a number of nodes is shown in fig. 6. It designates the total number of packets dropped in CBAOMDV was noted minimum while in AOMDV it was maximum.

B. Varying Nodes Speed:

In this set of simulations, the mobility speed of the nodes is varied. The nodes start with a low velocity of 0 m/s and then the node velocity increases up to 30 m/s with a step size of 5m/s. The data rate is kept constant and the pause time and the number of nodes were fixed at the 20s and 50 respectively.The packet delivery ratio has been evaluated by corresponding node speed variation which is presented in fig. 7. Results depicted that PDR was more in CBAOMDV as compared to AOMDV in every variation with respect to node speed. PDR with reference to CBAOMDV was observed less at speed 15m/s.

Retrieval Number: A1344109119/2019©BEIESP
DOI: 10.35940/ijeat.A1344.129219
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

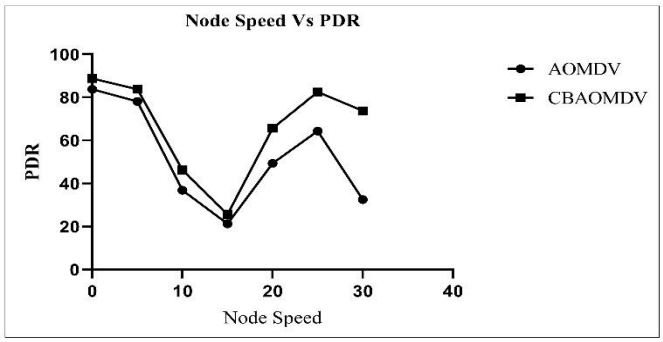

Fig. 7. Comparison of packet delivery ratio

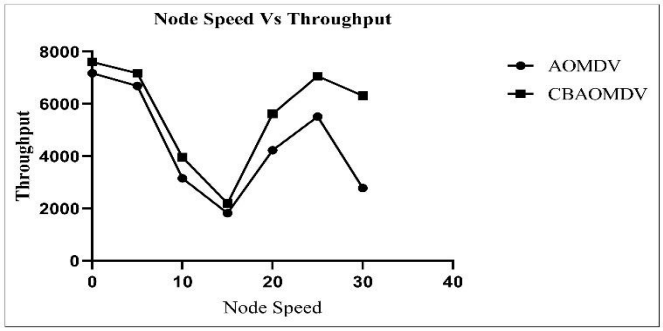

Fig. 8. Comparison of throughput

Fig. 8 shows CBAOMDV has higher throughput than AOMDV for slower nodes speed. Throughput for CBAOMDV and AOMDV decreases at node speed 15m/s and again starts increasing with the increase in node speed.

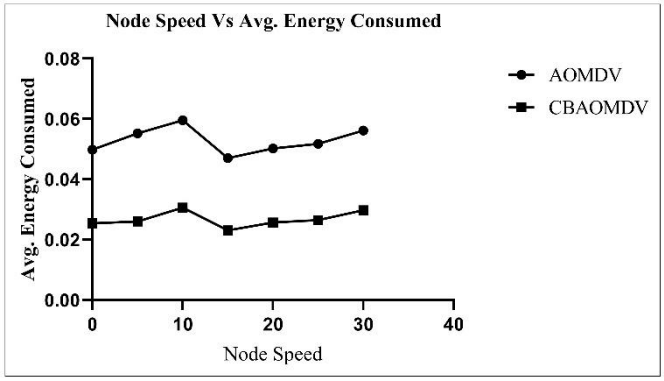

Fig. 9. Comparison of average energy consumed

As shown in fig. 9, energy consumed by CBAOMDV the protocol is less as compared to AOMDV. It is clearly indicating that CBAOMDV protocol is energy efficient than the AOMDV.

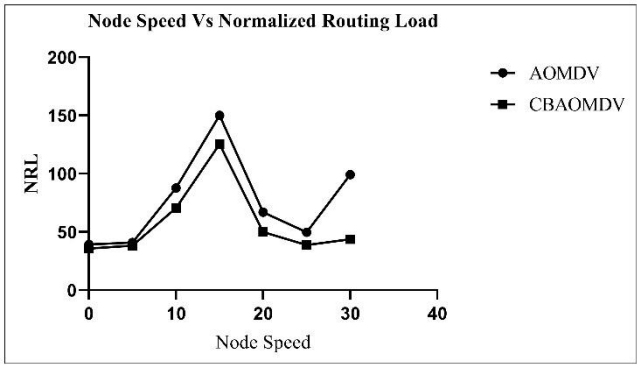

Fig. 10. Comparison of normalized routing load.

It is clear that NRL in case of CBAOMDV protocol was less than the base protocol AOMDV with an increase in the node speed as shown in fig. 10).

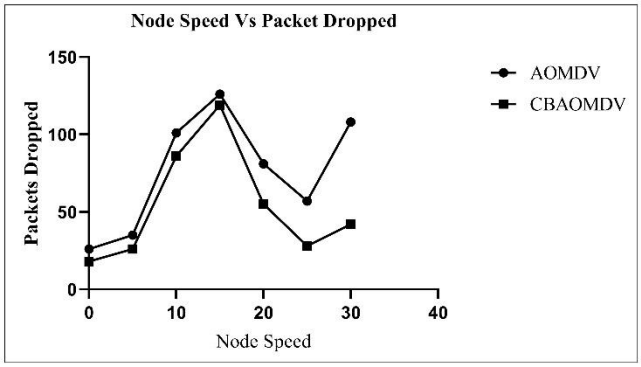

Fig. 11. Comparison of the packet dropped

Packet dropped is nothing but loss of packets in the networks. It was observed that at node speed 15m/s number of packets dropped for both the protocol was increased significantly. Fig.11 shows that the number of packets dropped in CBAOMDV protocol is less as compared with AOMDV.

C. Varying Malicious Nodes:

The following results are discussed by varying malicious nodes from 1 to 5. In this scenario, a total number of malicious nodes in the network were inserted purposefully to observe its effect on different parameters like PDR, throughput, NRL and average energy consumption, etc.

Fig. 12 clearly depicts that the packet delivery ratio of CBAOMDV is better than AOMDV.

In fig. 13 two protocols have compared with reference to malicious nodes and throughput, obviously, the throughput of CBAOMDV protocol was noted improved as compared with basic protocol AOMDV. The number of malicious nodes in the network increased, throughput starts decreasing.

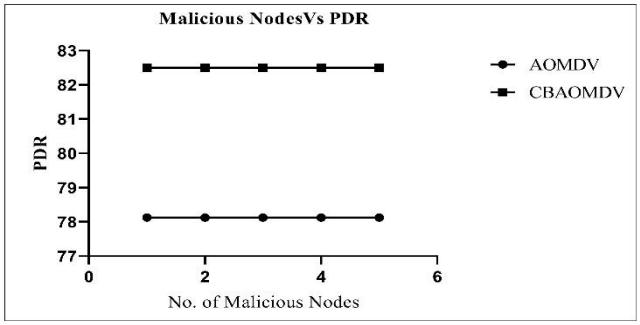

Fig. 12. Comparison of packet delivery ratio

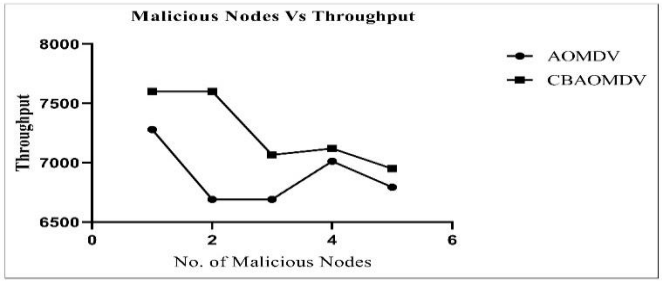

Fig. 13. Comparison of throughput

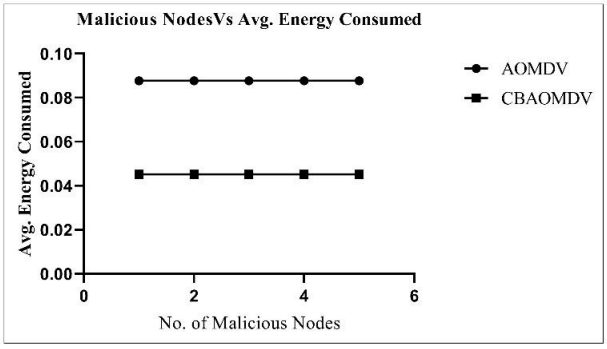

Fig. 14. Comparison of average energy consumed

Along with the increase in the malicious nodes in the network, there was no significant change observed in the energy consumption. Energy consumed by CBAOMDV protocol is less as compared with AOMDV which is as shown in fig. 14.

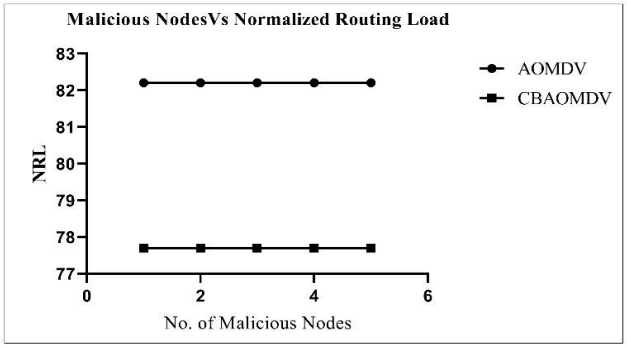

Fig. 15. Comparison of normalized routing load

As shown in fig. 15, normalized routing load in the case of CBAOMDV is observed low as compared with base protocol, with an increase in a malicious node in the network.

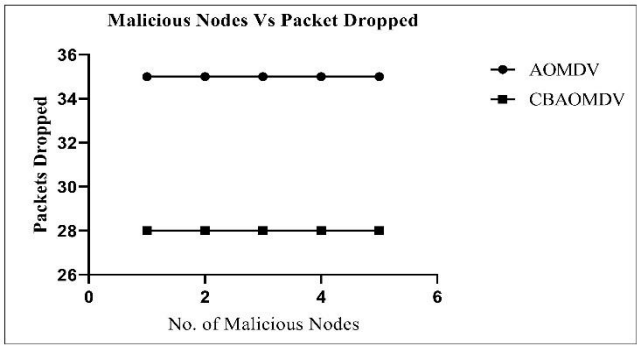

Fig. 16. Comparison of packet dropped

There was no significant change noted in the number of packets dropped in-network with an increase in the malicious node. Fig. 16 indicates that a result of the CBAOMDV protocol was better than the AOMDV protocol.

VI. CONCLUSION

The present work can be concluded that the implemented work provides a confidence based on-demand multipath routing protocol. It finds multidimensional confidence pats to the destination and also the shortest path is selected. In the present study path forwarding factor, node confidence level and path confidence were successfully estimated. This can be achieved by keeping confidence level record list and entries in the record list. The simulation was carried and parameters like packet delivery ratio, throughput, average energy consumption, normalized routing load and packet dropped were analyzed with varying various attributes. Furthermore, from the results of protocol, it can be concluded that the malicious nodes could be easily isolated. Moreover, this protocol is more energy efficient model than the base protocol AOMDV. Throughput, NRL and PDR are also better than that of AOMDV. Overall it can be concluded that CBAOMDV is efficient protocol over AOMDV on all the required aspects. This work can be extended by adding fuzzy based model in to protocol with mathematical modeling.

REFERENCES

1. Zapata, M.G., and Asokan, N., "Secure Ad-hoc On-Demand Distance Vector Routing", ACM Mobile Computing and Communications Review, 3, (6), pp.106-107, 2002.
2. Hu, Y.C., Perrig, A., and Johnson, D.B., "Ariadne: A Secure On Demand Routing Protocol for Ad-hoc Networks", in Proc. Int. Conf. Mobile Computing and Networking (Mobicom02), Atlanta, Georgia, pp.12-23, 2002.
3. Griffiths, N., Jhumka, A., Dawson, A., and Myers, R., "A Simple Trust Model for On-Demand Routing in Mobile Ad-hoc Networks", in Proc. Int. Symp. on Intelligent Distributed Computing (IDC 2008), pp. 105-114, 2008.
4. Gambetta D, "Can we trust trust?", in Gambetta, D. (Ed.): Trust: Making and Breaking Cooperative Relations (Oxford Press, 1st edn.), pp. 213-237, 2000.
5. Buchegger, S., and Boudec J. L., "A robust reputation system p2pand mobile ad-hoc networks", in Proc. Int. Workshop on the Economics of Peer-to-Peer Systems, Cambridge MA, U.S.A., 2004.
6. Josang, A., and Ismail, R., "The beta reputation system", in Proc. of the 15th Bled Electronic Commerce Conference, Bled, Slovenia, pp. 1-14, June 2002.
7. Sabater, J., and Sierra, C., "Regret: Reputation in gregarious societies", in Proc. Int. Conf. Autonomous Agents, Montreal, Canada, pp. 194-19, 2002.
8. Srivatsa, M., and Liu, L., "Securing decentralized reputation management using trustguard", Journal of Parallel and Distributed Computing, 66, (9), pp. 1217-1232. 2002.
9. Pirzada, A.A., and McDonald, C., "Trust establishment in pure ad-hoc networks", Wireless Personal Communications, 37, (1), pp.139-168, 2006.
10. X. Li Z. Jia P. Zhang R. Zhang H. Wang., "Trust-based security for Ad-Hoc network", IET Information Security, Vol. 4, Iss. 4, pp.212-232, 2010.
11. Selcuk, A.A., Uzun, E., and Pariente, M.R., "A reputation-based trust management system for P2P networks", in Proc. Int. Symposium on Cluster Computing and the Grid, pp. 251-258, 2004.
12. Xiong, L., and Liu, L., "Peer Trust: Supporting reputation-based trust in peer-to-peer communities", IEEE Trans. on Knowledge and Data Engineering, 16, (7), pp. 843-857, 2004.
13. A. A. Patil, T. I. Bagban, S. J. Patil., "Trust-based on-demand multipath routing in mobile Ad-hoc networks", International Journal of Engineering and Computer Science, Vol. 3, Iss. 5, pp. 6158-6164, 2014.
14. Perkins, CE., Royer, EM., and Das, S R., "Ad-hoc On-demand Distance Vector Routing", in Proc. Int. Workshop on Mobile Computing Systems and Applications (WMCSA), pp.90-100, 1999.
15. Perkins, C.E., and Bhagwat, P., "Highly Dynamic Destination Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", in Proc. Int. Conf. ACM SIGCOMM, pp.234-244, 1994.
16. Johnson, D., and Maltz, D., "Dynamic Source Routing in Ad-hoc Wireless Networks", in Tomasz, I., and Hank, K. (Ed.): Mobile Computing (Kluwer Academic Press, 1st edn.), pp. 153-181, 1996.
17. Marina, M.K., and Das, S R., "On-demand Multipath Distance Vector Routing for Ad-hoc Networks", in Proc. Int. Conf. on Network Protocols, pp.11-14, 2001.
18. Pirzada, A.A., McDonald, and C., Datta., "Performance comparison of trust-based reactive routing protocols", IEEE Trans. on Mobile Computing, 5, (6), pp. 695-710, 2006.

AUTHORS PROFILE

Mr. S. J. Patil - Completed BE degree in Electronics Engineering at DKTE'S TEI, Ichalkaranji, affiliated to Shivaji University, Kolhapur, and ME degree from same University, currently working as an Assistant Professor in the Department of Electronics, DKTE's TEI, Ichalkaranji. He has 11 years of teaching experience. He is a Ph. D. research scholar of VTU, Belgavi in the field of Wireless Networks.

Dr. Lalita S. Admuthe - (M'15) member of IEEE, Computer Society. The author has completed M.E. in 1994 and Ph.D. Degree in 2013 from Shivaji University Kolhapur, India in the subject of Electronics Engineering. The author focussed her research area specially in Neural Networks, Wireless Networks, Fuzzy Logic and Optimization Problems. Now she is working as Professor in Electronics Engineering at DKTE's Textile and Engineering Institute Ichalkaranji since 2013.

Dr. Meenakshi R. Patil -(M-07, SM-17) became member IEEE in 2007 and a senior member of IEEE in 2017. The Author has graduated from PVPIT, Budhgaon in Electronics and Communication Engineering. She has received Master's degree in Electronics Engineering from WCE Sangli. In 2011 author has received Ph.D. degree from Shivaji University Kolhapur. The core research area of Author includes digital watermarking, Digital Image processing, Communication, and network security. Currently She is Principal of JAGMIT Jamkhandi, Karnataka, India.