Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/120217

Trust Based Cluster-Energy Efficient Multicast Routing In Mobile Adhoc Networks

S. Baskaran[1,2,*], *J. Arputha Vijaya Selvi*[3] *and V. R. Sarma Dhulipala*[4]

[1] Department of CSE, VELS Institute of Science Technology & Advanced Studies, (VISTAS), Chennai, India.
[2] Department of CSE, Kuppam Engineering College, Andra Pradesh, India
[3] Department of ECE, Kings College of Engineering, Pudukkottai, Tamilnadu, India.
[4] Department of Physics, University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, Tamilnadu, India.

Abstract: MANET is a set of wireless communication module practiced globally for well-established networking. MANETS are largely utilized as a part of networking and used by large network users all over the world. These network communication utilize hubs for interconnection and consume large capacity of energy for processing. The consumption and protection of networking in MANET have been researched for the recent couple of years. Somehow the researches for limiting the resources has been explored to some level. The most challenging assignment is the security issues in MANETS. The adaptation of harmful elements can affect the system and its associated consumer which prompts problems in communication. The main objective of this research paper is to give optimal security and energy consumption during routing of the network nodes. This paper proposes a cluster based routing strategy to give optimal security and energy consumption during networking. The fuzzy k-means clustering is induced to cluster the network into same cluster heads. During routing the cluster, heads finds the optimal path to transmit data with a minimal energy. The proposed routing protocol is a trust based on demand multicast routing which gives optimal security by securing the transmission of data during routing. The proposed protocol is modeled and experimented in the Network Simulator 2, and the performance of the routing protocol proposed in this paper are evaluated with the existing approaches in terms of quality of service (QoS) and energy efficiency. From the analyzed results, it shows that the proposed protocol is an efficient routing strategy offering optimal security and energy efficiency in mobile adhoc networks

Keywords: Manet, Fuzzy K-Means Clustering, Multicast Routing, Network Simulator, Quality of Service (QoS)

1 Introduction

Over the most recent couple of years, the efficiency of wireless communication has expanded colossally by opening new fields of use in the area of systems networking. One of such field's concerns mobile adhoc networks systems (Manets) in which portable hubs compose themselves in a system without the assistance of any predefined foundation [1]. Manet is choosing up prevalence due to the convenience of ease cell phones and its capacity to give moment remote systems administration abilities where execution of wired system is impractical or exorbitant. Manets is a remote correspondence innovation. This enables individuals to impart, and it does not have a settled framework as the clients are persistently moving. The Adhoc network handles the system by control, i.e. to set up a network and so on [2]. Every hub is being able to assemble a network by finding the hub to communicate and share the information using radio waves. Manets are defenseless against different sorts of assault as a result of its elements like perpetual evolving topology, resource imperatives and inaccessibility of any brought together the infrastructure. Manet have specific security issues which won't be settled by another security instrument as a result of some issue. Trust control is vital because the foreordained conduct of hub can stay away from any additional harmful interchanges and let the reliable hubs impart quickly [3].

Due to the unsteady expansion of wireless communication utilization in the coming recent years, from satellite to personal wireless area networks [4]. Customarily, security requirements should not be setting delicate as registering existed inside a static situation. Nonetheless, as registering innovation turns out to be increasingly coordinated into a regular daily existence. It is essential that security components turn out to be more

* Corresponding author e-mail: yes.baskaran@outlook.com

adaptable and less interfering. In a perfect situation, a Manet should self-sort out and self-arrange. Every single accessible gadget on the system should work powerfully with no service from the established framework [5]. Security in pervasive computing must have the capacity to acclimatize changes in setting and situational data easily. In a regular wired network, each PC is physically secured to its condition by gadgets, for example, wires, alarms, and locks. Security in networking is disturbed about accomplishing objectives like verification, classification, uprightness, secrecy, and accessibility [6]. Conventional systems, for example, framework based neighborhood, utilize different security instruments to accomplish these objectives. Also, these gadgets are more helpless against physical security dangers like piracy as a solution to mobility. A gathering confronting such an unpredictable domain stands to profit by connection with these new gadgets. However, it can transfer significant benefits that permit shared advantage while maintaining up physical and computerized security [7]. The advanced security of these computers is controlled by the customary security systems, for example, cryptography, firewalls, and systems with devoted authoritative routers. These routers implement advanced security through an organized arrangement of strategies. From the earlier trust connections between routers can be obtained from these approaches because the personality of every route is validated before access to the network.

As indicated by the powerful topology of Ad hoc networks, routing and communication between the hubs in these systems have been examining missions. Energy utilization at the system interface is an issue for all portable processing gadgets, regardless of whether they work inside a base station framework or in an unsupported Manet. In future the utilization of energy is largely consumed and it can be lowered by lower energy protocols, energy observing user interfaces etc. [8, 9]. Thus the requirement for energy productivity is an issue that gets from the limitations forced by the battery limit and thermal dispersal, which is restricted by the need for scaling down and compactness. Battery-operated invention for thermal expulsion consume higher at a slower pace contrasted and the expanding calculation expected and the diminishing size of remote terminals. The constrained battery resource devoured by hubs in a Manet must be considered as a restricted resource in utilizing a routing protocol. Besides, outlining another steering convention that suited for Manet in light of accessible Ad hoc directing convention is as yet a testing issue for scientists [10]. Power constraints in hub joint by an organization of countless have made these difficulties to plan another routing protocol for Manet. Along these lines by outlining an energy efficient routing protocol diminishes the power utilization of the hubs by routing information on ways that expend minimal measure of energy [11]. The quality of service introduces to the ability of a system to give improved support to choose traffic in network against different advances. The QoS routing protocol requires not just finding a course from a source hub to an end point hubs. However, the course should have a least end delay, higher route throughput and less energy utilization [12]. Usage of lifetime of the battery source and the rate of it's should be considered to build the stability of the network.

2 Literature Survey

MANET is a self-organized accumulation of mobile hubs which speak with each other without the assistance of any settled framework or focal facilitator. Intrusion Detection Systems (IDS) are utilized as a part of MANETs to screen exercises to distinguish any interruption in the defenseless system. In this paper, Marchang et al. [13] have presented a probabilistic model that makes utilization of collaboration between IDSs among neighborhood hubs to decrease their dynamic time. The evaluation point is to reduce the IDSs dynamic time without effectiveness operation by displaying effective plans for investigating and optimizing the time length for which the system for intrusion detection need to stay dynamic in Manet.

In MANET, the pernicious aggressors may assault the area data and routing messages. The present wireless network package faces difficulties triggered by the intrinsic design. In this paper, Muthusenthil et al. [14] designed a security cluster geographic routing protocol in mobile adhoc networks. In this method, cluster head is picked in light of hub value which is assessed in light of degree difference, hub portability, and remaining energy. Subsequently, the target of this work is to develop routing protocol while consuming larger energy utilization and network overhead.

Energy utilization and network security are considered to be the major portions of Mobile Ad Hoc Networks (MANETs). In mobile adhoc network, security can be applied to the network by utilizing trust management, key performance, firewalls and harmful virus detections. The idea of MANET is conveyed and self-composed to play out the necessary network functionalities through the taking part hubs, and thus the collaboration of hubs is a critical factor for giving dependable correspondence all the more successfully. Muthurajkumar et al. [15] have proposed a Cluster Based Energy-Efficient Secure Routing Algorithm (CEESRA) in this paper which is vitality productive utilizes cluster routing in which the trust system utilize the hubs to distinguish the intrusion adequately. Thus the proposed steering calculation decreases the Denial of Service attacks and secure and control over the network during routing process.

In today world scenario, when each mobile devices correlates with human behavioral models. Individuals regularly run over with different groups having patterns, for example, flexibility in communication. Trust is a unique feature considered as an imperative part of the arrangement of such groups. Singh et al. [16] have

proposed a Trust based Intelligent Routing Algorithm, which interrupts the Call Data Record from Call Detail Record. The capacity of Artificial Neural Network is to predict the trust evaluation in the network. The proposed calculation brings down the need for hubs resources like energy consumption, network computational time and route overheads respectively. Manet system supports less system in which hubs convey to each other remotely. MANET is effortlessly inclined to assaults when contrasted with a wired system. There are techniques accessible to enhance the security of the system. In this work, Lodhi et al. [17] are applying Region Based Routing in the system and concentrate on the issue of secure route discovery and information transmission in an autonomous MANET. It has some issue and to beat this issue, Region Based Routing is utilized that dispenses with the copied passage from the routing table. Scalability, in this manner, extends the system measure and enhance the execution.

Most limited Path routing is dependable, not reasonable for any portable remote system as in high activity conditions; the briefest way constantly choose the most limited way which is as far as a number of hops, amongst source and goal subsequently creating more congestion. In this paper, Desai et al. [18] have organized receiving certainty based double fortification learning based versatile system directing is examined. The easiest and compelling strategy utilized as a part of the system is the briefest way of routing. In briefest way directing the way with least number of the packet is chosen to convey the bundle from source to the goal. This is the primary spurring factor for planning and actualizing different adaptive routing methodologies on a network.

Routing in submerged remote sensor systems (UWSN) is an essential and a computation movement because of the design of acoustic channels and to the relentless condition. Al Salti et al. [19] have proposed a novel multipath grid based geological directing (MGGR) convention for UWSNs. Routing is performed by the grid operation for transferring information to the sink nodes. Results demonstrate that EMGGR is an energy efficient routing in wireless network consumes lesser energy than conventional routing protocols.

Manet is another era correspondence innovation. In this condition, the system gadgets are completely Wi-Fi enabled gadgets. Furthermore to control these hubs not produced together control executive accessible. Along these lines, the topology arrangement and their management is the key of network service. Energy utilization is the most difficult issue in directing convention plan for MANETs since versatile hubs are battery fueled. In this presented work the energy conservation is the key point. In this manner, Acharya et al. [20] have modelled a weighted clustering approach for proposing an energy efficient routing in wireless networking. In this framework, the energy focused on nature of administration parameters are chosen for performance measures. In this manner, the buffer length, remain energy and the signal quality of the hubs are used for weight calculation.

Energy efficiency is a critical issue of stress in Manet as compact center points rely upon batteries, which are obliged wellsprings of essentialness, and, in various circumstances, it is a tremendous purpose to supplant or stimulate them. In this paper, Arora et al. [21] have addressed the power-saving issue for completely control mindful portable hosts to achieve energy saving on all these protocol layers. By proposing another EPAR-DSR routing estimation uniquely intended for MANETs. In this article, an ideal routing computation of attentive energy has been displayed in view of interest that causes to build organize lifetime by decreasing energy utilization. Likewise, the proposed technique causes conveyance of activity among hubs and divides energy utilization uniformly among network hubs, and prevents from the division of the system into small regions.

MANET is an exceptional kind of system that does not require any distinct framework or balance for its support because of high proficiency of their self-sufficient and self-overseeing hubs. Energy utilization and its appropriate usage play a key factor in routing innovation. As consistent quality is a central point in Mobile Adhoc Networks (MANET), numerous conventions have been intended for productive power utilization with limiting the delay. Rout et al. [22] have presented the outline of an honest steering convention with deferring improvement and power fitness for MANET. The plan depends on the routing strategy of Adhoc On request Distance Vector Routing routing which said to be a conspicuous responsive directing convention of MANET. This exploration work means to do performance examination of a balanced load convention and also compares other routing protocol, and the simulation comes about which guarantees better execution of the energy efficient protocols regarding QoS constraints.

3 Secure Energy Efficient Multicast (SEEM) Routing Protocol

Mobile adhoc network is a self-organizing network consumes less infrastructure for network operation. In networking, multicasting is one of the improved methods for efficient communication. Multicasting technique offers to send and receive messages to a group simultaneously. Somehow mobile adhoc network is facing numerous challenges during networks such as high energy consumption, low bandwidth ratio and network lifetime. Security is one of the concerned factors along with energy consumption since wireless network is an open sourced network, the intrusion formation in the networks are easily attacked and largely affect the network efficiency. The motive of this research methodology is to develop a trust-based energy efficient routing for improving the network security and thereby enhancing the energy consumption of networking.

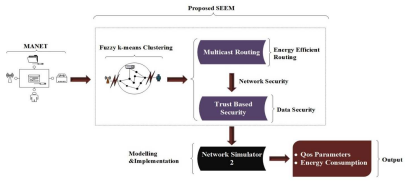

Fig. 1: Architecture of Proposed SEEM.

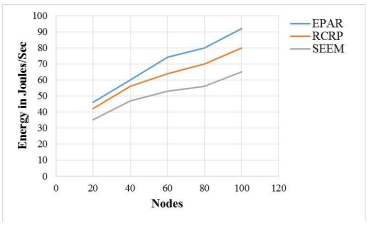

Fig. 2: Energy Consumption.

The main objective of this research paper is to propose a trust-based energy-efficient routing protocol for providing optimal security and energy consumption in mobile adhoc networks. The proposed protocol is a realistic model of fuzzy k-means and on-demand multicast routing strategy. The multicast routing strategy proposed in this paper to maintain a stable routing in the wireless node to attain higher data delivery and lower packet loss to obtain a stable connection to reduce overheads during routing. The advantage of multicast routing is to transmit data to set of receivers from a particular destination space. Therefore the cost of data transmission is lower for sending data to multiple users. The cluster approach proposed in this paper consists of fuzzy k-means to cluster the network nodes and selection of cluster heads for energy efficient routing. The cluster finds the optimal path for sending data from source to destination from the selected cluster heads. The cluster initializes with hello message to the nodes and evaluates the speed of node using coordinates. The cluster algorithm cluster the network node by distance metrics to find optimal path for energy efficient data transmission. The proposed protocol has implemented in network simulator 2, and the results have compared with the existing protocols such as RCRP Srinivas et al. [23] and EPAR Haseena et al. [24] regarding QoS and energy efficiency. From the results, it shows the proposed security routing proposed in this paper is an optimal method for consuming energy efficiency and gives optimal security to the mobile adhoc networks.

3.1 Fuzzy K-Means Clustering Method

Fuzzy clustering systems are one of the information clustering techniques performed for compelling information privacy and organizing. For a situation of systems administration, the clustering procedure is connected to group the system hubs for routing. The clustering procedure works with the participation capacity to characterize the element is in the set or not. In the conventional view, if a question is in a set which relates to the membership function of 1. If not the membership function is said to 0. The fuzzy logic reaches out by adding the set to more than 1 inside the response effort between from 0 to 1. For a given set in the point of Z with the standard element indicated as z, therefore the membership function in a similar set allocates the value $\gamma_A(z)$ to respectively Z as

$$\gamma_A(z) = \begin{cases} 1 & \text{if } z \in Z \\ 0 & \text{if } z \notin Z \end{cases} \tag{1}$$

In a fuzzy set theory, the membership function is assigned for an object at given set between two extreme value is $\gamma_A(z) : Z \to \{0,1\}$. Thus the membership sum of each object is said to be unity and closer to the value of $\gamma_A(z)$ to the upper bound. To the greater degree, z is a member off A of fuzzy set. The possibility of incomplete membership that underlies fuzzy set system gives a conspicuous method for handling the physical issue of ordinary clustering techniques, where a problem can have a position or not have a position with a specific group. A fuzzy cluster is a fuzzy subset with the participation capacity of individual problem delivering to how much it has a place with that cluster. If a cluster is a gathering whose individuals share the normal properties, at that point, the participation capacity of a problem demonstrates how much that protest shows these properties, with comparative items having a high response of the same cluster(s). The greater part of the fuzzy clustering techniques that have shown up in writing are augmentations of customary strategies that have joined fuzzy set data, with the fuzzy k-implies strategy being by a long shot the most generally utilized. The technique is mostly an iterative system for discovering groups of the substantial number of items in the component space that improve a target performance. The strategy has summarized in the below section. Let $k$be the active partition number, q is the index of fuzziness, and $\in$ is the threshold at stopping criteria. By Initializing centroid matrix with the cluster seeds and calculate the membership, γ_{ij} of each compound j, in each cluster i, using the following equation below.

$$\gamma_{ij} = \frac{\left(\frac{1}{\sum_k \left(z_{jk} - r_{ik}\right)^2}\right)^{1/(q-1)}}{\sum_i \left(\frac{1}{\sum_k \left(z_{jk} - r_{ik}\right)^2}\right)^{1/(q-1)}} \tag{2}$$

Where, z_{jk} is the data point of the jth compound at the kth number of variable and r_{ik} is the value of centroid in

the *i*th cluster at the *k*th number of variable. Updating the centroid position by using the following equation below.

$$r_{ik} = \frac{\sum_j (\gamma_{ij})^q z_{jk}}{\sum_j (\gamma_{ij})^q} \tag{3}$$

Calculate the difference between the centroid matrix from the current and previous iteration, if $\sum_{ik}(r_{ik\text{Current}} - r_{ik\text{Previous}}) < \varepsilon$, then

$$J_q = \sum_i \sum_j (\gamma_{ij})^q \left| z_j - r_j \right|^2 \tag{4}$$

In this fuzzy version of the k-means method the objective function (J_q) to be minimized.

3.2 On-Demand Multicast Routing Protocol

Multicasting is utilized when a similar message or a similar stream of information must be sent to different destination. Multicasting is a proficient information transmission strategy to maintain group oriented interchanges in many applications.

3.2.1 Mesh-based Multicast Routing

Mesh based protocols perform better in high versatility circumstance as they give access ways from source to ends while sending information parcels. However, mesh based approaches relinquish multicast proficiency in contrast with the tree based approach. Mesh based conventions have high packet conveyance proportions contrasted with tree-based conventions, yet acquire more control overhead in course support and access transmission. In this technique, the system hubs along the way interfacing the multicast source to the multicast collectors are in charge of rebroadcasting the multicast messages. This completely lowers the message overheads.

3.2.2 Trust-based On-Demand Multicast Routing Protocol

On-Demand Multicast Routing Protocol (ODMRP) applies a strategic routing methods to maintain a particulate distance from channel overhead and enhance flexibility. It utilizes the idea of transferring groups, an arrangement of hubs in charge of sending multicast data on most limited ways among member combines and assembles sending network for each multicast gathering. A delicate state methodology is followed in ODMRP to maintain multicast combined individuals. There is any need of direct control message for group to left behind. By trusting the diminishment of channel/storage overhead and the unexpected availability make ODMRP more adaptable and steadier for expensive systems in wireless networks.

3.2.3 Multicast Route and Membership Maintenance

In this routing protocol, the multicast membership function and routing are initializes on demand by the sources. If a data need to be send to a multicast source, it alternatingly communicates to the system called as join request to defining the data packets. This transmission excites the data packets and updates the routing. From there the hub get the proper join request and rebroadcast the packets. When the data forwarded from Join Request to a multicast receiver, the receiver update the part in its source. The extensive part in the table connected intermittently to the nearby join tables and evaluates for following ID is one of the coordinate of the passages. Thus the FG flag connects with its own join table based on coordinated passages. Thus the table along these lines generated by each sending group part until the point when it comes to the multicast source using the most limited way.

Data Forwarding: Cluster formation and route creation are mainly considered in this process in which a source path can multicast packages to the end point receiver by particular routes supported by the data sending groups. After delivery the data packets, a node is forwarded with FG FLAG settings unchanged and the path overheads are reduced with the packets send through the outdated routes which are stopped.

3.2.4 Trust Evaluation Criteria

Trust considered in the model is a hub's certainty on another hub. Trust value implies a level of a hub's dependability, which is processed in view of different trust valuation factors. Wireless hubs in this plan, don't figure every single other hub confide in values in the system. However, the process just neighbors hubs trust values mutually. Trust Evaluation Factor: The sensor nodes are employed with *k* trust matrices, which stores these matrices for evaluating trust for *k*th neighbour nodes. These matrices encompasses several trust factors which are elaborated in the following ways.

Link quality: Link quality is an encouraging parameter, as it characterizes a capacity of a connection and gadgets to help transfer density for the connection time frame. Connection state between two neighbors is influenced by parameters like distance, battery power, and versatility.

Distance: The distance metrics evaluation for the two nodes *z* and *x* for the *i* and *j* node coordinates will be

$$d_{i,j} = \sqrt{(z_i - z_j)^2 + (x_i - x_j)^2} \tag{5}$$

where, $0 \leqslant i, j \leqslant k$ and $i \neq j$.

Mobility: Mobility is a vital MANET routing protocols evaluation parameter. The mobility in mobile

adhoc networks for defining the network topologies is derived from the following equation below.

$$\text{mob} = \sum_{i=1}^{n} \frac{H_i}{n} \tag{6}$$

$$H_z = \sum_{t=0}^{T-\Delta t} \frac{|A_z(t) - A_z(t+\Delta t)|}{T} \tag{7}$$

$$A_z(t) = \sum_{i=1}^{n} \frac{\text{dist}(n_z, n_y)}{n-1} \tag{8}$$

where $\text{dist}(n_z, n_i)$ is the distance between nodes x and y, N be the nodes number. $A_x(t)$ be the average distance between the node x and all other nodes, at a time t. The H_z average relative mobility of node x regarding. where, T_i be the trust value of the node i, at $1 \leqslant i \leqslant k$.

Trust Value: The trust value factor is to determine the node trust factor for node and it is highlighted as evaluation factor.

Energy efficient multicast routing for Manet has extracted in a ton of consideration, and much work has been completed around there. There are predominantly three crucial classes of energy efficient multicast routing. Minimum power-on request multicast directing is to discover a multicast work with the base aggregate power for conveying a data packet from its source to all its destination. Every single existing calculation and conventions in this setting accept hubs can legitimately modify their transmission powers in view of communication ranges. Energy efficient routing protocol falls in too little no of classes as indicated by the way they accomplish energy effectiveness. Waste utilization of energy is in charge of an expansive bit of the general energy utilization in the wireless interfaces of the mobile hubs.

3.2.5 Energy Consumption

The energy consumption in message transmission during routing on a single route path is defined by

$$P_{\text{path}_l} = \sum_{l=1}^{\text{nod}_l} P_{\text{con}_l} \tag{9}$$

where nod_i is the counted node of route path I and the energy consumed during transmission is defined by

$$P_{\text{con}_l} = e_{\text{trans}} + e_{\text{recev}} \tag{10}$$

$$e_{\text{trans}} = \left(e_t + \psi_{\text{amp}} \times a^2\right) \times m \tag{11}$$

where e_{trans} the energy is the energy consumed during receiving m bits of data between the source and destination.

$$e_{\text{recev}} = e_r \times m \tag{12}$$

$$P_{\text{con}_l} = \left(e_t + e_r + \psi_{\text{amp}} \times a^2\right) \times m \tag{13}$$

Table 1: Network Simulator Parameters.

Network Simulator	:	NS-2.35
Network Channel	:	Wireless Channel
Network Interface	:	WirelessPhy
Radio Interface	:	Propagation/Two ray ground
Packet Frequency	:	50
Routing Protocol	:	SEEM
Initialized Nodes	:	100
Base station location	:	(50,50)
Deployment area	:	100 m × 200 m
Nodes in Source	:	One
Nodes in Destination	:	One
Initial energy in Joules	:	100
Sending rate	:	1packet/ sec
Packet size	:	1024bit
Connection Type	:	CBR/UDP/TCP
Initial Energy	:	100 Joules

where e_t and e_r are the energy consumed during the transmission and receiving one bit of data, 'ψ_{amp}' is the consumption of energy in the transmission amplifier. When the communication radius a is fixed and the sensor located randomly at any distance within the area be a^2.

In Fig. 2, the energy consumption during routing of proposed SEEM protocol is evaluated and contrasted with the conventional routing protocols like RCRP and EPAR respectively. During routing, the proposed protocol consumes low energy for routing than existing approaches and forms energy efficient in routing.

4 Experimentation and Result Discussion

The proposed SEEM is carried out in network simulator 2 based on java platform to enhance the energy consumption in the wireless sensor networks. The parameter utilized in the network simulator is given as below.

4.1 Network Simulation 2

Network Simulator 2, generally known as NS-2, is a simulation tool for experimenting the networking ability of mobile adhoc networks. The network simulator is an openly sourced simulation which can be implemented and executed in C++ and OTcl programming languages. In the proposed work, the simulation area of 100 m × 200 m has taken for simulation environment with a sending packet size of 1 packet/sec and transmission packet size of 1024 bit message is transferred to the adhoc networks. NS2 provides high efficiency of simulation in different networking protocols such as routing protocols with a connection type of TCP, UDP, and FTP etc. The programming language Tcl/OTcl has a simple syntax which can be combined with other languages. The parameters validated during routing simulation in network simulator 2 are as follows.

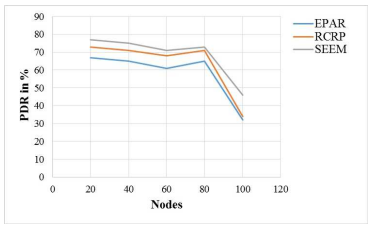

Fig. 3: Packet Delivery Ratio

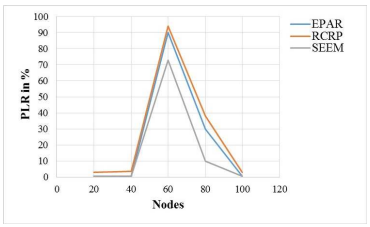

Fig. 4: Packet Loss Ratio.

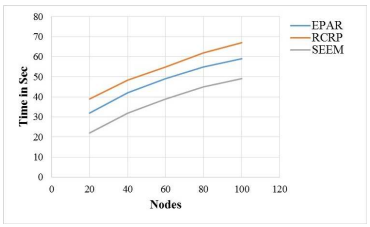

Fig. 5: Route Latency.

4.2 Evaluation of QoS in On-Demand Multicast Routing Protocol

The security issue in networking is a vital factor and QoS in Manet is one of the concerned factor facing networking these days. Interchanges in remote condition are not secure because of the reporting regulation of this variety of network. For the most part, MANETs have fewer resource than improved systems, and they are more impacted by the resource imperatives of the hubs. QoS routing is a steering procedure that assurances to help to an ordering of QoS parameters during building up a route. The QoS steering in MANETs is required just to help the mixed media constant correspondence like video-on-demand, news-on-demand, web surfing, traveler data framework and so on. MANETs have turned out to be extremely well known these days due to their integrity by utilizing and by the pervasiveness of wireless technology. As the development of interactive media applications proceeds and the necessities for genuine activity increment, there is a major test for specialists to discover advancements and methodologies fulfilling these prerequisites. QoS can be characterized as the capacity of the system to give diverse administrations to different sorts of system movement.

4.2.1 Packet Delivery Ratio (PDR)

The summation of the message acquired by the total messages sent has a proportion with the rate of packets received. The ratio of packet delivery during the proposed routing protocol can be evaluated from the following equation below.

In Fig. 3, the packet delivery during routing of the proposed protocol is executed and compared with conventional routing protocols such as RCRP and EPAR respectively. From the results, it shows the proposed SEEM scores more percentage of the delivery of packets in nodes than the existing approaches.

4.2.2 Packet Loss Ratio (PLR)

The ratio of packet loss during routing is defined as the ratio of message sent and message received during transmission. The estimation of packet loss during message transmission has compared with the proposed protocols, and it is highlighted in the below diagram. The following equation derives the packet loss ratio.

In Fig. 4, the maximum number of packet loss during routing of proposed SEEM protocol has compared with existing protocols like RCRP and EPAR respectively. From the simulation results, the proposed SEEM has lower loss ratio than the existing protocols and forms more optimal during routing.

4.2.3 Route Latency

The network latency is described as the maximum time utilized for the analysis response. Lower the latency rate make the efficiency of routing to the higher state. The evaluation of network latency can be estimated from the following equation below.

In Fig. 5, the comparison of route latency in proposed SEEM protocol is executed and compared with the conventional routing protocols such as RCRP and EAPR respectively. During routing, the proposed protocol has lower latency and forms more efficient of transmission during routing.

4.2.4 Route End to End Delay

The end to end delay in routing is defined as the maximum time utilized for sending and receiving messages within the network to attain the destination point. It is induced in the network transferring which can be evaluated from the following equation below.

In Fig. 6, the end delay of proposed SEEM routing protocol is executed and compared with the conventional routing protocols such as RCRP and EPAR respectively. The simulation results clearly shows, the proposed

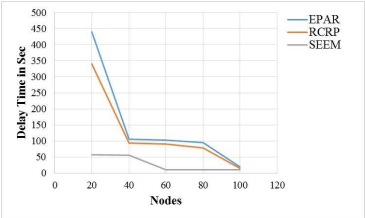

Fig. 6: End to End Delay.

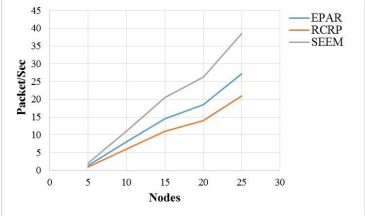

Fig. 7: Route Throughput.

protocol has lower transmission delay in nodes and performs routing in an efficient way.

4.3 Route Throughput

The route throughput in the network is defined as the number of the positive message transmitted over FSO-MANET network. The purpose of throughput is to analyze the message transferred in the meantime. The route throughput analysis of network can be derived from the following equation below.

In Fig. 7, the route throughput of proposed SEEM routing protocol is compared with an existing protocol like RCRP and EPAR respectively. During routing, the proposed protocol has a high throughput of node transmission than the existing approaches like RCRP and EPAR respectively. From the analysed results, it shows that the proposed protocol has a higher ratio of efficiency in the routing process.

5 Conclusion

Security is a dominant factor facing in networking; the mobile adhoc networks are vulnerable to different malicious attacks. To overcome the security efficacy in the network, the Manet is powered with a security protocol to protect the network from attacks. The undertaking to provide security in Manet to protect the network services are accessed by the nodes. Another factor affecting the network efficiency is the energy consumption. This research paper proposed a cluster-based security protocol to give optimal security and thereby consumes less energy for processing the network. The proposed protocol composed of fuzzy *k*-means clustering and trust based on-demand multicast routing protocol. The clustering module cluster the network into cluster nodes and these nodes have routed by a trust based on-demand multicast routing. During routing the protocol selects the optimal path for transmission and consumes the network operational energy. The proposed protocol is experimented in the network simulator and compared with the existing protocols in terms of energy efficiency and QoS parameters respectively. From the result discussion, it clearly defines that the proposed routing strategy is an efficient method for improving energy efficiency and security in mobile adhoc networks

References

[1] Li, Xu, et al. Optimized multicast routing algorithm based on the tree structure in MANETs, China Communications, **11(2)**, 90–99, 2014.
[2] Jain, Aaditya, and Bala Buksh. Solutions for Secure Routing in Mobile Ad Hoc Network (MANET): A Survey, Imperial Journal of Interdisciplinary Research, **2(4)**, 2016.
[3] Sarkar, Sajal, and Raja Datta. A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks, Ad Hoc Networks, **37(1)**, 209–227, 2016.
[4] Yan, Zheng, Peng Zhang, and Athanasios V. Vasilakos. A security and trust framework for virtualized networks and software-defined networking, Security and communication networks, **9(16)**, 3059–3069, 2016.
[5] Yadav, Ajay Kumar, and Sachin Tripathi. Qmrprns: Design of qos multicast routing protocol using reliable node selection scheme for Manets, Peer-to- Peer Networking and Applications, **10(4)**, 897–909, 2017.
[6] Singh, Tejpreet, Jaswinder Singh, and Sandeep Sharma. Energy efficient secured routing protocol for MANETs, Wireless Networks, **23(4)**, 1001–1009, 2017.
[7] Das, Santosh Kumar, Ajay Kumar Yadav, and Sachin Tripathi. IE2M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network, Peer-to-Peer Networking and Applications, **10(3)**, 670–687, 2017.
[8] Mazhar, Nauman. Energy efficient security in MANETs: A comparison of cryptographic and artificial immune systems, Pakistan Journal of Engineering and Applied Sciences (2016).
[9] Qiu, Tie, et al. Heterogeneous ad hoc networks: Architectures, advances, and challenges, Ad Hoc Networks, **55)**, 143–152, 2017.
[10] Zhang, Xiaoying, et al. Performance of Energy-Efficient Cooperative MAC Protocol with Power Backoff in MANETs, Wireless Personal Communications, **92(3)**, 843–861, 2017.
[11] Dhurandher, Sanjay K., et al. An energy-efficient history-based routing scheme for opportunistic networks, International Journal of Communication Systems, **30(7)**, 2017.
[12] Poongodi, T., and M. Karthikeyan. Localized secure routing architecture against cooperative black hole attack in mobile Ad hoc networks, Wireless Personal Communications, **90(2)**, 1039–1050, 2016.

[13] Marchang, Ningrinla, Raja Datta, and Sajal K. Das. A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks. IEEE Transactions on Vehicular Technology, **66(2)**, 1684–1695, 2017.
[14] Muthusenthil, B., and S. Murugavalli. Privacy preservation and protection for cluster based geographic routing protocol in MANET, Wireless Networks, **23(1)**, 79–87, 2017.
[15] Muthurajkumar, S., et al. An Intelligent Secured and Energy Efficient Routing Algorithm for MANETs, Wireless Personal Communications, **1(1)**, 1–17.
[16] Singh, Ajay Vikram, Vandana Juyal, and Ravish Saggar. Trust based Intelligent Routing Algorithm for Delay Tolerant Network using Artificial Neural Network, Wireless Networks, **23(3)**, 693–702, 2017.
[17] Lodhi, Ramniwas, and Neha Bhardwaj. Improving Scalability and Security using Region Based Routing Protocol in Mobile Ad Hoc Network, International Journal, **8(5)**, 2017.
[18] Desai, Rahul M., and B. P. Patil. Prioritized Sweeping Reinforcement Learning Based Routing for MANETs, Indonesian Journal of Electrical Engineering and Computer Science, **5(2)**, 383–390, 2017.
[19] Al Salti, Faiza, Nasser Alzeidi, and Bassel R. Arafeh. EMGGR: an energy- efficient multipath grid-based geographic routing protocol for underwater wireless sensor networks, Wireless Networks, **23(4)**, 1301–1314, 2017.
[20] Acharya, Priyanka, and Jayesh Surana. A weighted clustering algorithm for optimizing the energy consumption in MANET, International Journal of Contemporary Technology and Management **5(7)**, 2016.
[21] Arora, Saurabh. Minimization of Energy Consumption Using EPAR-DSR Protocol in Manet, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056, **4(6)**, 2017.
[22] Rout, Umesh Prasad, and Puspamitra Panda. Performance Evaluation of Power Efficient Protocol in MANET, Performance Evaluation, **1(1)**, 263–267, 2017.
[23] Srinivas, K., and A. A. Chari. A Random Congestion Routing Protocol Based on Queue Latency and Link Reliability Estimation in MANETs, Indian Journal of Science and Technology, **9(33)**, 2016.
[24] Haseena, K. S., Sheena Anees, and Neela Madheswari. Power Optimization Using EPAR Protocol in MANET, IJISET-International Journal of Innovative Science, Engineering & Technology, **1(6)**, 2014

S. Baskaran is a research scholar in VELS Institute of Science, Technology & Advanced Studies (VISTAS Deemed to be university) and Associate Professor in Department of Computer Science & Engineering, Kuppam, A.P., India. He received M.E from Anna University, Chennai and Master of Computer Applications from Madras University. He is in teaching profession for 17 years. His areas of interest is computer networks.

J. Arputha Vijaya Selvi received her B.E. degree in Electronics and Communication Engineering from Government college of Engineering Tirunelveli, in 1991, and M.E. degree at National Institute of Technology Tiruchirappalli, in 1997 and Ph.D. degree from National Institute of Technology Tiruchirappalli, in 2006. From 2003 to 2004, she was the principal of Idhaya Engineering College for Women, TamilNadu. In 2007, she joined as Dean in Kings College of Engineering, Thanjavur. Presently she is working as Professor in Electronics and Communication Engineering and Principal of Kings College of Engineering, Tamilnadu, India. She is in teaching profession for 19 years. Her research interest includes Adaptive Optics, Signal Processing, Simulation and Control, Biomedical Processing and Speech Processing.

V. R. Sarma Dhulipala is working as Assistant Professor in the Department of Physics, Anna University-BIT Campus, Tiruchirappalli, Tamil Nadu. He obtained his Ph.D degree in Wireless Sensor Networks from Anna University, Chennai in 2013, M.Phil from JNTU , Hyderabad in 2006 and M.Sc (Electronics) from Andhra University in 2000. His expertise in electronics leads him to teach subjects in electronics, Pervasive Computing. He worked as an associate in the departments of Nano Science and Technology and Pervasive computing Technology. His research interest includes Wireless and mobile ad hoc networks, Body Sensor Networks, Nano electronics. He published more than 70 research articles. Presently working towards design and development of frameworks and algorithms using WSN and AHN for Medicinal Applications.