An Efficient Multicast Routing Protocol Based on Ant with Improved Pheromone Updating Rule in Manet

Joshua Reginald Pullagura [1] and D.Venkata Rao [2]

Department of Electronics and Communication Engineering,
[1] Vignan's Foundation for Science Technology & Research, Vadlamudi-522 213, Guntur, A.P, India;
[2] QIS College of Engineering, Ongole, A.P, India.
E-mail: pjreginald@gmail.com

Abstract **- Multicast routing in Mobile Ad-Hoc Network (MANET) is s great challenge due to limitations like energy of the node and bandwidth. Routing protocols play important role in selecting path between source and destination nodes. Multicast protocols provide a bandwidth-efficient support for group-oriented applications. Even though many multicast routing protocols are developed for MANETs, security is still challenging issue. So, in this work, an Efficient Multicast Routing Protocol (EMRP) is proposed by using Ant with Improved Pheromone Updating Rule (AIPUR) for MANETs. In the improved pheromone updating phase, worst ants are identified by using modified TOPSIS method and it is removed. Initially, clustering is done to make authentication process easy and the optimal Cluster Head (CH) selection is done with the concern of their security level where the selected cluster head should be trustable and should contain increased energy and bandwidth availability. Here optimal CH selection is done by using AIPUR. CH is responsible for generating the secret key for its cluster members by using which cluster member would generate signature in their data which is to be shared with other nodes before transmission and these CH will perform authentication by using the key generated based on which authentication of the data would be guaranteed. The proposed optimal and reliable routing is guaranteed by establishing routing with nodes that satisfied the QoS conditions like increased energy and bandwidth.**

Keywords - Ant colony optimization, Cluster, Cluster Head and Routing.

I. INTRODUCTION

Wireless communication technology gained high momentum in modern age with development of two basic wireless models [1]. The wireless model with permanent infrastructure consisting many number of a Mobile Nodes (MNs) and temporary network [2], which is a self-organizing collection of MNs sharing wireless medium without utilizing any fixed networking infrastructure. The data transfer between the nodes within their transmission range occurs via unguided transmission medium. Data transfer can be accomplished either by single-hop transmission or by multi hop transmission [5]. Intermediate nodes play a vital role in routing the packets from source to destination.

All the nodes will communicate with each other with in their fixed range. Limitation of transmission range is one of the main concerns; therefore multiple hops may be needed for exchange of data with another throughout the network. Every mobile node (MN) operates both as a host and also as a router. Apart from source, every intermediate node participates in route discovery process. Due to wider applications, MANETs are attracting modern day researchers. Multicast routing techniques belonging to different routing strategies are proposed in the literature. A proactive routing protocol pre-determines the path between communicating nodes, while reactive discover routes only when needed. Multicast protocols [5], [6], [7] that consider nodes energy during packet transfer are also discussed in the literature. Apart from computing multiple paths, these protocols will also maintain all the paths between nodes. To attain productive routing, the concept of clustering is used.

Generally, clustering is division of the network into various virtual groups based on predefined rules such that every group will have few numbers of nodes [11]. To reach scalability clustering is one of the widely used technique. The nodes in a cluster are grouped into four categories namely, Cluster Head(CH) node, which acts like a central coordinator of the cluster maintaining routing information and topological information of nodes, Gateway nodes(GN) located at the boundaries, Member nodes(MN) and Guest nodes. Previous researches have proposed many cluster head selection approaches for constructing clusters. But, still the CH selection is a great challenging task.

So, in this paper, an effectual MRP is proposed by using AIPUR algorithm in MANETs. Initially, clustering is done to make ease authentication process and the optimal Cluster Head (CH) selection is done with the concern of their security level where the selected cluster head should be trustable and should contain increased energy and bandwidth availability. Here optimal CH selection is done by using ACO with IPUR. Then, the multicast routing is done for secured data transmission. The experimental results show that the proposed EMRP with AIPUR attained better performance compared than existing multicast routing protocols. The remainder of the paper is organized as follows: Section 2 summarizes existing methodologies of multi-cast routing protocols. Section 3 proposes the cluster-based EMRP algorithm. Experimental results are discussed in section 4 and conclusions are discussed in last section.

II. CURRENT WORK

In this section, the existing multicast routing protocols with clustering based schemes has been discussed. V.Gupta, S.K.Sharma [3] proposed an improvement to low energy clustering hierarchy protocol (LEACH-MA) which improves the average energy consumption of the network effectively, buy using the concept of Ant colony algorithm. Modified Ant colony algorithm (MACO) [4] which provides Multicasting routing with less time was designed by Sudip Kumar, Mohammed AL-Fayoumi, Prabhat Kumar Mahanti. Wang [9] proposed power-aware dual tree-based multicast scheme to increase network life time by balancing load. Akbari and Riza designed a ‘‘distributed learning and weighted learning automata’’ based algorithm to find more stable route for multicast networks [10]. A Link Stability Based Multicast Routing (LSMRM) protocol designed by Biradar et al.[11] [12]. computes routes using power and distance metrics. Biradar et al. [13] designed a Multipath Multicast routing in MANETs using Reliable Neighbor Selection (MMRNS) mechanism. In [14], authors investigated the problem in multicast routing by using network coding technique to obtain the maximum flow multicast routes in ad-hoc networks. Karthikeyan et al. [15–17] proposed a multicast routing protocol using Genetic Operator Algorithm (GOC) that reduces delay.

Yu el al [18] proposed robust multiple tree routing with security features which comes under multicast scheme. Yadav et al. [19] proposed a traffic load balanced multicast routing protocol (LBMRP) to reduce the network overhead and increase the network life. Singal et al. [20] presented a QoS aware routing based on link stability cost function (LSF). Protocol based on Residual energy (RERMR) is proposed to attain more network lifetime and increased packet delivery and forwarding rate. Sethuraman et al [21] proposed an algorithm that sends packets securely in the network with less power consumption. Finding a reliable route between source and destination nodes abiding QoS parameters is much needed. However, existing protocols are not much efficient in computing stable and long lasting routes.

III. EMRP-AIPUR METHODOLOGY

In this section, the proposed EMRP-AIPUR based routing has been discussed.

A. System Overview

In this paper, Efficient Multicast Routing Protocol by using Ant colony optimization with pheromone updating rule is presented. Clustering is done to improve the data transmission security. In this clustering process, the CH is selected by using ACO with IPUR. The QoS parameters like residual energy and bandwidth are considered to select the reliable route between the sender and the receiver. Figure 1 shows the block diagram of EMRP-AIPUR.

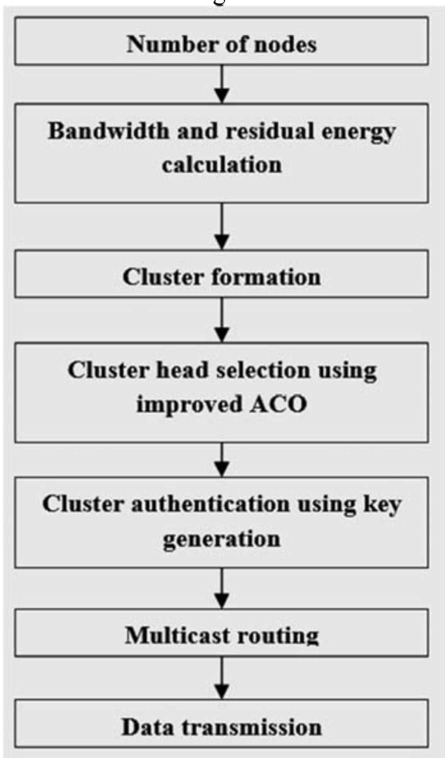

Fig 1: EMRP-AIPUR based multicast routing process.

B. Cluster Formation

Process of dividing network into small number of sub groups interconnected with each other is termed as clustering. Clustering provides a fair solution to the issues like scalability, out of range communication, key management and provides optimal availability of network resources for every node. For better management of nodes a Cluster head is selected within the cluster. Figure 1 shows the proposed methodology where at the outset nodes are divided into many clusters. Cluster head will perform the functions like nodes coordination with in their cluster, key distribution and management. The performed clustering mechanism should be effective in a way that it divides the network into number of small groups and must preserves the basic network features for longer duration. Cluster head should be properly selected as the entire strength of Cluster is based on it, if cluster head collapses, the entire cluster formation goes vain. The main reasons attributed for the failure of Cluster head are mobility, nodes energy, heavy traffic flow and other constrained resources. For the selection of effective cluster head, we considered two parameters i.e, total energy and bandwidth.

DOI 10.5013/IJSSST.a.19.06.19

ISSN: 1473-804x online, 1473-8031 print

The total energy E_t consumed:

$$E_t(s_i, d) = \begin{cases} s_iE + s_i\varepsilon_{fs}d^2, d \le d_0 \\ s_iE + s_i\varepsilon_{mp}d^2, d > d_0 \end{cases} \quad (1)$$

$$d_o = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}} \quad (2)$$

where E represents the energy taken for transmission or reception of one bit message; $\varepsilon_{fs}$is the amplification coefficient of free-space signal and ε_{mp} is the multi-path fading signal amplification coefficient, d represents the distance between source node and receiver node and s_i is the bit amount of sending information.

Available bandwidth (Bw)

Bandwidth estimation is much needed for efficient data transfer. When a node wants to transfer the data packets it should aware of its own limited bandwidth and its neighboring mobile nodes information within the interference range. Bandwidth is shared by all the neighboring nodes. Local bandwidth (BW_L) is given as:

$$BW_L = C_{CH} * (T_i/T_{in}) \quad (3)$$

where C_{CH} is the channel capacity, Ti is the idle period in the predefined period Tin. Bandwidth (Bw) of the node is given by

$$Bw = BW_L - BW_{min} \quad (4)$$

C. Cluster head selection and cluster formation using AIPUR

Ant Colony algorithm is a nature inspired evolutionary algorithm introduced by Dorigo [24]. Here the Improved Ant Colony algorithm is used for forming clusters and selecting the cluster head in wireless ad hoc networks. Cluster Head is selected by considering parameters like node position, residual energy and available bandwidth. By computing the above mentioned parameters the weight of every node in the network is estimated by iteration.

Network can be considered in the form of a graph and each node's location is represented using its x and y coordinate values. Here hierarchical routing is done to minimize routing control overhead. ACO is used to select Cluster Head (CH). A cluster head is identified by computing the pheromone value of every node and its visibility. For every iteration the pheromone value is updated. Initially a node with high values of pheromone and visibility is selected as cluster head and the next cluster head is selected based on the pheromone and visibility after iteration. Whenever a node is selected as a cluster head, its pheromone value is updated. At each time t, an ant k moves from its current node i to an unvisited node j based on the distance between them and the amount of pheromone on the edge that connects them. If there is more than one unvisited node, the ant k will choose its next node according to the following transition probability:

$$p_{ij}^k(t) = \begin{cases} \frac{[pc_{ij}(t)]^\alpha . [vi_{ij}(t)]^\beta}{\sum_{s\in all_k}[pc_{ij}(t)]^\alpha . [vi_{ij}(t)]^\beta} j \in all_k \end{cases} \quad (5)$$

where α and β are weighting parameters and all_k is the set of nodes not visited by ant k, pc_{ij} represents the pheromone concentration on the path: node i to node j and vi_{ij} denotes the visibility of the node j from the node i as follows:

$$vi_{ij} = \frac{1}{d_{ij}}, d_{ij} = \text{distance among two nodes} \quad (6)$$

The pheromone updating formula is given by:

$$vi_{ij}(t+1) = (1-\rho)pc_{ij}(t) + \sum_{k=1}^{m} \Delta vi_{ij}^k \quad (7)$$

Where ρ is the pheromone evaporating rate, m is the number of ants and Δvi_{ij}^k represents the amount of pheromone left by the ant k at the current iteration, which can be expressed as follows:

$$\Delta vi_{ij}^k = \begin{cases} \frac{Q}{L_k} \text{edge(i, j) is used in search} \\ 0 \text{ otherwise} \end{cases} \quad (8)$$

where L_k is the length of the path that was found by the ant k and Q is a constant. The conventional ACO based routing mechanisms are not yielding good performance due to the appearance of bad pheromone. So, to improve the process of ACO, here we presented improved pheromone rule.

Improved pheromone updating rule

In order to find the shortest route to the destination the amount of pheromone is main factor , however, it contains a certain amount of bad pheromone which is generated by the bad ants, and this make other good ants move to nodes where the goal is inaccessible..

Here worst ants are identified and removed by using modified TOPSIS method. Modified TOPSIS method would identify the ants that are worse in their behavior which is measured based on energy consumption and bandwidth. Thus the pheromone updating is done efficiently. Problem in multi criteria decision making can be handled effectively using TOPSIS method. *D* Numbers theory is a advanced representation of uncertain information, which can denote the more fuzzy conditions. So the combination of TOPSIS and *D* numbers is a new experiment to make decisions in an uncertain environment. The steps in the Modified TOPSIS are given as follows:

Step 1: Construct of the Decision Matrix

Step 2: Determine *D* Numbers

Step 3: Find the positive ideal and negative ideal solutions
Step 4: Compute the separation measures of the existing alternatives from the positive ideal and negative ideal solutions.
Step 5: Calculate the relative closeness to the ideal solution:
Step 6: Give the Rank to the alternatives according to the relative closeness to the ideal solution
Step 7: Select CH based on the rank

D. Cluster based Authentication

Existing public key mechanism will have a fixed Registration Centre (RC), All the members will use the services of RC for achieving authenticity and security .But the problem here is single point failure, As RC fails, the desired goal is not accomplished which leads to security threats. Manets have distributed nature and it needs a distributed authentication model. In the proposed method, cluster head acts like RC. It overcomes single point of security problem. Our proposed method uses Chebyshev polynomials, which is defined as follows:

cosnθ can be written as polynomials in cosnθ then:

$$\cos n\theta = T_n \cos\theta$$

$$\cos\big((n+1)\theta\big) = 2\cos(n\theta).\cos\theta - \cos\big((n-1)\theta\big) \quad (9)$$

$$T_{n+1}(\cos\theta) = 2T_n(\cos\theta)\cos\theta - T_{n-1}(\cos\theta)$$
$$T_{n+1}(X) = 2XT_n(X) - T_{n-1}(X) \quad (10)$$

$$T_n(X) = \big(2XT_{n-1}(X) - T_{n-2}(X)\big) \quad (11)$$

Equation 11 represents the Chebyshev polynomial $T_n(X)$. Semi group property of Chebyshev polynomials is used to provide authentication .In above equations n≥ 2 and N is a large prime number and $X \in (-\infty, +\infty)$. In equation (11) given$T_n(X)$, X and N, it is mathematically not possible to compute the value of 'n', and this is termed as, Chaotic Maps-Based Discrete Logarithm problem.

Chebyshev polynomials have Composition property which states as:

$$T_n\big(T_m(X)\big) = T_m\big(T_n(X)\big) = T_{nm}(X) \quad (12)$$

In equation (12) given $T_n(X)$, $T_m(X)$, X and N, it is mathematically not possible to find the value of $T_{nm}(X)$, i.e, Chaotic Maps Based Diffie-Hellman problem. From equation (11, 12) our proposed methodology is developed.

Key Generation and Distribution

In the proposed Chebyshev polynomials based cluster authentication mechanism, Consider a network with clusters. Cluster heads are designated as CH_i, (i = 1,2,3,4,5..)and corresponding cluster members are CM_i, (i = 1,2,3..)

1. Mobile hosts in network are assigned with a new identities i.e cluster heads as CH_i, (i = 1,2,3.4,5.) and cluster members as CM_i, (i = 1,2,3,4,5..)
2. Let cluster heads in a network $CH_i$with identities ID_{chi} randomly pick a prime numbers X_i and K_i and compute $T_{Ki}(X_i)$ where public information is $(X_i, K_i, ID_{chi}, T_{Ki}(X_i))$ and private information is 'K_i' . Cluster members CM_j with identities ID_{cmj} will take a large prime number K_j and calculates the value of $T_{Kj}(X_i)$,
3. Cluster head public information (ID_{cmj},$T_{Kj}(X_i)$ is distributed to cluster members whenever cluster is formed and whenever updates about nodes takes place.
4. Cluster member share their public information with cluster heads whenever changes takes place.

To achieve robust authentication our proposed scheme uses two keys i.e. Cluster key and Session key. The entry of new node into cluster set will be identified by Cluster head with the help of hello packets. Clusters public information, identities, cluster head public key (PK) and common encryption and decryption algorithms are sent to members by Cluster head. Nodes in the cluster will compute their cluster key(CK) by using PK of cluster head, and transmits its PK to CH. Cluster key(CK) is used to check authentication between cluster head and members. Due to mobile nature of nodes they may leaves the cluster and joins other cluster. New node getting the key is shown in Fig 2.

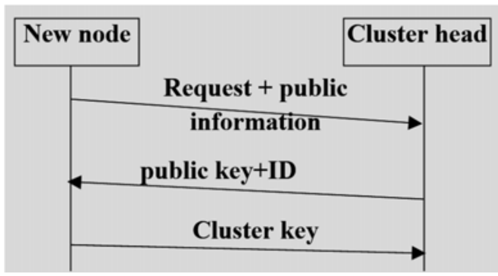

Fig 2: Node getting cluster key

To achieve authentication the session key is computed and shared among nodes that are exchanging data with the help of key exchange mechanism. Confidentiality is achieved by the process of encryption and decryption with session key.

E. Multicast Routing

After authentication, the multicast routing is introduced for secured data transmission. Nodes with high residual energy and density are given high priority. Next node selection and multicast routes are selected based on above said criteria. The multicast routing here is summarized in three phases:

E1. Route Request Phase: Source will find the route to multiple destinations by using RRQ packets. The operation can be summarized in following phases:

- Source node initiates RRQ packets and selectively transmits the packet to neighbors considering residual energy and node density.
- Duplicate RRQ packets are discarded by intermediate node, based on sequence number in RRQ packet. If RRQ packet is not a duplicate, intermediate node checks routing table for availability of routes, if routes are available, RRP packet will be propagated to source.
- If RRQ packet is a duplicate, then discard it and stop transmission of RRQ packet, if it is not duplicate and no route available in Routing Information table, then RRQ packet is transmitted by updating its fields.

E2. Route Reply Phase: When RRQ packet reaches the destination node, Multicast destinations will generate RRP which is transferred to source.

E3. Route Maintenance Phase: As the routes selected in proposed mechanism are stable, route failure is a rare phenomenon. But in unusual cases three types of link failures are noticed; link failure between intermediate nodes in the network, link failure between source node and intermediate node, and path failure between destination node and intermediate node. If the above said cases arise, the network problem can be addressed by the following techniques:
- In case of link failure between two intermediate nodes, the node, detecting failure condition will use RRQ and RRP packets to find stable path to the destination. The new path from intermediate node to destination will be informed to source where RRQ packet originated. If a new path cannot be found, the node will send RRQ packet to source to rediscover the paths.
- In case of link failure between source and intermediate node, source node will use alternate backup path.
- In case of link failure between destination and intermediate node, the intermediate node will use RRQ and RRP packets to discover paths to destination from itself and informs the source about the new path.

IV. RESULTS AND DISCUSSION

In this section two existing protocols are compared with our proposed mechanism. The simulation parameters are shown in Table I.

TABLE I. SIMULATION PARAMETERS

Area	1000*1000
Number of nodes	80
Tool	NS-2.35
BS location	(50,50)
Routing Protocols	LEACH-MA, MACO, EMRP-AIPUR

A. Numerical Evaluation of Proposed Method Against Existing Methods

Figures 3, 4, 5, 6 and 7 illustrate the performance of EMRP-AIPUR, MACO and LEACH-MA with different number of nodes and Table 2,3,4,5 and 6 shows comparison values respectively. As shown in Fig 3 the PDR increases with the increase in multicast receiving nodes. EMRP-AIPUR achieves a higher PDR as compared to MACO and LEACH-MA because of proper management of energy and bandwidth while establishing the stable multicast routes. From tabulated results it is concluded that the EMRP-AIPUR shows 2.32% increased PDR than MACO and 8.94% increased PDR than LEACH-MA.

TABLE II PACKET DELIVERY RATIO VALUES

Number of Nodes	Packet delivery ratio comparison values		
	LEACH-MA	MACO	EMRP-AIPUR
10	0.3	0.31	0.32
20	0.6	0.63	0.65
30	0.75	0.79	0.8
40	0.89	0.93	0.95
50	0.95	1.02	1.05
60	1.03	1.12	1.14
70	1.1	1.19	1.21
80	1.18	1.25	1.29
Avg	0.85	0.905	0.926

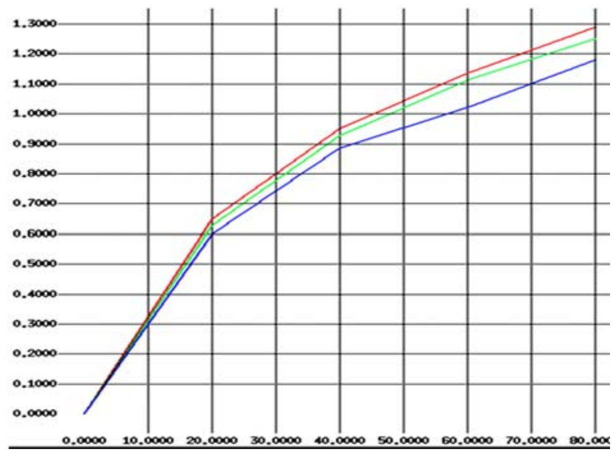

Fig 3: Packet delivery ratio comparison among various protocols: **Red**=LEACH-MA-delay, **Green**=MACO-delay, **Blue**=EMRP-AIPUR-delay

Fig 4 shows the Packet Loss Rate (PLR) of EMRP-AIPUR, MACO and LEACH-MA. From the results we can see that the PLR of proposed protocol EMRP-AIPUR is less than that of MACO and LEACH-MA. The reason is EMRP-AIPUR uses the reliable paths for data transmission .The packet drop of EMRP-AIPUR is thus lower than the other protocols.

TABLE III. PACKET LOSS RATIO VALUES

Number of Nodes	Packet Loss Ratio Comparison Values		
	LEACH-MA	**MACO**	**EMRP-AIPUR**
10	150	230	240
20	300	260	250
30	400	360	350
40	500	460	450
50	625	600	675
60	750	715	700
70	850	800	800
80	940	900	900
Avg	564.375	540.625	546.625

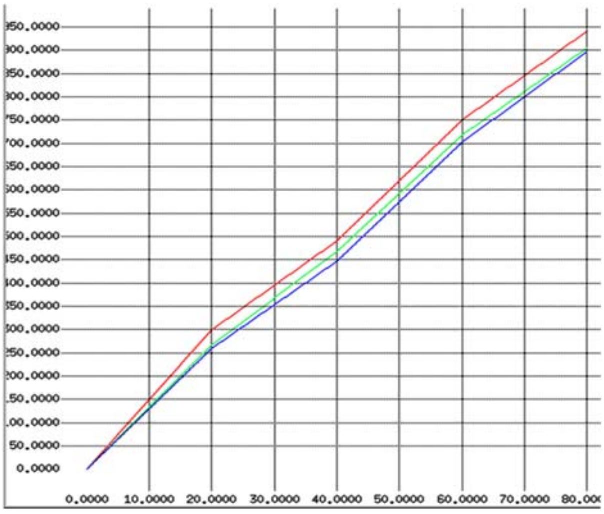

Fig 4: Packet loss ratio comparison among various protocols: **Red**=LEACH-MA-delay, **Green**=MACO-delay, **Blue**=EMRP-AIPUR-delay

From this comparison figure it is confirmed that the proposed research method EMRP-AIPUR achieves lesser packet loss ratio than the existing research methods where it is 0.92% lesser than LEACH-MA and 3.24% lesser than the MACO.

Packet delay is defined as the time it has delayed to complete the packet transmission completely. In this research work, end to end delay is considered for the measurement of packet delay.

TABLE 4. PACKET DELAY VALUES

Number of Nodes	Packet Delay Comparison Values		
	LEACH-MA	**MACO**	**EMRP-AIPUR**
20	100	60	60
40	400	350	325
60	630	675	640
80	740	700	675
Avg	467.5	446.25	425

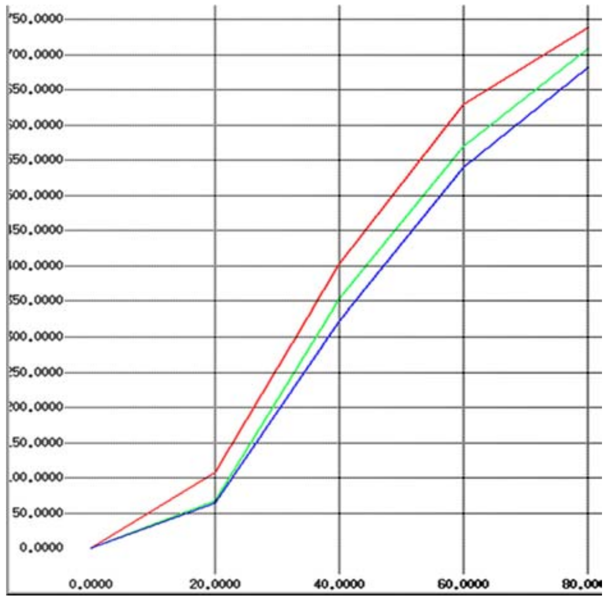

Fig 5: Packet delay among various routing protocols: **Red**=LEACH-MA-delay, **Green**=MACO-delay, **Blue**=EMRP-AIPUR-delay

From above figure it is evident that proposed EMRP-AIPUR protocol reduces the packet delivery delay because it considered the reliable routing path then MACO and LEACH-MA .The packet delay of proposed method EMRP-AUPIR is lesser than other methods where it is 4.76% lesser than MACO and 9.09% lesser than LEACH-MA.

B. Throughput

Throughput is defined as total number of packets successfully delivered in a given time period. The graphical representation of throughput comparison among proposed EMRP-AIPUR and existing protocols like MACO and LEACH-MA are shown in the Fig 6 and corresponding results are tabulated in Table 5. The results show that the proposed protocol attained high throughput compared than other protocols, due to the effectual cluster head selection and authentication mechanism used.

TABLE 5. THROUGHPUT COMPARISON

Number of Nodes	Throughput Comparison Values		
	LEACH-MA	**MACO**	**EMRP-AIPUR**
10	0.39	0.4	0.42
20	0.78	0.8	0.87
30	0.94	1	1.02
40	1.12	1.15	1.2
50	1.22	1.29	1.3
60	1.33	1.39	1.41
70	1.5	1.54	1.59
80	1.63	1.7	1.72
Avg	1.11375	1.15875	1.19125

DOI 10.5013/IJSSST.a.19.06.19 ISSN: 1473-804x online, 1473-8031 print

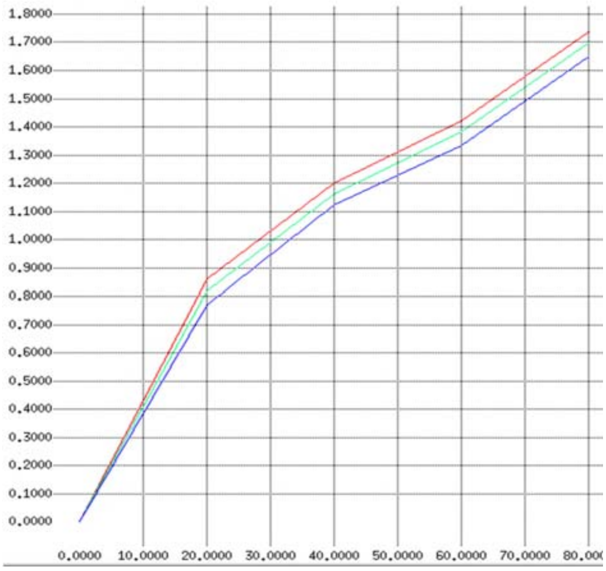

Fig 6: Throughput comparison among various protocols: **Red**=LEACH-MA-delay, **Green**=MACO-delay, **Blue**=EMRP-AIPUR-delay

From Fig 6, it is concluded that the proposed method EMRP-AIPUR achieves higher throughput than the existing methods where it is 2.8% higher than MACO and 6.9% higher than LEACH-MA.

C. Energy Consumption

The energy consumption values are tabulated in Table 6 and corresponding graphical representation for proposed mechanism and existing protocols like MACO and LEACH-MA are shown in the Fig 7. The graph shows that the proposed protocol attained less energy compared than other protocols due to the effectual cluster head selection and updation of Cluster Head for every iteration.

TABLE 6. ENERGY COMPARISON

Number of Nodes	Energy Consumption Comparison Values		
	LEACH-MA	Maco	EMRP-AIPUR
20	110	75	75
40	155	125	105
60	360	325	300
80	550	475	450
Avg	293.75	250	232.5

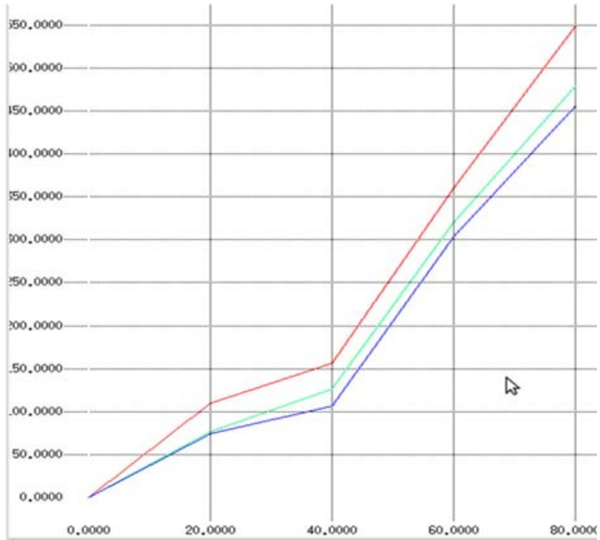

Fig 7: Energy consumption comparison among various routing protocols: **Red**=LEACH-MA-delay, **Green**=MACO-delay, **Blue**=EMRP-AIPUR-delay

Proposed research method EMRP-AIPUR consumes lesser energy than the existing methods where it is around 7.0% lesser than MACO and 20% lesser than LEACH-MA.

TABLE 7. ENCRYPTION TIME COMPARISON

Bits	Encryption Time Comparison Values	
	ECC	Chebyshev
50	340	315
100	380	360
150	425	400
200	460	440
250	490	475
Avg	419	398

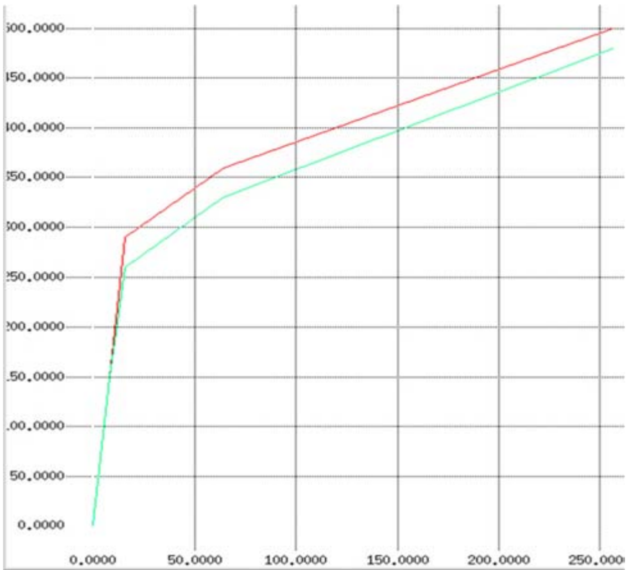

Fig 8: Encryption time comparison values, **Red**=ECC-enc-rime, **Green**=Chebyshev-enc-time

In Fig 8, Chebyshev Polynomial based encryption and the Elliptical Curve Cryptography based encryption is compared. From this comparison we can conclude that the proposed method Chebyshev can complete the encryption with less encryption time than the existing method. From this numerical evaluation it is confirmed that the proposed Chebyshev method can perform authentication with less time where it is 5.2% lesser than the existing method.

TABLE 8. KEY SIZE COMPARISON

Bits	Key size comparison values	
	ECC	Chebyshev
50	100	80
100	200	150
150	300	215
200	400	275
250	500	375
Avg	300	219

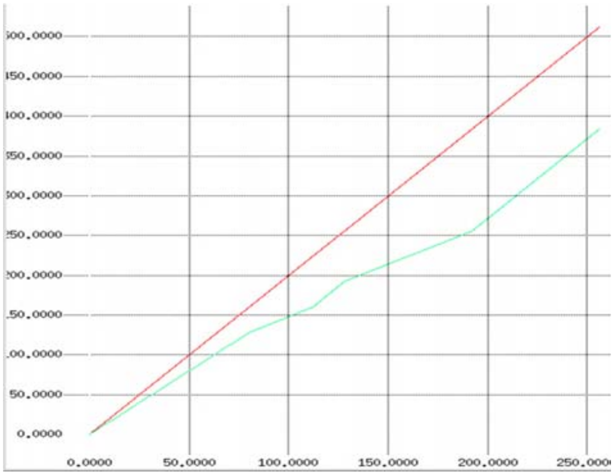

Fig 9: Key size comparison, **Red=**ECC-enc-rime, **Green**=Chebyshev-enc-time

Key size of the proposed method should be lesser for the better performance which would ensure the secured encryption with less overhead. And also smaller key size would ensure the secured authentication outcome which would be faster than the other research methods. From the numerical analysis given in Table 8 and from Fig 9 it is concluded that the proposed method generates keys with lesser size than ECC.

TABLE 9. FALSE POSITIVE RATE COMPARISON

Bits	False positive rate comparison values	
	ECC	Chebyshev
50	380	300
100	425	400
150	445	420
200	470	435
250	480	460
Avg	440	403

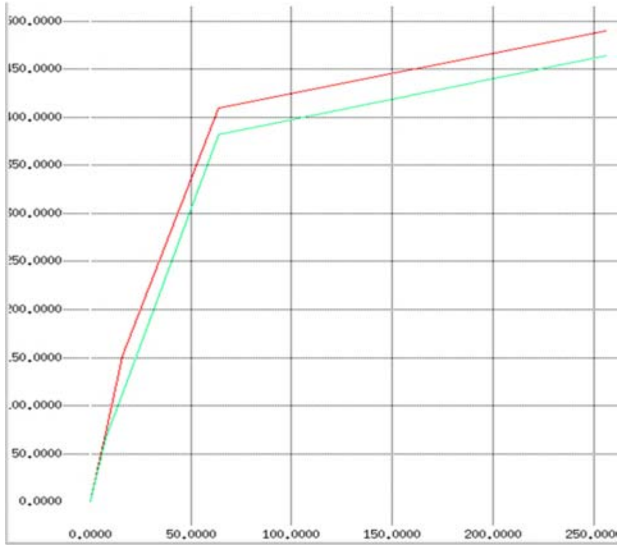

Fig 10: False positive rate comparison, **Red=**ECC-fp, **Green**=Chebyshev-fp

In Fig 10, false positive rate comparison evaluation of the proposed Chebyshev Polynomial based cryptography and existing ECC is shown and values are tabulated in Table 9. From this comparison evaluation, it is confirmed that the proposed method Chebyshev can perform authentication with less error rate where it achieves 8.401% lesser false positive rate than ECC.

TABLE X. OVERHEAD COMPARISON

Bits	Overhead comparison values	
	ECC	Chebyshev
50	5.75	5.6
100	5.95	5.75
150	6	5.75
200	6	5.75
250	6.05	5.8
Avg	5.95	5.73

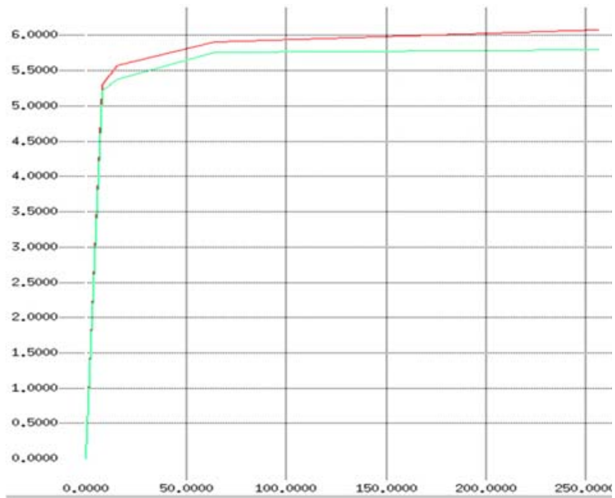

Fig 11: Overhead comparison, **Red=**ECC-overhead, **Green**=Chebyshev-overhead

In Fig 11, comparison of the proposed and existing method in terms of overhead after authentication process is given. The overhead of the proposed system's authentication should be less for the efficient and secured process. From this numerical evaluation it is confirmed that the proposed method Chebyshev achieves 3.69% lesser overhead than the existing ECC method.

V. CONCLUSION

In this work, an EMRP is proposed by using AIPUR algorithm in MANETs. Initially, clustering is done to make ease authentication process and the optimal Cluster Head (CH) selection is done with the concern of their security level where the selected cluster head should be trustable and should contain increased energy and bandwidth availability. Here optimal CH selection is done by using AIPUR. Then, the multicast routing is done for secured data transmission. The simulations show that the proposed EMRP with AIPUR attained better performance compared than existing MACO and LEACH-MA multicast routing protocols in terms of PDR, PLR, packet delay,throughput and energy consumption. In future, some other factors like mobility and delay will be focus for cluster formation.

REFERENCES

[1] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless adhoc networks," IEEE Commun. Mag., vol. 40, no. 10, pp. 70–75, Oct.2002.

[2] M. Younis and S. Z. Ozer, "Wireless ad-hoc networks: Technologies and challenges," Wireless Commun. Mobile Computing, vol. 6, no. 7, pp. 889–892, Nov. 2006.

[3] V.Gupta, S.K.Sharma "Cluster Head selection using modified ACO" K.N.das et al, Springer Proceedings of Fourth International Conference on Soft Computing for problem solving.

[4] Sudip kumar, Mohammed AL-Fayoumi, Prabhat Kumar Mahanti "Applications of Modified Ant Colony Optimization for Multicast routing Problem", I J Intelligent Systems and Applications, 2016, 4,pp 43-48.

[5] Joshua Reginald Pullagura, D.Venkata Rao " Simulation based performance evaluation of energy efficient protocols in ad hoc networks", Journal of Advanced Research in Dynamical and Control Systems , Special Issue – 02 / 2017, volume 9,pp 1141-1149

[6] S. Guo and O. Yang, "Energy-aware multicasting in wireless ad-hoc networks: A survey and discussion," Computer Commun., vol. 30, no.9, pp. 2129–2148, June 2007.

[7] X. Chen and J. Wu, "Multicasting techniques in mobile ad-hoc networks, "The Handbook of Ad-hoc Wireless Networks, pp. 25–40, 2003.

[8] L. Junhai and Y. Danxia, et al., "Research on routing security in MANET," Application Research of Computers, vol. 25, no. 1, pp. 243–245, Jan. 2008.

[9] N-C. Wang, "Power-aware dual-tree-based multicast routing protocol for mobile ad hoc networks" IET Communications vol. 6 , Issue: 7 , May 1 2012.

[10] Javed Akbari and Mohammed Reza, "A learning automata-based heuristic algorithm for solving the minimum spanning tree problem in stochastic graphs" The journal of super computing 59(2):1035-1054 · February 2012.

[11] Biradar R, Manavi S, Reddy M (2010) Link stability based multicast routing in MANET. Comput Netw 54:1183–1196 (Elsevier).

[12] Biradar RC, Manvi SS (2011) Neighbour supported reliable multipath multicast routing MANETs. J NetwComputAppl 35:221–229 (Elsevier).

[13] Biradar RC, Manvi SS (2011) Neighbour supported reliable multipath multicast routing MANETs. J NetwComputAppl 35:221–229 (Elsevier).

[14] Surendar, A., Arun, M., & Periasamy, P. S. (2013). Hardware based algorithms for bioinformatics applications-A survey. Int. J. Appl. Eng. Res.(6), 745-754..

[15] Karthikeyan P, Baskar S (2013) Improvement in genetic algorithm with genetic operator combination (GOC) and immigrant strategies for multicast routing in ad hoc networks. Lect Notes ComputSci 8297:481–491.

[16] Karthikeyan P, Baskar S, Alphones A (2013) Improved genetic algorithm using different genetic operator combinations (GOCs) for multicast routing in ad hoc networks. Soft Comput 17(9):1563–1572 (Springer).

[17] Karthikeyan P, Baskar S (2015) Genetic algorithm with ensemble of immigrant strategies for multicast routing in Ad hoc networks. Soft Comput 19(2):489–498 (Springer).

[18] Yu Y, Zhou Y, Du S (2009) Video multicast over mobile ad hoc networks using network coding.in: International conference on management and service science, pp 1–5, 20–22 September 2009.

[19] Ajay yadev, Sachin tripati "Design of Load Balanced Multicast Routing Protocol for Wireless Mobile Ad-hoc Network" Wireless personal communications, 85(4):1815-1829 · December 2015

[20] J., Yakubu H., Aboiyar T., and Zirra P. B.. "An improved RSA image encryption algorithm using 1-D logistic map." International Journal of Communication and Computer Technologies 6.1 (2018), 1-6

[21] Sethuraman, P.; Kannan, N. Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET. Wirel. Netw. 2017, 23, 2227–2237. [CrossRef]

[22] M.dorigo, L.M Gambardella" Ant colony system: a cooperative learning approach to the traveling salesman problem "IEE transactions on Evolutionary Computation Volume: 1 , Issue: 1 , Apr 1997.