Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 11, November -2017

CLUSTER BASED IMPROVED ANT COLONY OPTIMIZATION ROUTING TECHNIQUES TO IMPROVE THE EFFICIENCY OF MANET

S.S.Kokila[1], Dr.C.L.Brindha Devi[2]

[1]Assistant Professor, Department of Computer Applications
Vellalar College for Women, Erode
[2]Assistant Professor, Department of Computer Science
Queen Mary's College, Chennai

Abstract:- *Routing in MANET is a challenging problem due to nodes mobility, dynamic topology and lack of central point like base station. Clustering of devices in MANET could reduce overhead, flooding and collision in communication and make the network topology more stable. Clustering can be made effective in CBAR (Cluster Based Improved Ant-Colony Optimization Routing)MANETs by opting for a cluster head mechanism which ensures that control rests with a single powerful node within a cluster. This cluster head takes on the responsibility of routing the packets efficiently by coordinating with the base station. Generally route maintenance and route discovery is a very important mechanism for maintaining route life. However, due to node mobility in CBAR MANETs, frequent link breakages may lead to frequent path failures and route discoveries, which could increase the overhead of routing protocols and reduce the packet delivery ratio and increases the end-to- end delay.*

Keywords: *Routing, Cluster, Ant-colony Optimization, Throughput, MANET*

I. Introduction

Wireless networks, especially MANETs usually have a lot of is- sues to be addressed due to their intrinsic design. A major challenge is to integrate the different wireless networks and make them cooperate with each other to meet the users' expectations. Research is also underway to include multimedia services among these heterogeneous networks and to promote sharing of these services seamlessly within the wireless networks. The fast growth of wireless multimedia communication has paved the way to develop applications that are capable of providing high wireless bandwidth. Selecting suitable routing proto- cols is very essential in maintaining the link quality throughout the transmission. This helps in improving the QoS of the network. The aim of network routing is to minimize ma maximum edge congestion and maximum path length. Basically there are two different approaches in broadcasting techniques namely static and dynamic, but compared with static, local broadcast algorithms based on the dynamic approach and self-pruning algorithm can achieve a optimum solution and WSNs with web server model to sharing the data with other nodes through web signals. A number of overlapped or disjoint clusters are formed in a MANET for better data transmission. In a cluster based net- work scheme we generally have three types of mobile nodes in a MANET. A competent cluster based broadcasting algorithm has been applied to take advantage of the additional coverage area which greatly tries to improve the packet delivery ratio in Proposed MANETs.

II. RELATED WORKS

This section describes the various existing trust based routing protocols and bio-inspired protocols for MANET.
Nilesh N. Dangare.et.al (2015) Mobile ad-hoc network (MANET) is used widely today. The work of MANET is totally depends on the cooperation of various nodes in the network. As we compared with the wired network, wireless network has various advantages, such as MANET doesn't require any infrastructure; it is decentralized system and dynamic in nature. Hence MANET is popular in various areas such as Military application, wireless sensor network, Public network and more. But these advantages of MANET may become disadvantages: As its openness, decentralized and dynamic nature, it is highly prone to various attacks. That's why security is the challenging job in MANET. Various existing system for detection of attacks is in-efficient and may require more computation and space as in cryptography technique. In this paper, the focus is given on the Trust based approach to mitigate the attack. In Trust based approach, the most trusted path is selected rather than the shortest path [1].

R. Menaka.el.al (2013) Collaboration and cooperation is critical and challenging in managing trust in a distributed Mobile Ad Hoc Network (MANET). This is also critical in achieving mission and system aims like reliability, availability, scalability, or re-configurability. Defining and managing trust in a MANET requires consideration of interactions between composite social, information and communication networks and also considers resource constraints like computing power, energy, bandwidth, and dynamics. This paper discusses concepts and properties of trust and provides a survey of MANET developed trust management schemes. The accepted classifications, potential attacks, and trust metrics in MANETs are discussed [7].

Mohammed S. Obaidat.el.al (2012) Securing the routing of message in mobile ad hoc networks (MANETs) is still a challenging issue. This paper proposes an enhanced trust-based multipath Dynamic Source Routing (DSR) protocol (so-called ETBMDSR) to securely transmit messages in MANETs. The author's method consists in a combination of soft-encryption, novel trust management strategy, and multipath DSR routing. Simulation results are presented to validate our proposal, showing that our ETB-MDSR scheme outperforms a recently proposed Trust-Based Multipath DSR message scheme (TB-MDSR), in terms of route selection time [9].

Isaac Woungang.et.al (2012) Mobile ad hoc network (MANET) is a collection of mobile nodes that communicate with each other without any fixed infrastructure or a central network authority. From a security design perspective, MANETs have no clear line of defence; i.e. no built-in security. Thus, the wireless channel is accessible to both legitimate network users and malicious attackers. In this paper, a novel scheme for Detecting Black hole Attacks in MANETs (so-called DBA-DSR) is introduced. The BDA-DSR protocol detects and avoids the black hole problem before the actual routing mechanism is started by using fake RREQ packets to catch the malicious nodes. Simulation results are provided, showing that the proposed DBA-DSR scheme outperforms DSR in terms of packet delivery ratio and network throughput, chosen as performance metrics, when black hole nodes are present in the network [6].

Mehdi Keshavarz.et.al (2012) Free-riding by packet dropping is one of the most important issues for the establishment and survivability of the open multi-hop wireless networks. In this paper, we focus on the data packet dropping in a rather dense Mobile Ad-hoc network. To encounter this situation, we propose a scheme based on using MAC-layer acknowledgements to detect and punish packet dropper nodes. The author used simulation-based results to evaluate the performance of our scheme. All simulations have been performed using NS-2 [8].

R. Sudha.et.al (2011) Mobile Ad Hoc Network (MANET) is collection of multi-hop wireless mobile nodes that communicate with each other without centralized control or established infrastructure. The wireless links in this network are highly error prone and can go down frequently due to mobility of nodes, interference and less infrastructure. Therefore, routing in MANET is a critical task due to highly dynamic environment. In recent years, several routing protocols have been proposed for mobile ad hoc networks and prominent among them are DSR, AODV and TORA However, the majority of these MANET secure routing protocols did not provide a complete solution for all the MANETs' attacks and assumed that any node participating in the MANET is not selfish and that it will cooperate to support different network functionalities. Much work is going on to provide security to the network. One of the solution to the problem is ARAN –(Authenticated routing protocol) which is a secure protocol and provides Integrity, availability, Confidentiality, Authenticity, Non repudiation, Authorization &Anonymity but an authenticated selfish node can infer to this protocol performance and can disturb the network by dropping packets. This paper discusses Temporal table based schemes that can be applied to ARAN to detect selfish node and improve the performance [4].

Ramasamy Mariappan.at.al (2011) In this paper, the author presented new protocol design scenario like Re - Pro Routing Protocol (RPRP) for Broadcasting in wireless mobile Ad-hoc Network and a comparative performance for Mobile Ad hoc Networks protocols like as Ad-hoc On-Demand Distance Vector Routing protocol focusing on the effects of changes such as the increasing number of receivers or sources and increasing the number of nodes. Although some simulation results of MANET protocols have been published before, these protocols have not been compared in isolation. A systematic performance evaluation of these protocols is done by performing certain simulations and the trust methods are one of the security methods in mobile Ad-Hoc networks and these methods are prone to security risks but have found their acceptance due to efficiency over computationally expensive and time consuming cryptographic methods. The major problem with the trust methods is the period during which trust is growing and is yet to reach the requisite threshold. This paper also proposes security mechanism dependent upon Electronic Code (EC) combined with permutation functions. The proposed mechanism has low time complexity, is easier to implement, computationally inexpensive and has very high brute force search value [5].

Poonam, K. Garg.et.al (2010) Ad-hoc networks establish communication in improvised environments without requiring any fixed infrastructure. These networks are inherently prone to security attacks, with node mobility being the primary cause in allowing security breaches. Therefore secure routing is a must for such networks. A number of secure routing protocols based on trust have recently been proposed. However, all these protocols use the traditional route discovery model, where a node drops RREQ packet if its own ID is in the source route of the packet, or if it has previously processed the packet. A misbehaving node takes advantage of this vulnerability and forwards the RREQ fast, so that the RREQ received from other nodes are dropped and the path discovered includes itself (the misbehaving node). In this paper, the author presented a unique trust based method which is not vulnerable to this behaviour. In this method, each node broadcasts a RREQ packet if it is received from different neighbours. A secure and efficient route to the destination is calculated as a weighted average of the trust value of the nodes in the route, with respect to its behaviour observed by its neighbouring nodes and the number of nodes in the route. The author evaluated the misbehaving node detection rate and the efficiency of our method along a number of parameters. Results show that his method increases the throughput of the network while discovering a secure route [2].

SHEN Ming-yu.et.al (2010) This paper published by the author describes the Authentication Test Theory of strand space firstly and the theory is expended because of the demands of mobile ad hoc network routing protocol security analysis. By analyzing the existing security DSR routing protocol leaks, a new Ariadne-S protocol model is proposed based on Ariadne routing protocol. And finally it is proved that the returning routing information from the process of routing finding are secure and credible by using strand space model [3].

III. CONTRIBUTION

Proposed work CBAR focus on intrusion detection and address the following:

- Security of data packets during transmission.
- Time involved in the formation of clusters and the election of a cluster head.
- Route discovery procedures and maintenance of the discovered routes.
- Mobility of the nodes and their effect on the clusters.

Mobility based clustering

In mobility based clustering clusters are deployed in such a way by which the mobile nodes whose has low speed are gathered in same place and with the higher directional mobility gathered in different places. Therefore the mobility is a primary constrain of cluster head selection process. Thus to deploy a mobility based cluster a mobility metric is computed over a small periods of time by which difference between relative mobility of nodes are calculated. All the nodes send their mobility metrics to their neighbor. The node whose mobility is lowest is selected as a CH.

ACO Based Routing Algorithm (ARA)

ARA is a purely reactive MANET routing algorithm. It does not use any HELLO packets to explicitly find its neighbours. HELLO packets are sent by the routers to compute the time delay to send and receive datagrams to and from its neighbors. A HELLO packet also consists of clock and timestamp information. When a packet arrives at a node, the node checks it to see if routing information is available for destination *d* in its routing table. In the FANT flooding scheme, when a FANT arrives to any intermediate node, the FANT is flooded to all its neighbours. If found, it forwards the packet over that node; if not, it broadcasts a FANT to find a path to the destination. By introducing a maximum hop count on the FANT, flooding can be reduced. In the FANT forwarding scheme, when a FANT reaches an intermediate node, the node checks its routing table to see whether it has a route to the destination over any of its neighbours. If such a neighbour is found, the FANT is forwarded to only that neighbour; else, it is flooded to all its neighbours as in the flood scheme. In ARA, a route is indicated by a positive pheromone value in the node’s pheromone table over any of its neighbours to the FANT destination.

Key generation using Skein Hash function

In this work it is proposed an Improved Dynamic Digital Signature technique that is combined with the Symmetric block cyber Three Fish Cryptographic algorithm. This technique guarantees that nodes do not attack within themselves. It will also ensure a strong cryptographic authentication technique that can be utilized to safeguard the data to be transmitted. The Dynamic key generation process generates distinct dynamic keys based on the classified parameters in the network with a secret secure digital sig- nature number. This helps in producing a strong cryptographic key and ensures that the Three Fish algorithm converts the given data into an unrecognizable cryptic text that is difficult to break. The cryptographic format changes every nano second, thereby providing a safe network environment for secure data forwarding. This is made possible by the fact that this scheme uses a dynamic key which is not repeated and which is generated after every iteration of the cryptic process. The intruder can never predict the crypto- graphic format as it would be difficult for him to guess the key that would be applied to the data (Sathiyamoorthy et al 2017).

IV. FRAMEWORK OF PROPOSED ROUTING

The purpose of Clustering is to construct a scalable network with quality repairable routing path for maintenance. For scalability purpose, the network is divided into several clusters and proactive routing protocol is adopted inside the clusters and reactive routing protocol is adopted outside the clusters. When two mobile nodes communicate with each other, the connecting path between source and destination may be from one cluster or through several intermediate clusters. Therefore, the maintenance and management efforts can be distributed into
several intermediate clusters.

The Working of Clusters

Initially all the nodes in the network are in state none. Then the whole ad hoc network is clustered using a clustering algorithm for selecting Cluster Head and Gateway Nodes. After the initial cluster formation, the honey bees are generated and used for maintaining the cluster and for disseminating the information for cluster and network updates.

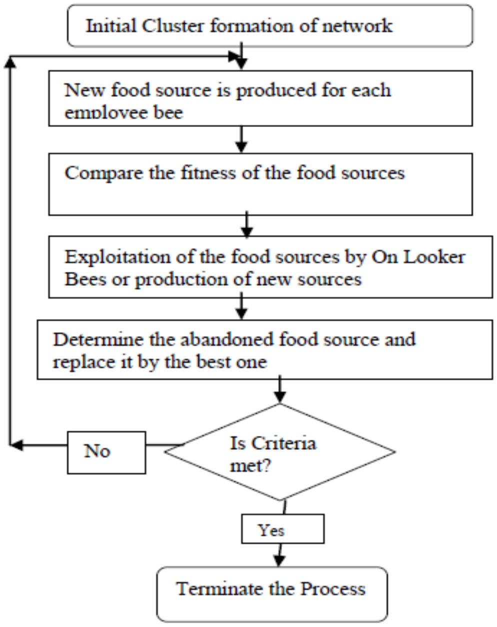
Initial Cluster formation of network
New food source is produced for each employee bee
Compare the fitness of the food sources
Exploitation of the food sources by On Looker Bees or production of new sources
Determine the abandoned food source and replace it by the best one
Is Criteria met?
No
Yes
Terminate the Process

Figure 1:Cluster based Ant Colony Optimization Techniques

V. METHODOLOGY

A clustered network is formed, when the mobile nodes start discovering each other. The discovery process can be initiated by any node at an application level program or may be initiated by end user. Application of Artificial bees is a good way for topology discovery within cluster rather than disseminating beacon packet within the entire network for updated information.

- Network formation
- Neighbor discovery
- Electing the cluster head
- Cluster member selection
- Updating the link state database
- Route discovery
- Optimal path selection
- Node authentication

Initially, the network is formed with certain number of nodes. Then, the neighbors are discovered for communicating among the nodes and the hello packets are transmitted among the nodes. If the node is the neighboring node then, the individual node IDs are updated in the neighboring table. After the discovering the neighboring nodes, the nodes with highest energy is preferred as the CH. The nodes' requirements that are similar in nature are grouped together. In order to update the link state database, the link state advertisements are broadcasted among the nodes. The information available in the link state database is the queue length, energy, and bandwidth. Then, the learning agents are used for updating the link state database based on the link state information. After updating the link state database, the routes are discovered by using the forwarding table, then the optimal path is selected and the nodes are authenticated. If there is a necessity to offload the data then, the local data are stored in the CH and based upon the requirements, the data's are grouped. If the nodes have a less receiving capacity for eg., 256 bps but, the CH has an extraordinary transmission capacity for eg.,1024 bps, then the entire data is partitioned into many 256 bps and stored in CH. In accordance with the needs of the node, the data is transmitted.

Advantages of the proposed work

The major advantages of the proposed method over the existing methods are as follows:

- It enables the data reusability and re-sharing
- Reduces the burden at both user and server side
- In this environment, the master node (i.e. CH) can store the data that are obtained from the server, then it forwards to the requested nodes in the cluster. So, it reduces the delay time and increases the speed of processing
- Moreover, it reduced the data cost and increased the data retrieval rate.

Proposed Algorithm

Cluster based message dissemination Algorithm

```
Step 1: Start
Step 2: Initiate Transmission
Step 3: If (Any Collision WHEN broadcasting)
Step 4: Stop Transmission and CALL Vigil node Step
5: Else Step
6: Note DISTINCT_ID of node‘s’
Step 7: End If
Step 8: If (node ‘ s’ broadcast → new message ‘ msg’) Then
Step 9: ‘msg’ → Forwarded
Step 10: Else
Step 11: ‘msg’ → Discarded (return)
Step 12: End If
Step 13: If (node ‘s’ receives ‘msg’ = = first time) Then
Step 14: CREATE_NEW_LIST (msg)
Step 15: Else
Step 16: UPDATE _EXISING_LIST (msg)
Step 17: End If
Step 18: DELETE added to the ‘msg’ by the Earlier broadcasting node
Step19: If (‘ msg’ IN Head of the Queue) Then
Step 20: If (No Collision Exist) Then
Step 21: msg’ → Transmitted EFFECTIVELY
Step 22: End If
Step 23: Else
Step 24: STOP forwarding until ‘msg’ at Head of the Queue;
Step 25: End If
Step 26: End
Step 27: Stop
```

Procedure for discovering efficient route to destination node

Repeat the process until packet reached to destination node

```
Step1: if (node = = Destination_node) then
Step2: Find Primary Path();
Step3: Find Secondary Path ();
Step4: else if (node = = Primary_node) then
```

```
Step5: Find Primary Path();
Step6: Find Secondary Path();
Step7: else if (node = = Secondary_node) then
Step8: Find Primary Path();
Step9: end if
Step10: until (node = = Source_node)
```

VI. PERFORMANCE ANALYSIS

In this paper the simulation are carried out based on the following NS-2 simulation setup environment

These three parameters are:
1) Number of nodes per route.
2) Node mobility speed.
3) Node transmission range.

There are numbers of performance metric by which gives the performance of CBAR .we here calculate packet delivery fraction, average end to end delay, normalized routing load and packet loss.

Gauss Markov Mobility Model:

The Gauss Markov Mobility model was originally used to suggest the group of nodes in a Personal Communication System (PCS). In this model, the level of random group of the nodes can be changed by using a tuning parameter. Each movable node is assigned a current speed and direction initially. At fixed time intervals, n, the speed and direction of each node is updated based on the (n-1)st instance using the equations –

$$d_n = \alpha d_{n-1} + (1-\alpha)\bar{d} + \sqrt{(1-\alpha^2)}\, d_{x_{n-1}}$$

$$S_n = \alpha_{Sn-1} + (1-\alpha)\bar{s} + \sqrt{(1-\alpha^2)}\, s_{x_{n-1}}$$

Where,

- s_n and d_n are the new speed and direction of the MN at time interval n;
- ∞, where $0 \le \infty \le 1$, is the tuning parameter used to vary the randomness;
- s and d are constants representing the mean value of speed and direction as

  n → ∞; and $S_{x_{n-1}}$ and $d_{x_{n-1}}$ are random variables from a Gaussian distribution

Simulation Parameters	Value
Simulation period	15M
Speed	1
Terrain range	500x500
No. of nodes	150
Node placement	Random
Radio type	Radio accumulated noise

Mobility model	Gauss Markov
Pause time	600sec
Maximum speed	35 m/sec
Packet size	512 Bytes
Routing protocol	CBAR,HE-SERIes,OAWCA
Application traffic	CBR

Table 1: Simulation Setup Properties of Proposed Work

Throughput

The throughput is the total number of packets delivered within the total amount of time. Mathematically, it is given by the following Eq. (1).

Throughput = Total Number of packets / Total amount of time….(1)

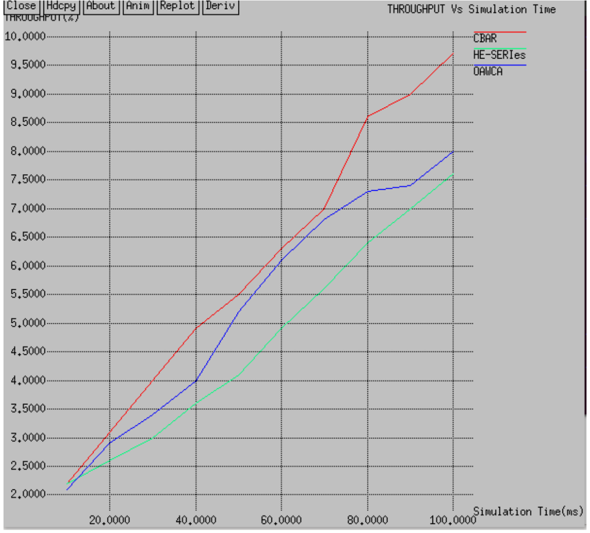

Fig 2: Throughput vs Simulation Time

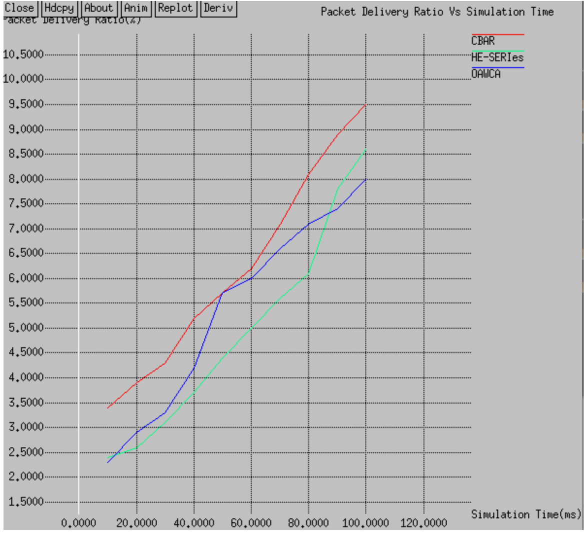

Fig 3: PDR vs Simulation Time

Packet Delivery Ratio (PDR)

PDR is the metric used for analyzing the performance of the proposed CBAR algorithm. The PDR is defined as the percentage of number of data packets received to the number of data packets transmitted. The PDR is defined by the following Eq. (2).

PDR = Sum of data packets received by the destination node / Sum of data packets generated by the source node …………(2)

End-to-end delay vs. simulation time

The comparison of end-to-end delay with respect to the number of nodes for the existing OAWCA, He-SERIeS algorithms and the proposed CBAR algorithm is represented in Fig.3 The comparison results show that the suggested algorithm provides minimal end to end delay than the existing algorithms.

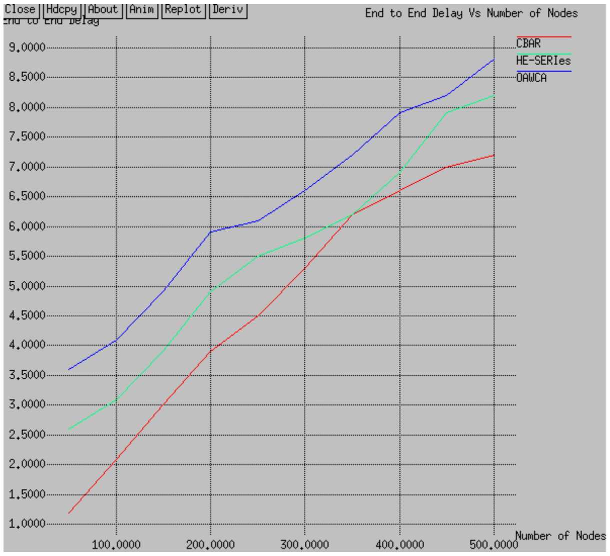

Fig 4: Tend to End Delay vs No.of Nodes

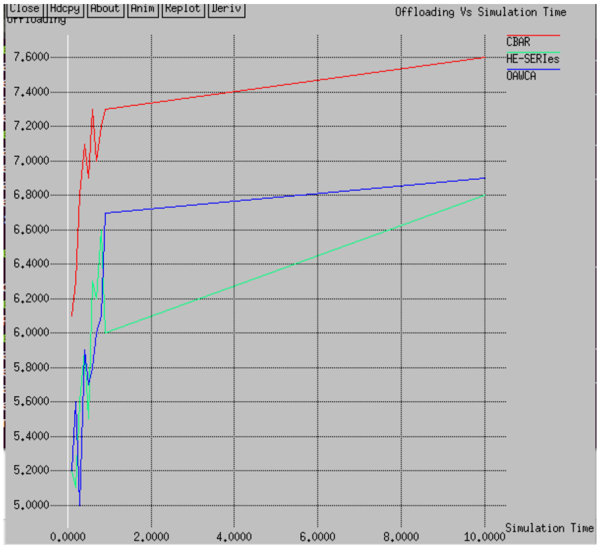

Fig 5: Offloading vs Simulation Time

Offloading ratio

The offloading ratio is defined as the ratio of offloading the data traffic to the overall traffic. It estimates the number of successful offloading performed by the CH. Fig. 5 explains the offloading ratio vs. the simulation time. The x-axis describes the simulation time in ms and the y-axis describes the offloading ratio. From graph it is clear that the proposed CBAR algorithm is compared to that of the existing OAWCA and He-SERIeS algorithms. The simulation time is varied from 10 to 100 ms. The offloading ratio is increased as the simulation time is increased. When compared to the existing algorithms, the proposed algorithms achieved high offloading ratio. Because, there is no self-downloading process in the network and it do not takes the time for downloading. Moreover, it represents how efficiently we provide the services based on the request. So, the offloading ratio can be increased in the proposed system.

VII. CONCLUSION

This Research paper proposed a novel algorithm, namely, CBAR algorithm for providing the scalability and Heterogeneity in MANET. The key intend of this work is to modify the existing He-SERIeS algorithm by using the learning agents, to cluster the similar requests from the nodes and to elect the CH that has the highest energy. There are two main algorithms developed for this purpose are Dynamic on-demand clustering and Ant Colony Optimization member selection based on the similar request generation. The proposed system supports the service providers, who provides the services based on the factor of Quality of Service (QoS) and the service provides should support the data offloading mechanism. The performance of the proposed algorithm is compared with the existing OAWCA and He-SERIeS algorithms. The metrics used for evaluating the performance of both existing and proposed techniques are throughput, delay, offloading ratio, and PDR. From the results, it is analyzed that the proposed CBARprotocol achieved a high throughput of 76.5% and PDR of 82.1%, when compared to the existing algorithms. The advantage of the work is to balance the load among several nodes using the offloading mechanism.

REFERENCES

[1] Nilesh N. Dangare M. Tech. (CSE) BDCOE, R. S. Mangrulkar Associate Professor Head Comp. Engg, BDCE, "Design and Development of Trust Based Approach to Mitigate Various Attacks in Mobile Ad-hoc Network", International Journal of Computer Applications (0975 – 8887) International Conference on Quality Up-gradation in Engineering, Science and Technology (ICQUEST2015).

[2] Poonam, K. Garg, M. Misra, Indian Institute of Technology Roorkee, India "Trust Based Multi Path DSR Protocol", 2010 International Conference on Availability, Reliability and Security.

[3] SHEN Ming-yu, LI Cang-yuan, School of Computer & Information. Hefei University of Technology Hefei, China, "Research and Analysis On Secure DSR Routing Protocol Based on Strand Space", 2010 International Conference on Electrical and Control Engineering.

[4] R. Sudha, S.Lecturer, CSE, Dr.Pauls Engineering College. Villupuram, Dr. D. Sivakumar, Professor & Head Department of IT, Adhiparasakthi Engineering College. Melmaruvathur, “A Temporal table Authenticated Routing Protocol for Adhoc Networks”, 978-1-4577-1894-6/11/$26.00©2011 IEEE.

[5] Ramasamy Mariappan Sangameswaran Mohan Professor, Department of CSE Department of CSE Adhiparasakthi Engineering College, Melmaruvathur, “Re-Pro Routing Protocol with Trust Based Security for Broadcasting in Mobile Ad hoc Network”,978-1-4673-0671-3/11/$26.00©2011 IEEE.

[6] Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi, Mohammad S. Obaidat, “Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks”, 978-1-4673-1550-0/12/$31.00 ©2012 IEEE.

[7] R. Menaka, Dr. V. Ranganathan, “A Survey of Trust related Routing Protocols for Mobile Ad Hoc Networks” International Journal of Emerging Technology and Advanced Engineering,ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013.

[8] Mehdi Keshavarz, Mehdi Dehghan, "MAC-Aided Packet-Dropper Detection in Multi-Hop Wireless Networks" 978-1-4673-0682-9/12/$31.00 ©2012 IEEE.

[9] Isaac Woungang, Mohammed S. Obaidat, Sanjay Kumar Dhurandher, Han-Chieh Chao, Chris Liu, "Trust-Enhanced Message Security Protocol for Mobile Ad Hoc Networks" 978-1-4577-2053-6/12/$31.00 ©2012 IEEE.

[10] Priyanka Goyal, Sahil Batra and Ajit Singh “A Literature review on Security Attack in Mobile Adhoc Networks” International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010

[11]. R.Rajeshkanna, Dr.A.Saradha "Cluster Based Load Balancing Techniques to Improve the Lifetime of Mobile Adhoc Networks"Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, Volume-2| Issue-5 , October 2015.

[12] Raja ML, Baboo CDSS. An overview of MANET: applications, attacks and challenges. Int J Comput Sci Mobile Comput 2014;3:408–17.

[13] Gavalas D et al. Clustering of mobile Ad hoc networks: an adaptive broadcast period approach. In: IEEE international conference on communications; 2006.p. 4034–9.

[14] Kaur K et al. Weightage based secure energy efficient clustering algorithm in MANET. In: International conference on advances in computing, communications and informatics (ICACCI); 2015. p. 1006–12.