TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

QoS Aware Multicast Routing Protocol using Reliability based Pruning Technique

Joshua Reginald Pullagura[1*], Dr. D Venkata Rao[2]
[1]*Vignans foundation for Science Technology and Research Deemed to be University, Guntur,*
[2]*QIS College of Engineering and Technology, Ongole*
*pjreginald@gmail.com**

Article Info
Volume 82
Page Number: 3260 - 3277
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 20 January 2020*

Abstract:
Multicast routing is the process of forwarding data packets to the multiple destinations through multi route paths. Secure and reliable multicast routing is a challenging task which needs to be done with proper management of nodes energy. This paper proposes pruning nodes based stable and efficient multicast routing protocol (PN-SEMRP) for Mobile Adhoc Networks. In this work, multicast routing is guaranteed by establishing the multiple route paths to the multiple destinations with the concern of energy. Initially clustering of nodes is done to ensure the organized data transmission. The cluster head is selected by using modified firefly algorithm. Multipath route computation is done with the guaranteed QoS parameters like increased energy and bandwidth to reach the destination nodes. Reliability pair factor is computed between the neighbouring nodes involved in the multiple paths and pruning of neighbour nodes that have reliability pair factor lesser than a threshold is done by using Cuckoo based optimized multilayer feed forward neural network. Finally unique key based secret key establishment Method (UKSKEM) is introduced for the secured data transmission and authentication. The implementation of the work carried in NS2 simulation environment from which it is proved that the proposed routing technique tends to provide better results than existing techniques under Sybil and Black hole attacks.

Keywords:*Energy consumption, Multicast routing, QoS consideration, Reliability, Security.*

I. INTRODUCTION

Due to remarkable growth in adhoc networking, Multicast applications also increased rapidly both in civilian and defence fields [1].Some of the applications like video conferencing, web learning and discussion forums etc are widely seen in day to day life[2]. In multicasting packets are transmitted from a source to a group of nodes [3]. Multicasting reduces the transmission cost when sending the same packet to multiple recipients. All the multicast packets should be delivered with same quality as regular unicast packets [4].

Some of the other major advantages of Multicast servicesare reducing communication costs, processing time and bandwidth [5]. In addition, it can provide a simple and robust communication mechanism when the receiver's individual address is unknown or changeable [6]. Apart from the regular routing issues multicast ad hoc networks face some security related challenges like authentication, integrity, access control and confidentiality [7]. Multicast sessions

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

should be properly established and maintained [8].Session can be either public or private[9]. In private session, access is restricted through a registration and authentication process. Only nodes that are authorized will be able to participate in the session [10].

X.800 has defined various security mechanisms which need to be incorporated in multicast routing to avoid possible threats and attacks. Robust security mechanisms need to be implemented to overcome the threats in multicast routing [11]. In this paper, secured and reliable multicast routing is proposed and is compared with existing protocols. The methodologies that are proposed tend to ensure the better performance in terms of increased security level. This is done by selecting the multicast routing in terms of route stability and pruning the nodes that are having less reliability.

II. RELATED WORKS

Lu et al [13] presented an energy-efficient genetic algorithm mechanism to resolve quality of service (QoS) multicast routing problem, the proposed genetic algorithm depends on bounded end-to-end delay and minimum energy cost of the multicast tree. Garcia-Luna-Aceves et al [14] presented protocol for routing in Interest-defined Mesh Enclaves (PRIME) to implement the proposed framework for integrated routing in MANETs. PRIME establishes meshes that are activated and deactivated by the presence or absence of interest in individual destination nodes and groups and confines most of the signalling overhead within regions of interest (enclaves) in such meshes. The routes established in PRIME are shown to be free of permanent loops. Experimental results based on extensive simulations show that PRIME attains similar or better data delivery and end-to-end delays than traditional unicast and multicast routing schemes for MANETs (AODV, OLSR, ODMRP). Singal et al [15] initiated QoS aware routing metric where route establishes is based on cost function of the link. It out performs ODMRP multicast routing protocols.

Viswanath et al [16] proposed two variations of flooding, scoped flooding and hyper flooding, as a means to reduce overhead and increase reliability, respectively. Another contribution of the work is a simulation-based comparative study of the proposed flooding variations against plain flooding, mesh, and tree-based MANET routing. In our simulations, in addition to "synthetic" scenarios, we also used more realistic MANET settings, such as conferencing and emergency response.Ahmed et al [17] anticipated Flooding Factor based Framework for Trust Management (F3TM) in MANETs. True flooding methodology is used to recognize faulty nodes. Here optimised path is established to deliver the packets. Chen et al proposed [18] proposed protocol for increasing network capacity which is useful for large networks.

Hu et al [19] proposed novel algorithm that can avoid the two problems to construct bandwidth-satisfied multicast trees for QoS applications. Furthermore, it also aims at minimizing the number of forwarders so as to reduce bandwidth and power consumption. Simulation results show that the proposed algorithm can improve the network throughput.Biradar et al [20] proposed an agent-based multicast routing scheme that builds a backbone in the form of a reliable ring and finds multicast routes. The reliability is modelled by using probabilistic measure of link failures.

Wang [21] introduced a power-aware multicast routing protocol where nodes are categorised into groups which yields load balance. Results showbetter performance than multicast ad hoc on-demand distance vector routing protocol (MAODV), Reliability of the multicast ad hoc on-demand distance vector (RMAODV) and Parallel multiple nearly-disjoint trees multicast routing (Parallel MNTMR) schemes. M.Vijayalakshmi

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

[22] proposed Link stability based priority multicast ad hoc on demand routing protocol (LSPMAODV) where links with long life time are found and are used for forwarding packets. Raja shekhar C. Biradar, Sunil kumar S. Manvi[23] proposed routing scheme based on Information Priority (IPMRM) where reliability pair factor is computed considering power level and signal strength between nodes.

III. QOS AWARE MULTICAST ROUTING

In this work, multicast routing is guaranteed by establishing the multiple route paths to the multiple destinations with the concern of energy conservation. Initially multipath route computation would be done with the guaranteed QoS parameters increased energy and bandwidth to reach the destination node. Then reliability pair factor is measure between the neighbouring nodes involved in the multiple paths that are established. Here the Pruning neighbour nodes that have reliability pair factor lesser than a threshold is done. Finally unique key for each node would be generated from which data to be transmitted which is then transmitted to their corresponding destinations.

3.1. CLUSTERING AND CLUSTER HEAD SELECTION USING MODIFIED FIREFLY ALGORITHM

The Modified FireFly (MFF) algorithm is used for selecting the cluster head and forming clusters in wireless sensor network. The main parameters considered in the MFF algorithm for selecting the cluster head is node position, residual energy and available bandwidth. These parameters are used to calculate the weight of each and every node in the network using iteration. Here fitness evaluation is calculated by using Fuzzy Topsisinstead of weighted sum method in the firefly algorithm. Thus, the modified firefly algorithm will give better and accurate prediction than the traditional firefly algorithm.

Firefly Algorithm (FA) is a metaheuristic algorithm for global optimization.In 2008 Xin-She Yang proposed this algorithm. Fireflies use the flashing behaviour to attract other fireflies. Brightness defines the attractiveness. Less bright firefly will be attracted by highly brighter one. Usually in multi-objective optimization, performance increase of one objective function may degrade the performance of another objective function. So achieving optimal solution is one of the greatest challenges, hence tradeoff treatment is needed in order to make a balanced optimization. In this paper, concept of fuzzy TOPSIS is used for this purpose.

Peer-to-Peer network can be considered in the form of a graph. Value of x and y coordinates of graph are used to represent the location of every node. Unique node number is given to all the nodes. If two nodes, Euclidian distance is within each other's range ,then they are said to be in range of each other. Here clustering based hierarchical routing is done to reduce overhead. Cluster head with minimal set are computed by MFF. Local solution corresponds to an output and it an iterative process. The flow chart for the Modified firefly algorithm is given below:

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

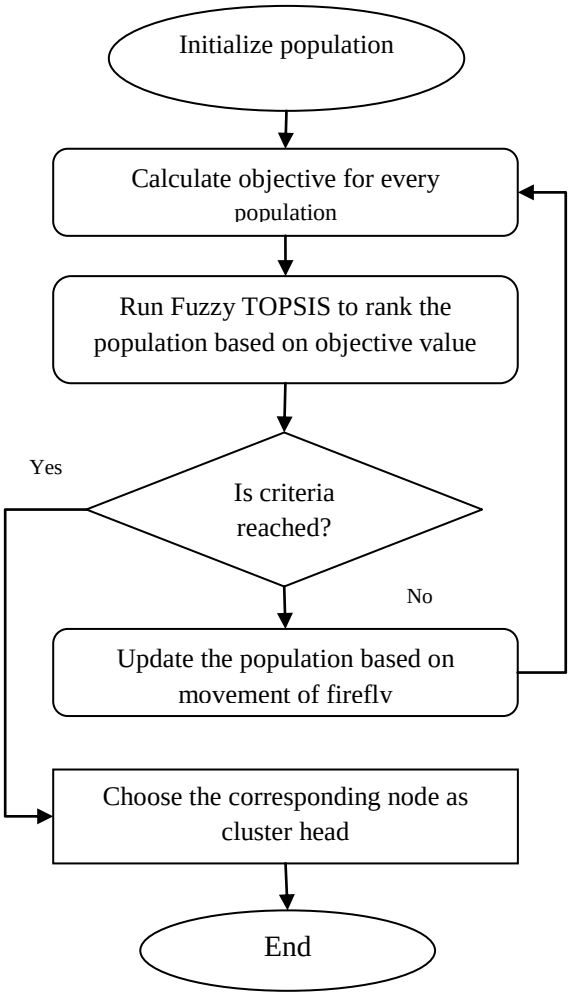

Fig.1. Flowchart of modified firefly algorithm

3.2. RELIABILITY PAIR FACTOR ESTIMATION

Two connected nodes are designated as reliable by means of Reliability pair factor (F_{RP}).F_{RP} gives the link connectivity status. In order to compute F_{RP}, let us assume F as the full battery capacity of a node, then remaining battery power of node iat time t ($W_t^{rem}(t)$) is given by Eq. 1

If Node's full battery capacity is assumed as F for the computation of F_{RP}. At time t, node I's remaining battery power ($W_t^{rem}(t)$) is expressed as,

$$W_t^{rem}(t) = W_t^{rem}(t-1) - P \times B(t-1,t) - P_I(t-1,t) \quad (1)$$

Where, power required to transmit a bit is represented as P , number of bits transmitted from time t−1 to t is represented as B(t−1, t), power required to perform node i's internal operations for duration t to t –1 is represented as P_I(t−1, t).

$$\text{At } t = 0,\ W_t^{rem}(t) = F \quad (2)$$

Equation (2) defines power ratio. Based on this $W_t^{rem}(t)$ lies in two ranges.

$$\text{Power ratio} = \frac{W_t^{rem}(t)}{F} \quad (3)$$

Node I's, $W_t^{rem}(t)$ will be in low range or in high range as expressed in equation (4)

$$W_i^{rem}(t) = \begin{cases} \text{Low range} & \text{if } 0 < Power\ ratio < 0.1 \\ \text{H igh range} & \text{if } 0.1 < Power\ ratio \leq 1 \end{cases} \quad (4)$$

Reliability pair node's status of connectivity and power of transmission is decided by node I's $W_i^{rem}(t)$range. Coordinate values (x1, y1) gives the initial position of node i and Coordinate values (x2, y2)gives the initial position of node j. $d_{(ij,0)}$represents the distance between node i and j at time 0. $d_{(ij,t)}$represents the distance between node i and j at time t, where nodes are moved to a

TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

new positions.

Between nodes iand j, FRP defines the packets successful transmission. This value is directly proportional to differential signal strength (D_S) and minimum remaining battery power level of either nodes (W_i^{rem}, W_j^{rem}) and it is inversely proportional to distance between nodes ($d_{(ij,0)}$, $d_{(ij,t)}$). Equation (5) gives, the value of FRP at T=0.

$$F_{RP} = K\frac{\text{Min}\left(W_i^{rem}, W_j^{rem}\right)+D_s}{d_{(ij,0)}} \quad (5)$$

Where, proportionality constant is given by K. In equation (4),$d_{(ij,t)}$ is used to replace $d_{(ij,0)}$ in order to find F_{RP} at T=t.

F_{RP} measured by using the equation 5 is used to predict the reliability pair factor of nodes. Nodes with higher F_{RP} will be defined as nodes with increased reliability pair factor which cannot be pruned. These nodes have greater role in the successful packet transmission. However nodes with lesser F_{RP} are considered to have low reliability pair factor. These cannot be considered for the data transmission; hence they need to be pruned.

3.3. NODE PRUNING USING CUCKOO BASED OPTIMIZED MULTI LAYER FEED FORWARD NEURAL NETWORK

In this work Node pruning is done by using cuckoo based optimized multilayer feed forward neural network. Here nodes having lesser reliability pair factor and lesser threshold are eliminated using cuckoo based optimized multilayer feed forward neural network.

Back-propagation learning algorithm is used to train the MLF neural network. Neurons are contained by MLF neural network. Layers are used to order them. Input layer is a first layer and output layer is a last layer and hidden layer corresponds to a layer between them. Mapping function Γ is used to describe the neurons formally. For given neuron i, subset $\Gamma(i) \subseteq V$ is assigned by mapping function and all predecessors are contained by this subset. Every neuron in a layer is connected to all the neurons in next layer.

A subset $\Gamma^{-1}(i) \subseteq V$ than consists of all predecessors of the given neuron i. Each neuron in a particular layer is connected with all neurons in the next layer. Threshold coefficient ϑ_i is used to characterize ith neuron and weight coefficient $w_{ij}$is used to characterize the connection between jth and ith neuron. In neural network, connection's importance is reflected by weight coefficient. Equation (1) and (2) is used to compute the ith neuron x_i's output value.

$$x_i = f(\xi_i) \quad (6)$$

$$\xi_i = \vartheta_i + \sum_{j\in\Gamma_i^{-1}} w_{ij}x_j \quad (7)$$

Where, potential of ith neuron is represented as $v\xi_i$ and transfer function is represented as functionf(ξ_i). With formally added neuron j, connection's weight coefficient corresponds to threshold coefficient, where $x_j = 1$. Following holds for transfer function,

$$f(\xi) = \frac{1}{1+\exp(-\xi)} \quad (8)$$

Sum of squared difference between required and computed output is minimized by varying weight and threshold coefficients by the process of supervised adaptation. Objective function E is minimized to accomplish this:

$$E = \sum_o \frac{1}{2}(x_0 - \hat{x}_0)^2 \quad (9)$$

Where, vectors composed of computed activities of output neurons is represented as x_0 and required activities of output neurons is represented as $\hat{x}_0$and all output neurons o are summarized.

In MLF neural network, learning parameters corresponds to weight coefficient $w_{ij}$and and threshold coefficientϑ_i. Sum of squared difference between required and computed output is minimized by varying weight and threshold coefficients by the process of supervised adaptation.Thusϑ_i and w_{ij}values needs to be chosen and adjusted with more concern for the increased performance efficiency. These values are chosen optimally in this work by using cuckoo search algorithm. In nests of other host birds, eggs

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

are laid by cuckoo species. This behaviour is used to form a CS algorithm. Direct conflict is engaged by few host birds with intruding cuckoos. Eggs are thrown away or new nest are formed by host bird, it other eggs are discovered by it. Following representations are used in Cuckoo search (CS).

Solution is represented by a nest eggs and new solution is represented by a cuckoo eggs. In nests, not-so-good solutions are replaced by a new as well as a better solution. Every nest is going to have one egg. Set of solutions for a complicated case can be represented by a nest with multiple eggs.

Three idealized rules form the base of CS:

1. In a nest which is chosen randomly, one egg is laid by every cuckoo and dumps it in a time.
2. For next generation, carry over the best nests having eggs with high quality.
3. Fix the number host nest available. With a probability $p_a \in (0,1)$, host bird discovers the egg laid by cuckoo. Few worst nests set is used for discovering. From farther computations, dump the discovered solutions.

MLP algorithm is used for pruning the nodes. In MLP algorithm, threshold coefficient and weight coefficient are important parameters which plays an important role in attaining final solution. In this work, cuckoo search algorithm is utilized for choosing the optimal values for the threshold coefficient and weight coefficient values. In cuckoo search algorithm, nest is considered as optimal valuesof threshold coefficient and weight coefficient. Cuckoo search algorithm will find out the optimal nest for each cuckoo egg to lay of their egg. That is optimal value of threshold coefficient and weight coefficient will be identified for the optimal MLF outcome. Here fitness value of cuckoo search algorithm is taken as error value obtained in the MLF algorithm. Thus cuckoo search algorithm will select the most optimal value for which lesser error rate is obtained.

3.4. NODE AUTHENTICATION AND SECURE DATA TRANSMISSION

To ensure the secured data transmission and successful authentication, in this work unique secret keys are generated for each cluster members to perform authentication to the cluster head node. Whenever the new node established it will send REQ packet to the cluster head for generating the secret keys. The REQ packet format is given below:

$$REQ = \{Source=ClusterMember, Destination=ClusterHead, CMI||R_0||MAC(K_{SS}, monitoring\ node||CMI||R_0)\}$$

Where source ➔ ClusterMember address
Destination ➔ ClusterHead address
CMI ➔ClusterMember identifier
R_0➔Random value
MAC ➔Message authentication code
K_{SS} ➔ Shared secret key

Upon reception of this REQ packet, ClusterHead will check pruned node lists to analyse whether the corresponding ClusterMember already present in pruned list or not. If it is present, then this packet will omitted. If not then ClusterHead will analyse the MAC and will create the session key K_S. The format of session key is given below

$$K_S = H(K_{SS}, ClusterMember||R_0||R_l)$$

Where
H ➔ one way hash function
R_l➔ random value generated by ClusterHead

After generation of this session key, successful acknowledgement (SucAck) will send back to the sink node along with session key K_S. The packet format of SucAck is given below

$$SucAck = \{Source=ClusterHead, Destination=Sink, E(K_{SS}, ClusterMember||R_0||R_l||K_S)\}$$

Where
E ➔ Encryption method
K_{SS} ➔shared secret key

Upon reception of this SucACk, sink node will extract the session by encrypting it and this

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

information will be send back to the ClusterMember.

Alert = {Source=Sink, Destination=ClusterMember, $R_0||R_l||MAC (K_S, Sink||ClusterMember||R_0||R_l)$}

This information will be utilised for authentication with the most recent session key received from the ClusterHead.

The overall processing flow of this authentication is given in the following figure 1.

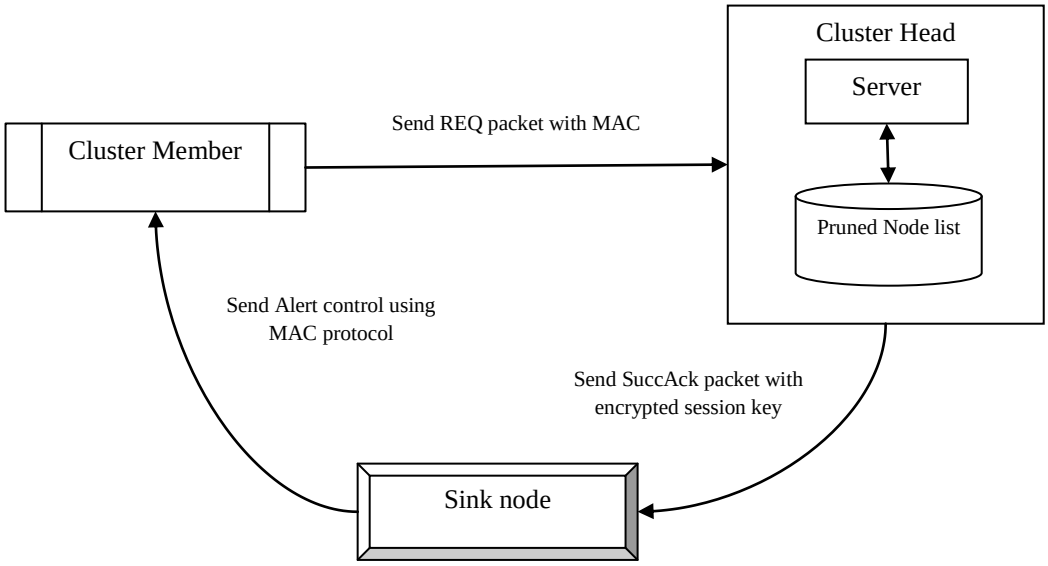

Fig.2. Overall flow of Authentication Process

3.5. MULTI CAST ROUTING

In a route, every link will have probability of success and it depends on individual probabilities at each link in route. Probability of entire route from source to destination is computed by using this computed RPF. At every link, product of individual probabilities corresponds to a route probability. Computed probability value is stored by every node for this purpose. At 1-second interval, every node generates and broadcast the HELLO packets to 1-hop neighbour node.

Equation (5) is used to compute the every link's probability, before transmitting join query. For pre-set interval of time, join query is buffered by every receiver node. Probability of previous hop is multiplied with current node link's probability after the completion. The steps involved are given below.

1. At time interval of 1 second, HELLO packets are generated and send by every node.
2. At every node, count the reception of HELLO packets. Equation (5) is used to compute the probability. In Data_HELLO, with address of sender, this probability is stored.
3. JOIN QUERY is created and broadcasted by source node.
4. QUERY is received and checked by intermediate node, Discard the QUERY if it is duplicated.
5. Timer is set by every node, if it is not a duplicate one. QUERY is buffered In Msg_Cache, sequence number, last address, source address of QUERY is stored.
6. At every node, extract partial route's probability, after exceeding buffer time. Compute current node to partial route up's overall probability.
7. Select partial route having maximum probability at receiver node. At current node, this probability value is stored.
8. If two or more nodes have same probability, consider First received QUERY.
9. Broadcast JOIN QUERY till it reaches final intended receiver.

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

10. After route selection, JOIN REPLY is created and unicasted by final receiver.

IV. RESULTS AND DISCUSSION

In this subsection, different performance metrics are analysed for both proposed and existing protocols PN-SEMRP, IPMRM and LSPMAODV. In this work, Sybilattack and Black hole attack is considered to check the robustness of protocols and prevention against the attack is ensured with the help of keying mechanism adapted.

.

Table 1
Packet delivery ratio comparison(Sybil attack)

Attackers	Packet delivery ratio		
	LSPMAODV	IPMRM	PN-SEMRP
2	0.8845	0.9001	0.959
4	0.91	0.9318	0.9891
6	0.929	0.942	0.9999
8	0.9295	0.9521	0.9999
10	0.9396	0.9556	1

Table 2
Packet delivery ratio comparison(Blackhole attack)

Attackers	Packet delivery ratio		
	LSPMAODV	IPMRM	PN-SEMRP
2	0.8964	0.8998	0.9599
4	0.9256	0.9379	0.9698
6	0.9341	0.9397	0.9895
8	0.9478	0.9677	0.9897
10	0.9521	0.9725	0.9999

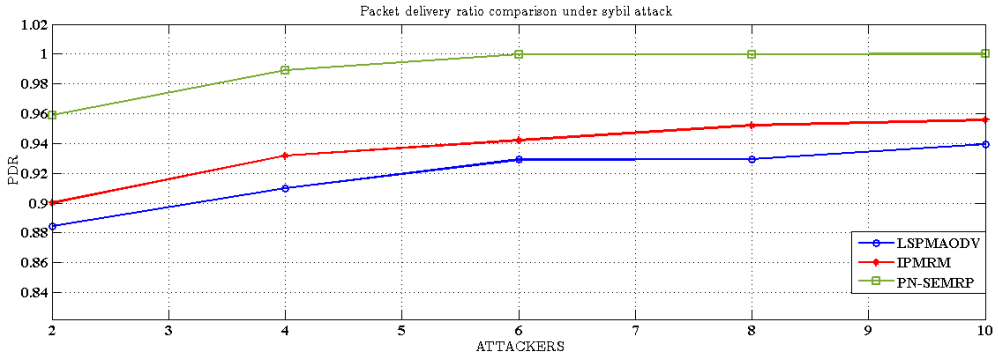

Fig.3.Packet delivery ratio comparison among various protocols (Sybil attack)

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

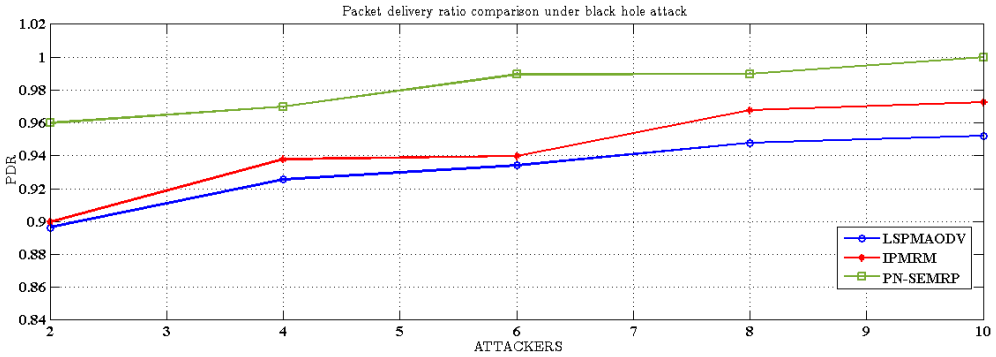

Fig.4.Packet delivery ratio comparison among various protocols (Black hole attack)

As shown in Figure 3 and Figure 4 the Packet delivery ratio increases with the rise of multicast receivers due to more paths. PN-SEMRP achieves a higher PDR as compared to IPMRM and LSPMAODV because of optimal cluster head selection. Parameters like power, delay, and bandwidth are properly managed while establishing the stable multicast routes. Thus, the PDR of PN-SEMRP is higher than that of IPMRM and LSPMAODV. Table 1 and Table 2 shows PDR values under sybil and black hole attacks respectively. Nodeauthentication performed in this work reduces the security threats and also increases the packet delivery ratio.

Delay

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

Table 3
Delay comparison(Sybil attack)

Attackers	**Delay (ms)**		
	LSPMAODV	**IPMRM**	**PN-SEMRP**
2	0.51	0.488	0.41
4	0.5512	0.542	0.385
6	0.5578	0.514	0.32
8	0.5675	0.5369	0.315
10	0.567	0.5345	0.302

Table 4
Delay comparison(Black hole attack)

Attackers	**Delay (ms)**		
	LSPMAODV	**IPMRM**	**PN-SEMRP**
2	0.525	0.517	0.394
4	0.541	0.532	0.405
6	0.579	0.556	0.467
8	0.581	0.577	0.472
10	0.589	0.578	0.342

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

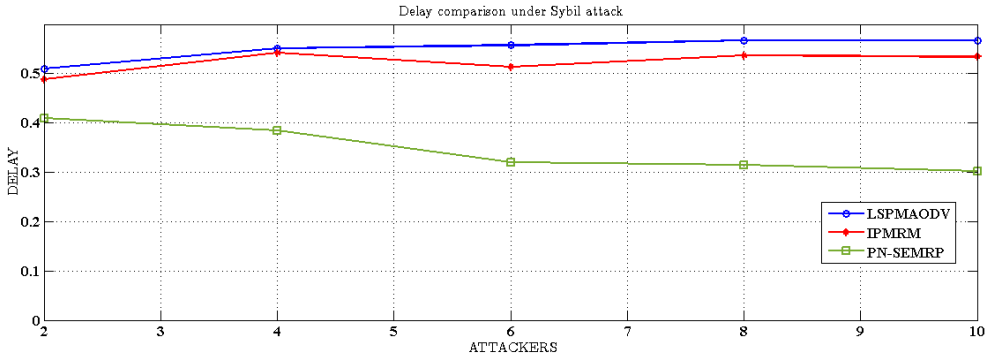

Fig. 5.Delay comparison among various protocols (Sybil attack)

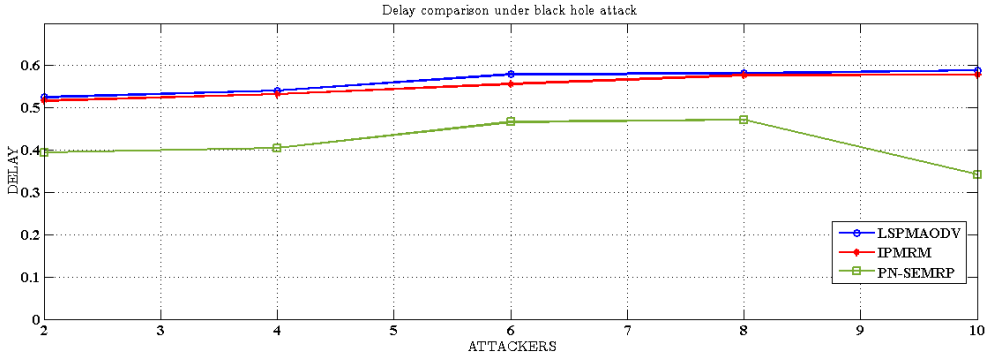

Fig.6. Delaycomparisons among various protocols (Black attack)

Table 3 and 4 shows delay values under sybil and black hole attacks respectively. From Figure 5 and Figure 6 we see that the delay of proposed protocol PN-SEMRP is lesser than IPMRM and LSPMAODV under sybil and black hole attacks. PN-SEMRP achieves lesser delay by pruning the unreliable nodes from the network before route path establishment, thus the successful packet transmission can be achieved with reduced delay value. Multicast routing adapted in this work also leads to reduced delay.

Throughput

Throughput is defined as an amount of data moved successfully from one place to another in a given time period.

Throughput = Number of packets moved / Simulation time

.

Table 5

Throughput comparison(Sybil attack)

Attackers	**Throughput (kbps)**		
	LSPMAODV	**IPMRM**	**PN-SEMRP**
2	165	178.2	223.3
4	169.8	179.8	249.3
6	172.5	182.5	252.1
8	177	183.6	255.75
10	185	186.7	259.74

Table 6
Throughput comparison (Black hole attack)

Attackers	Throughput (kbps)		
	LSPMAODV	IPMRM	PN-SEMRP
2	151	167	211
4	157	173	252
6	169	179	277
8	181	193	296
10	186	201	305

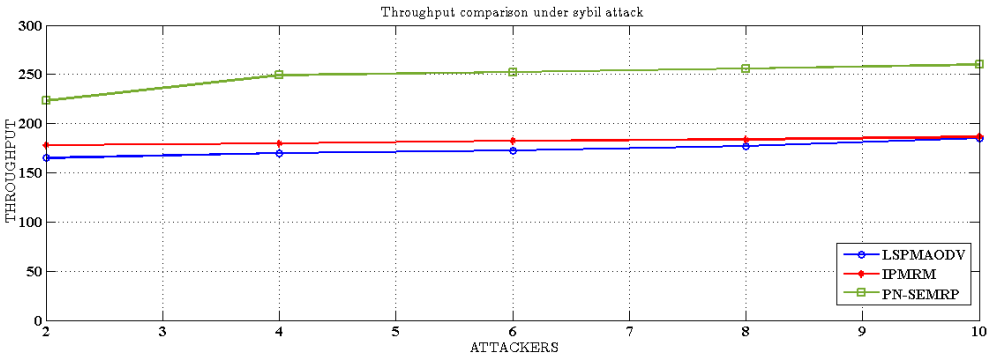

Fig.7.Throughput comparison among various protocols (Sybil attack)

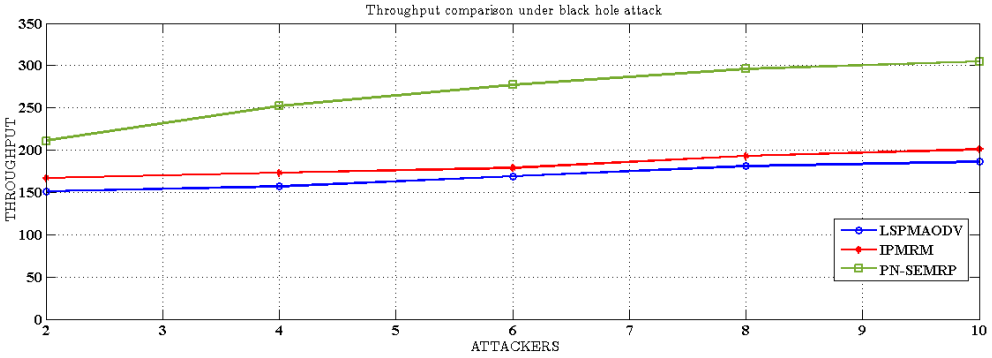

Fig.8. Throughput comparison among various protocols (Black hole attack)

From above figures it can be concluded that the proposed method PN-SEMRP achieves higher throughput of 259 and 305 kbps for 10 number ofsybil and black hole attacks respectively.Existing methods such as LSPMAODV and IPMRM provides higher throughput values. The plot shows that the proposed protocol attained high throughput compared than other protocols due to the effectual cluster head selection and authentication. With the presence of attackers reliable data transmission might get affected which leads to reduced throughput, however in this work throughput of the proposed method is increased considerably even in the presence of attackers due to security method incorporated.

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

Table 7
Overhead comparison (Sybil attack)

Attackers	Overhead		
	LSPMAODV	IPMRM	PN-SEMRP
2	2.26	2.05	1.11
4	2.75	2.16	1.22
6	2.83	2.46	1.25
8	2.99	2.51	1.35
10	3.01	2.65	1.47

Table 8
Overhead comparison (Black hole attack)

Attackers	Overhead		
	LSPMAODV	IPMRM	PN-SEMRP
2	2.15	1.98	1.51
4	2.32	2.18	1.65
6	2.51	2.35	1.76
8	2.67	2.52	1.81
10	2.75	2.82	1.99

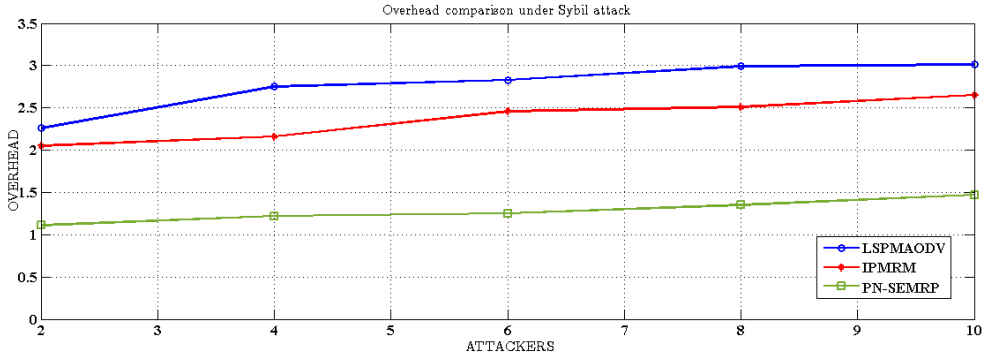

Fig.9. Overhead comparison among various protocols (Sybil attack)

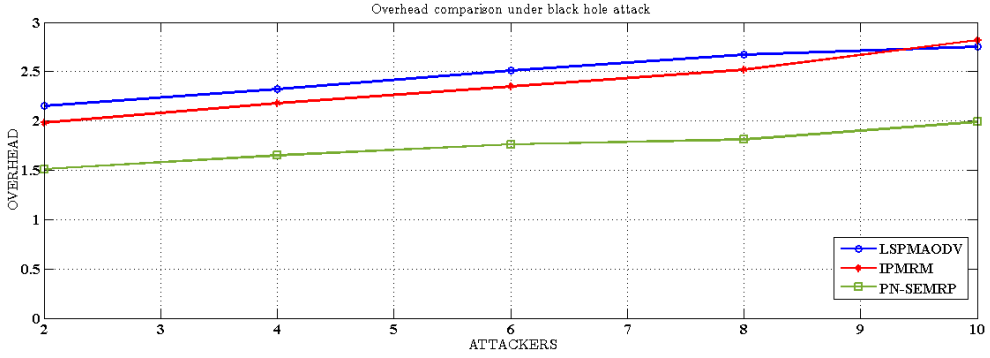

Fig.10. Overhead comparison among various protocols (Black hole attack)

When number of nodes increases or when the number of attackers increase overhead usually will increase. From Figure 9 and Figure10, we see that that the proposed method PN-SEMRP achieves lesser overhead of 1.47 and 1.99 for 10 number ofsybil and black hole attacks.Existing methods

such as LSPMAODV and IPMRM provides higher overhead. The overhead of the proposed method is considerably reduced by managing the data transmission and security mechanism by centralized node instead of separating it to the multiple nodes.

Table 9
Packet delivery Ratio

Data Rate	Packet delivery Ratio (PDR)		
	LSPMAODV	IPMRM	PN-SEMRP
128	0.8574	0.8826	0.989
256	0.8926	0.8951	1.1341
512	0.8999	0.9156	0.9999
1024	0.9105	0.9178	1.0034
2048	0.9178	0.9258	1.1023

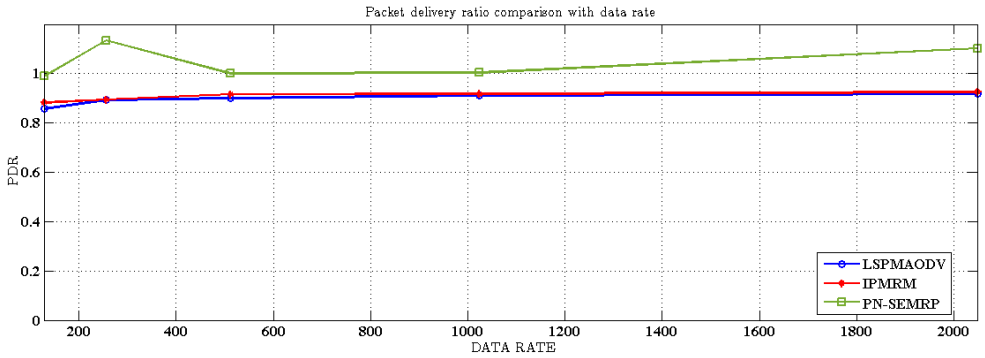

Fig.11. Packet delivery ratio comparison among various protocols

As shown in Figure 11 the PDR increase with the data rate. The proposed protocol PN-SEMRP outperforms LSPMAODV and IPMRM in terms of PDR with data rate, the proposed PN-SEMRP algorithm provides higher PDR results of 1.1 for 2048 bytes, whereas LSPMAODV and IPMRM provides lesser PDR of 0.9178 and 0.9258 for 2048 data rate respectively.

Table10
Delay

Data rate	Delay (ms)		
	LSPMAODV	IPMRM	PN-SEMRP
128	0.5126	0.4568	0.219
256	0.6123	0.5996	0.2834
512	0.6845	0.6785	0.3856
1024	0.7426	0.7356	0.4912
2048	0.8156	0.7936	0.5001

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

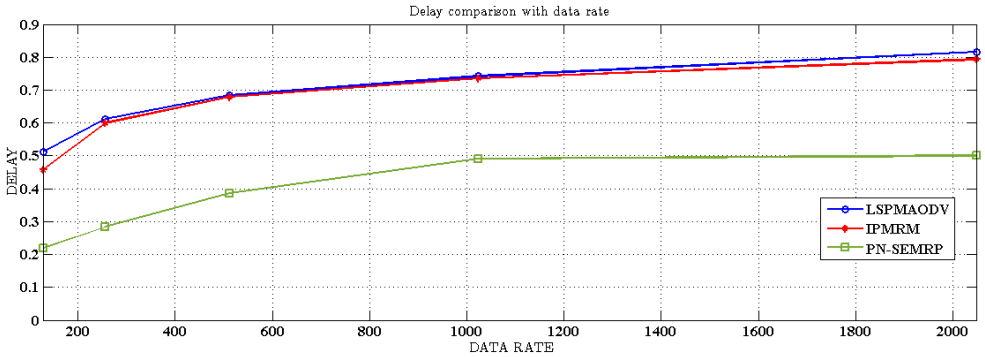

Fig.12.Delay comparison among various protocols

As shown in Figure 12 the delay increases with the data rate. The proposed protocol (PN-SEMRP) outperforms both LSPMAODV and IPMRM in terms of delay. The proposed PN-SEMRP algorithm provides lesser delay results of 0.5001ms for 2048 data rate, whereas LSPMAODV and IPMRM provide higher delay of 0.8156 and 0.7936msrespectively. Effective cluster head mechanism and node pruning performed in the proposed method leads to reduced delay value even in case of increased data rate.

Table 11
Packet delivery ratio

Speed	Packet delivery ratio		
	LSPMAODV	IPMRM	PN-SEMRP
2	0.8565	0.8965	0.989
4	0.8975	0.9125	0.9912
6	0.8988	0.9156	0.9901
8	0.9126	0.9198	0.9901
10	0.9259	0.9256	0.9979

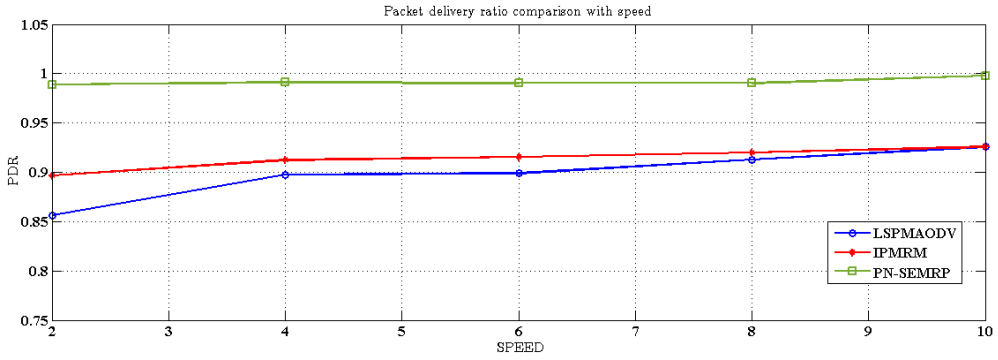

Fig.13.Packet delivery ratio comparison among various protocols (speed)

As shown in Fig. 13 the PDR increase with the speed (nodes mobility). The proposed protocol PN-SEMRP shows good performance when compared to LSPMAODV and IPMRM in terms of PDR with speed, the proposed algorithm provides higher PDR results of 0.99 for 10 speed, whereas LSPMAODV and IPMRM provides lesser PDR of 0.9259 and 0.9256 respectively.

Table 12
Delay comparison values

Speed	Delay(ms)		
	LSPMAODV	IPMRM	PN-SEMRP
2	0.15	0.095	0.012
4	0.17	0.0952	0.044
6	0.189	0.152	0.089
8	0.452	0.356	0.1
10	0.489	0.419	0.215

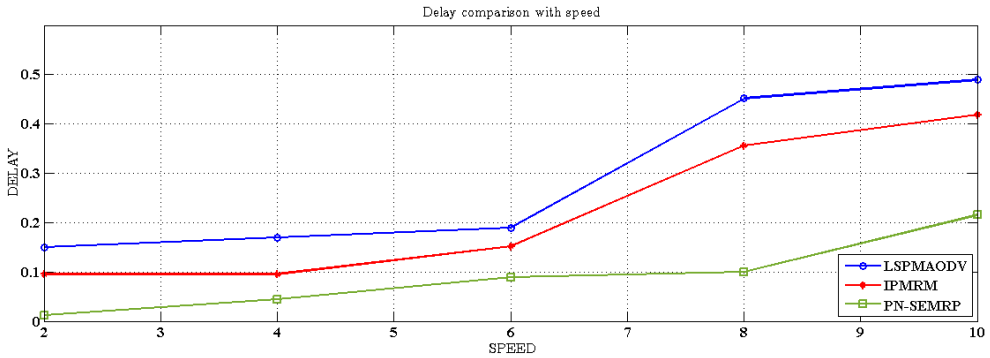

Fig.14.Delay comparison among various protocols

Above Figure 14 shows the delay comparison with respect to increased speed.The proposed protocol PN-SEMRPoutperforms compared LSPMAODV and IPMRM in terms of delay with speed. The proposed PN-SEMRP algorithm provides lesser delay results of 0.215 ms for 10 m/s, whereas LPMAODV and IPMRM provide higher delay of 0.489 and 0.419 msrespectively. Pruning technique adopted here has reduced unreliable nodes present in the environment which in turn reduced delay even with increased speed.

Table 13
Latency

Speed	Latency(Seconds)		
	LSPMAODV	IPMRM	PN-SEMRP
2	0.078	0.065	0.031
4	0.082	0.069	0.043
6	0.087	0.075	0.045
8	0.092	0.078	0.0532
10	0.099	0.087	0.061

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

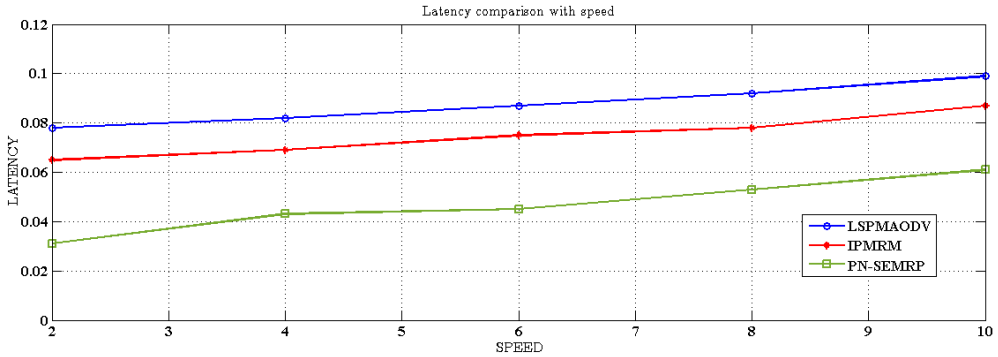

Fig.15.Latency comparison among various protocols (speed)

In Figure 15, comparison evaluation of the proposed and existing methods in terms of latency is given. From this numericalevaluation it is confirmed that the proposed method gives lesser latency of 0.061 whereas LSPMAODV and IPMRM provide higher latency of 0.0925 and 0.085 ms respectively. Latency of the proposed research technique is reduced considerably with increase in speed.

Table 14
Residual energy with number of nodes

No of nodes	Residual energy		
	LSPMAODV	IPMRM	PN-SEMRP
100	90.2	91.2	96.3
200	89.6	90.6	95.7
300	88.2	90	95
400	86.8	87.4	93.4
500	84.3	87.2	92.5

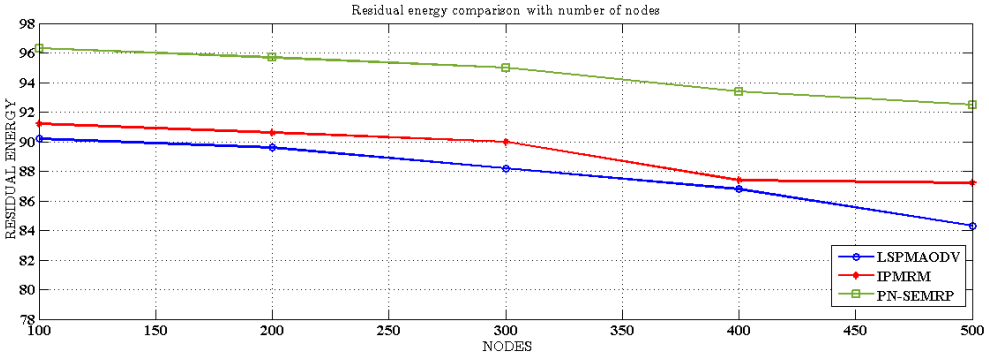

Fig.16.Residual energy comparison among various protocols with increase in nodes

Table 15
Residual energy with time

Time	Residual energy		
	LSPMAODV	IPMRM	PN-SEMRP
20	94.5	95.8	98.8
40	92.8	94	95.9

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

60	92.6	92.8	95.2
80	91.3	91.5	93.7
100	89	89.1	92.3

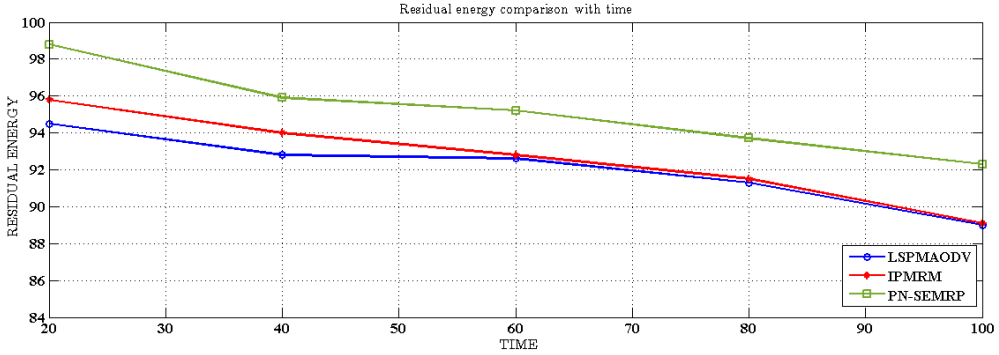

Fig.17. Residual energy comparison among various protocols with Time

From Figure16 and Figure 17 it is evident that when number of nodes and time are increased residual energy is decreased. Proposed routing method shows better results when compared to other because of proper energy management and clustering mechanism incorporated.

V. CONCLUSION

In this paper we proposed pruning nodes based stable and efficient multicast routing protocol (PN-SEMRP).The proposed routing mechanism provides successful data transmission with reduced delay and increased packet delivery ratio. The reliable and successful packet delivery is achieved by introducing the pruning technique and keying mechanism which will eliminate unreliable nodes from the environment. The common security attacks associated with multicast routing are taken care by introducing unique key based authentication method. The overall framework of this research tends to achieve increased packet delivery ratio with reduced delay and latency when compared to existing methods.

VI. REFERENCES

[1]. Dong, C., Qu, Y., Dai, H., Guo, S., & Wu, Q. (2018). Multicast in multi-channel cognitive radio ad hoc networks: Challenges and research aspects. Computer Communications.

[2]. Yadav, A. K., &Soni, S. (2017). Secure multicast key distribution in mobile and adhoc networks. Adv. Wirel. Commun, 10(4), 781-782.

[3]. Nyrkov, A. P., Belousov, A. S., &Sokolov, S. S. (2015). Algorithmic support of optimization of multicast data transmission in networks with dynamic routing. Modern Applied Science, 9(5), 162.

[4]. Bacthu, N., Chippa, A., Grover, H., Sivaramu, R., &Farinacci, D. (2017). U.S. Patent No. 9,736,054. Washington, DC: U.S. Patent and Trademark Office.

[5]. Montalban, J., Scopelliti, P., Fadda, M., Iradier, E., Desogus, C., Angueira, P., ...&Araniti, G. (2018). Multimedia multicast services in 5G networks: Subgrouping and non-orthogonal multiple access techniques. IEEE Communications Magazine, 56(3), 91-95.

[6]. Rump, F., Jopen, S. A., & Frank, M. (2016, November). Using probabilistic multipath routing to improve route stability in MANETs. In 2016 IEEE 41st conference on local computer networks (LCN) (pp. 192-195). IEEE.

[7]. Qiu, T., Chen, N., Li, K., Qiao, D., & Fu, Z. (2017). Heterogeneous ad hoc networks: Architectures, advances and challenges. Ad Hoc Networks, 55, 143-152.

[8]. Bongyong, S. O. N. G., Ananthanarayanan, A., & Gill, H. (2016). U.S. Patent No. 9,313,620. Washington, DC: U.S. Patent and Trademark Office.

[9]. Jackson, D. L., Hansen, R. A., & Smith, A. H. (2018). Multicast delivery of IPTV over the

January - February 2020
ISSN: 0193 - 4120 Page No. 3260 - 3277

Internet. GSTF Journal on Computing (JoC), 1(1).

[10]. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), 1250-1258.

[11]. Madhusudhanan, B., Chitra, S., &Rajan, C. (2015). Mobility based key management technique for multicast security in mobile ad hoc networks. The Scientific World Journal, 2015.

[12]. Nazir, M. K., Rehman, R. U., &Nazir, A. (2016). A novel review on security and routing protocols in MANET. Communications and Network, 8(04), 205.

[13]. Lu, T., Chang, S., Guo, W., & Huang, Q. (2017). Genetic algorithm for energy-aware QoS multicast routing in manets. Computer, 5(1), 10-20.

[14]. Garcia-Luna-Aceves, J. J., &Menchaca-Mendez, R. (2011). PRIME: An interest-driven approach to integrated unicast and multicast routing in MANETs. IEEE/ACM Transactions On Networking, 19(6), 1573-1586.

[15]. Gaurav Singal, Vijay Laxmi, M.S. Gaur, Swati Todi, Vijay Rao, MeenakshiTripathi, RitiKushwaha, Multi-constraints Link Stable Multicast Routing Protocol in MANETs, *Ad Hoc Networks* (2017), doi: 10.1016/j.adhoc.2017.05.007

[16]. Viswanath, K., Obraczka, K., &Tsudik, G. (2005). Exploring mesh and tree-based multicast. Routing protocols for MANETs. IEEE Transactions on mobile computing, 5(1), 28-42.

[17]. Ahmed, M. N., Abdullah, A. H., Chizari, H., &Kaiwartya, O. (2017). F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs. *Journal of King Saud University-Computer and Information Sciences*, *29*(3), 269-280.

[18]. Chen, Y. H., Hu, C. C., Wu, E. H. K., Chuang, S. M., & Chen, G. H. (2017). A delay-sensitive multicast protocol for network capacity enhancement in multirate MANETs. IEEE Systems Journal, 12(1), 926-937.

[19]. Hu, C. C., Wu, H., & Chen, G. H. (2008). Bandwidth-satisfied multicast trees in MANETs. IEEE Transactions on Mobile Computing, 7(6), 712-723.

[20]. Biradar, R. C., &Manvi, S. S. (2011). Agent-driven backbone ring-based reliable multicast routing in mobile ad hoc networks. IET communications, 5(2), 172-189.

[21]. Wang, N. C. (2012). Power-aware dual-tree-based multicast routing protocol for mobile ad hoc networks. IET communications, 6(7), 724-732.

[22]. M.Vijayalakshmi, Dr D Sreenivasa Rao "Cluster based Multicast Adhoc on Demand Routing protocol for increasing link stability in Manets" Global Journal of Computer science and Technology(E) Vol XVII Issue 11, 2017.

[23]. Raja shekhar C. Biradar, Sunil kumar S. Manvi "Information Priority based Multicast Routing in Manets"International Journal of Wireless and Mobile Networks(IJWMN) Vol 3 No3, June 2011.

[24]. Joshua Reginald Pullagura and Dr.D.Venkata Rao, "Simulation based Comparison of Vampire attacks on Traditional Manet routing Protocols" Information and Communication Technology for Sustainable Development, Springer Lecture Notes in Networks and Systems, 2017, DOI: /10.1007/978-981-10-3932-4_52501.