# Secure MANET Communication Using Cluster Based Multicast with Fair Key and Resource Scheduler

[1]D. Anitha, [2]Dr.M.Punithavalli

[1] Research Scholar, Karpagam University,
Coimbatore, Tamilnadu, India

[2]Director, MCA, Shri Ramkrishna College of art and science,
Coimbatore, Tamilnadu, India

**Abstract**

In current Mobile Adhoc Network (MANET) scenario of social network, Delay Tolerant Networks (DTNs) are needed to handle frequent network partitions and large end-to-end delays for efficient multicasting. Existing scheme presented adaptive multicast routing to handle multicast delivery schemes for DTNs. However performance and reliability obtained on sparsely connected nodes in the MANET social network communication is not up to the required standards. So, this paper presents Energy and Bandwidth-based Fair Queue Scheduling algorithm (EBFQS) and cluster based multicasting (CBM) using Fair Key and Resource scheduler (FKRS) in MANET. The proposed algorithm is able to converge under different network models, where each model reflects a different set of assumptions about the multicasting capabilities of the network. . It introduces a novel data structure for the nodes to communicate and to consider the own load states when forwarding packets. The priorities of packets are assigned according to the current node's load level. When nodes are leisure, they should help other nodes to construct route first. The cluster is formed with the nodes which has fair key and a possible resource schedules for an effective communication with less network delay. The simulation results show that the proposed EBFQS and Cluster Based Multicasting (CBM) using FKRS in MANET effectively decrease the Energy Usage, Bandwidth, network transmission delay, communication overhead, increased security and clustering effectiveness.

**Keywords:** *Mobile Adhoc Network (MANET), Multicasting, Clustering, Fair Key, Resource Scheduler, Social Network Communication.*

## 1. Introduction

A MANET is an independent system of mobile nodes coupled through wireless links. It does not have any fixed infrastructure. MANET is quite different from distributed wireless LAN and wired network. There is no centralized control, and it is quite difficult for any single mobile host to have an accurate picture of the topology of the whole network. Nodes in a MANET keep moving randomly at varying speeds, ensuing in constantly changing network topologies. Each node in the network serves as a router that forwards packets to other nodes. The scarcity of bandwidth implies that there should not be high communication overhead among various nodes.

In addition, error-prone communal broadcast channel, concealed and uncovered terminal problems, and limitation on battery power, all these above factors make end-to-end packet delivery and delay guarantee in MANET in a rough intention Each flow from the source to the destination traverses multiple hops of wireless links. The quick rising mobile ad hoc network's main application is emergency rescue operations and battlefields. This work also lecture to the problem of power aware routing to increase lifetime of overall multicast ad hoc network. Since nodes in mobile ad hoc network can move randomly, the topology may change arbitrarily and frequently at unpredictable times. Transmission and reception parameters may also impact the topology. Therefore it is very difficult to find and maintain an optimal power aware route.

Multicast, on the other hand, is more effective for data dissemination and multi-party communication, but is also more difficult to model and implement in opportunistic DTNs. Although there are some initial efforts on studying multicast in DTNs, they are limited to semantic multicast models and multicast capacity analysis, and none of them considers multicast in DTNs from the social network perspective.

The fair share of each packet flow is defined with respect to the corresponding flow contending graph. Each one-hop flow always receives a fair share in the bottleneck area of the network, represented by the high clique in the flow contending graph. Energy and Bandwidth-based Fair Queue Scheduling Algorithm (EBFQS) identifies the flows that currently receive reduced services in their locality, and ensures their access to the wireless channel. The scheduling coordination in EBFQS is localized within the flow's one-hop neighborhood in the flow contending graph.

EBFQS further enhances three dimensions. First, it offers larger fair share to each flow, characterized by the fair share in the maximum clique of the flow contending graph. Second, it is more resilient against incomplete and erroneous scheduling information origin by collisions. Finally, EBFQS realizes delay and throughput decoupling, leading to more efficient utilization of the wireless channel among applications with different bandwidth requirements.

Clustering consists of dividing the multicast group into a number of sub-groups. Each sub-group is managed by a local controller (LC), accountable for local key management within its cluster. In addition, multicast group clustering thinks about the energy difficulty to understand an efficient key distribution process, whereas energy constitutes a foremost concern in ad hoc environments. Key distribution systems typically involve a trusted third party (TTP) that acts as an intermediary between nodes of the network. Key management in the ad hoc network is a challenging issue concerning the security of the group communication. Group key management protocols can be approximately classified into three categories; centralized, decentralized, and distributed.

## 2. Literature Review

Many of these applications require certain rate guarantees, and demand that the network be utilized more efficiently than with current approaches to satisfy the rate requirements [1]. Traffic mapping is one particular method to carry out traffic engineering, which deals with the existing works on multicast routing with power constraints are refer in the literatures. The key problem is to determine appropriate ferry selection strategy and data forwarding criteria. Recent trace-based study on campus wireless networks [2] shows that different nodes have heterogeneity in their contact patterns, and such heterogeneity validates the use of Social Network Analysis (SNA) for data forwarding in DTNs.

Fair queuing has been a popular scheduling paradigm in both wire line networks [3, 4] and packet cellular networks. Fair queuing in a wireless ad-hoc network is a distributed scheduling problem by nature. Finally, the wireless channel capacity is limited. Improving channel utilization through spatial channel reuse i.e., simultaneously scheduling flows that do not interfere with each other is highly desirable.

Normally, an ad hoc network is a collection of independent nodes that correspond with each other, most frequently using a multi-hop wireless network. A node in an ad hoc network has direct association with a set of nodes, called neighboring nodes, which are in its communication range. New nodes may connect the network whereas existing ones may be cooperated or become un-functional [5]. Mobile Ad-Hoc Network (MANET) is one where there is no predestined infrastructure framework such as base stations or mobile switching centers. The services of MANET includes authentication, data confidentiality, data integrity is the establishment of a key management protocol [6]. A key is used by the resource to encrypt multicast data and by the receivers to decrypt it. As a result only genuine members are capable to obtain the multicast flow sent by the group source [7]. Key management is an essential part of any secure communication. In an ad-hoc network, [10] proposed a cluster based scalable key management protocol Ad hoc networks. Their proposed protocol is supported on a novel clustering technique. A key management system for safe and secure group communication in MANETs was described in [8]. They demonstrated a hierarchical key management scheme (HKMS) for secure group communications in MANETs. A novel group key management protocol for wireless ad hoc networks presented in [11].

Temporal Data clustering proposes a novel weighted consensus function guided by clustering validation criteria to reconcile initial partitions to candidate consensus partitions from different perspectives, and then, introduce an agreement function to further reconcile those candidate consensus partitions to a final partition [9, 12]. As a result, the proposed weighted clustering ensemble algorithm provides an effective enabling technique for the joint use of different representations, which cuts the information loss in a single representation and exploits various information sources underlying temporal data.

## 3. Secure MANET Communication Using Cluster Based Multicast with Fair Key and Resource Scheduler

The Fig 3.1 represents the architecture of Energy and Bandwidth-based Fair Queue Scheduling algorithm (EBFQS) and Cluster Based Multicasting (CBM) using Fair Key and Resource scheduler (FKRS) in MANET. MANET forwards the packets to the nodes and they perform the three operations. i.e., creating fair key and resource scheduler for nodes, cluster the nodes, multicasting based on first two operations outcomes.

The first operation described the process of assigning fair key and consumption of resources used by the nodes in MANET. The key is assigned to the nodes based on Group Key management. The cluster head is chosen for the group and the secret key is shared for an authorized access of nodes in MANET.

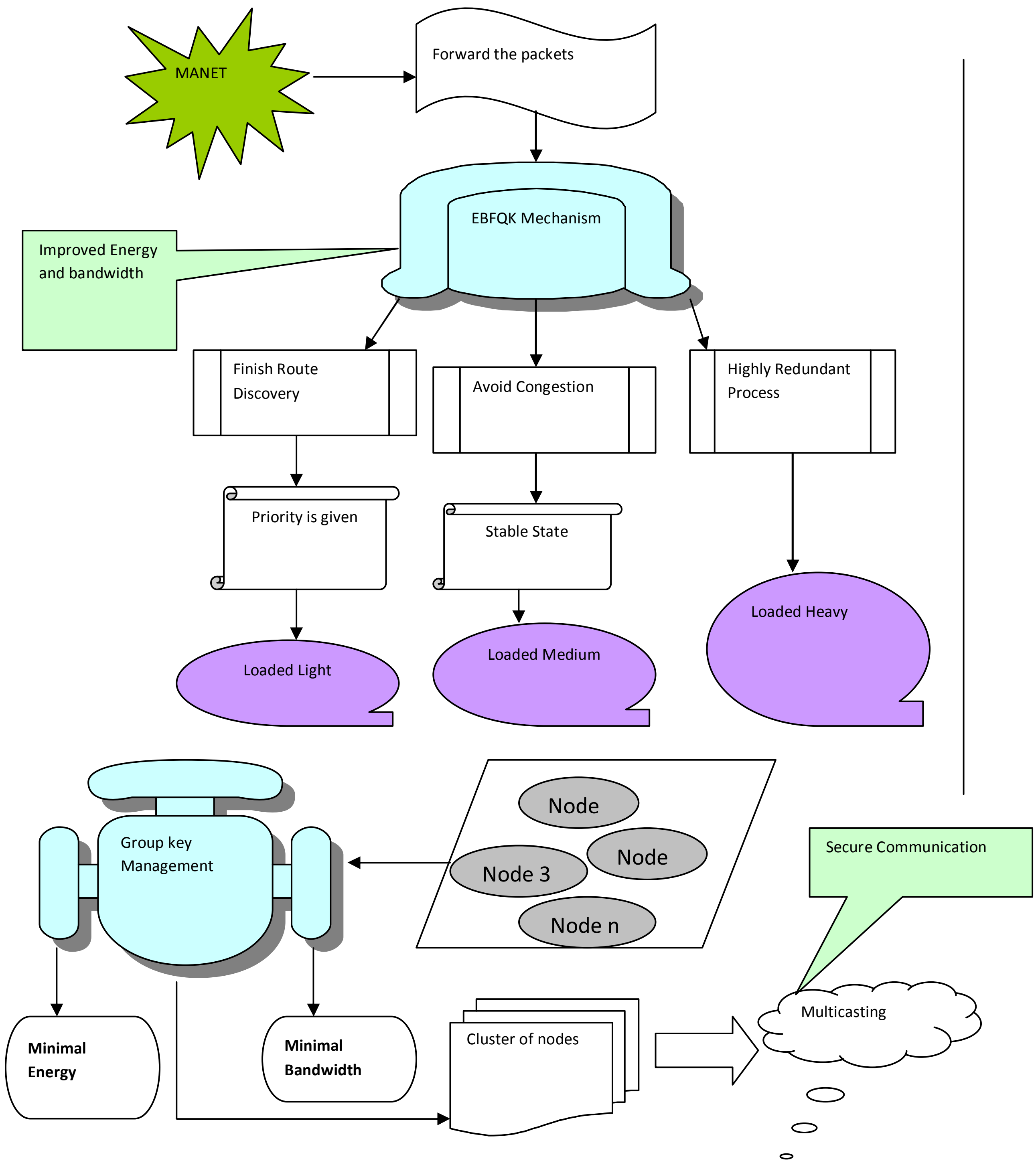


Fig 3.1 Architecture Diagram of EBFQS and CBM using FKRS in MANET

The second operation describes the clustering process based on fair key and resource scheduler multicasting. The nodes are clustered based on the levels of the nodes in MANET for communication. The clustering is done efficiently based on the nodes which have fair key and uses minimal number of resources, energy and bandwidth for communication.

The third operation described the process of multicasting. The efficiency with which multicast communication can take place is largely determined by the network level support available for such communication. To eliminating the lack of reliability and scalability of multicast communication in ad hoc network, there presents a source-tree-based reliable multicasting scheme and partial multicasting scheme is presented. This allows messages to be delivered to subsets of multicast destinations efficiently and secure communication.

Energy and Bandwidth based Fair Queue Scheduling mechanism (EBFQS) is proposed with different queue scheduling policies which are adopted according to the current load of node. Queue length is used as the load indicator and three load levels are defined by two thresholds Minth and Maxth. The first level is light load that the queue length is less than Minth. The second level is medium load that the queue length is between Minth and Maxth. And the last level is heavy load that the queue length is bigger than Maxth. For the Light Load the priority is given to complete the route discovery. Medium Load contains the stable state to avoid the congestion. Heavy Load surround by the highly redundant process.

## 3.1 Fair Queue Scheduling Mechanism

The objective of our energy competent packet scheduling algorithm is to adapt the output rate S(t) to match the instantaneous workload. At the same time, we would like to bind the performance impact that may result. However, buffering the input variations leads to a performance penalty due to an increase in packet delays. Therefore, the crux of the problem reduces to formative the degree of buffering while bounding the increase in packet delays.
If every server always runs at Smax, Weighted Fair Queuing guarantees the following end-to-end delay bound for each connection i,

$$\frac{C_i + (J_i - 1)\,Q_i}{D_i} + J_i\,\frac{\max_i Q_i}{S_{max}} \quad \text{-------> (1)}$$

Where Ci, Di, Ji and Qi are respectively the burst size, connection rate, hop count and maximum packet size for connection i. Our major result is that for any rate-adaptive policy that uses rates between Smin and Smax and always uses rate Smax when the queue exceeds a threshold V, if we schedule according to Weighted Fair Queuing then the end-to-end delay is bounded by

$$\frac{C_i + (J_i - 1)\,Q_i}{D_i} + J_i\,\frac{\max_i Q_i}{S_{min}} + \frac{S_{max}\,V}{S_{min}\,D_i} \quad \text{------> (2)}$$

We begin our analysis by focusing on a single server in isolation. This will allow us to determine some of the basic tradeoffs between queue size and energy usage. Recall that opt R(t) is the minimum amount of energy required by time t if it wish to keep the queue bounded by R at all times. Let opt R(t, t') be defined similarly on the interval (t, t'). It derive a simple bound on opt R(t, t').

For a single server s,

$$Opt\,R(t, t') \ge f\left(\max\left(S_{min}, \frac{M_s(t,t') - R}{t' - t}\right)\right) * (t' - t) \quad \text{----------> (3)}$$

Intuitively, guaranteeing a better bound on queue size should incur higher energy usage. We establish that such a tradeoff is inherently unavoidable.

$$y_1 = \frac{R}{S_{min}}, \quad \text{----------> (4)}$$

y2 y3, …… be a sequence that satisfies

$$\frac{R}{2y_j}\, y_j f \ge n \sum_{l<k} \frac{R}{y_l}\, y_l f \quad \text{----------> (5)}$$

Which implies that the amount of data rate adaptation can serve is no more than R/2. Equation (5) shows our proposed EBFQS used the less energy resource and minimized the bandwidth.

### 3.2 Group Key Management for Fair Key and Resource Scheduler (FKRS) of nodes

The Group Key Management (GKM) encompasses of three operations, namely, registration, re-keying and data security. The registration process of nodes in MANET is done via one-to-one bidirectional secure channels. The re-keying process is done at the initial stage and updated its key for a security purpose. The data security process secures the data. The GKM is done based on the nodes present in MANET. The activities of the nodes are monitored and the key is assigned to each and every node in MANET for a secure communication. Based on key, a group is formed and it identifies the resource consumption of each node in the system. The GKM shares every sender and receiver node in MANET to verify that whether the sender/ receiver are an authorized one or not.

The Group Key Management is done based on the nodes present in MANET. For instance, consider the average number of nodes in the MANET is $N=\lambda pA$, where $\lambda p$ specifies the node density of the randomly distributed nodes and A indicates the operational area of MANET wireless medium.

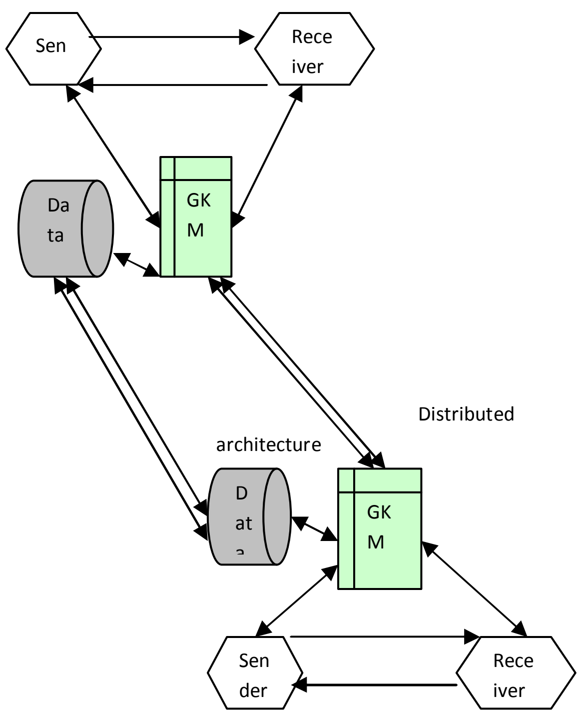


Fig 3.2 Architecture of Group Key Management

Based on homogeneous spatial Poisson process, the random distribution of nodes is done. Therefore, the probability of the node is in any group is $\lambda/(\lambda+\mu)$ and the probability that it is not in any group is $\mu/(\lambda+\mu)$. Consider AJ and AL be the aggregate join and leave rates of all nodes, correspondingly. Then, AJ and AL, can be calculated as follows,

The important requirement for secure group communication is reliable transmission. As a result, whenever there is a change in the leader of the group, the leader key, KRL is rekeyed. The regional key (KR) is rekeyed whenever there is a regional membership change, including a local member group join/leave, a node failure, and a group merge or partition event.

### 3.3 Fair key Clustering process

Clustering consists in dividing the group into a number of sub-groups. Each sub-group is supervised by a local controller (LC), responsible for local key management within its cluster. Besides, not many solutions for multicast group clustering imagine about the energy trouble to appreciate a proficient key distribution process, while energy comprises a primary concern in ad hoc environments. Clusters may be used for achieving different targets. Some of them are clustering for transmission management, clustering for backbone formation, and clustering for routing efficiency. Group key management must be differing to a wide range of attacks by both outsiders and rouge members. The clustering process based on fair key is shown in Fig 3.3.

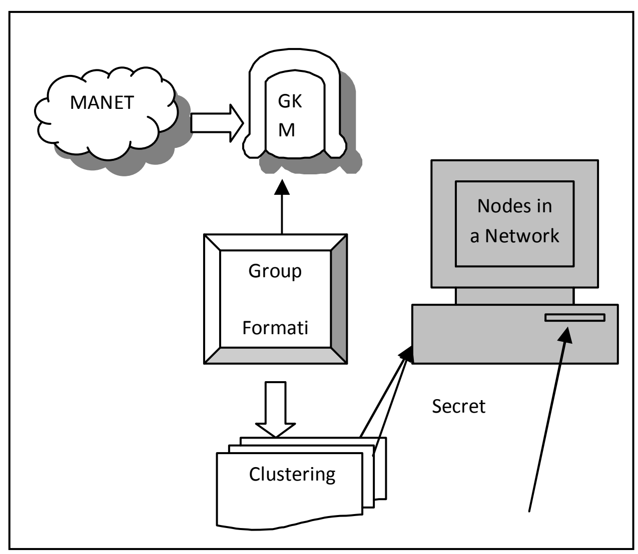


Fig 3.3 clustering based on Fair Key

The steps for generation of cluster based on GKM are as follows:

- Identify the group based on fair key KF and minimal resource (MINr)

- Form the cluster based on the group and generates its own key (Ck)
- Identify the cluster root node (r) and generate secret key (Sk)
- The secret key of root node will become the clustered group key for every operation.
- Cluster group changes its key Ck (re-key) for a secure communication and dispersed among all members of cluster.

### 3.4 Cluster based Multicast Communication Security

Cluster based multicast communication presents an effective way to broadcast information to potentially large number of receivers. Multicasting is the liberation of a message to a collection of destination nodes in MANET concomitantly in a single communication from the source. The cluster based multicasting is done based on the GKM and the architecture diagram of cluster based multicasting based on FKRS is shown in Fig 3.4.

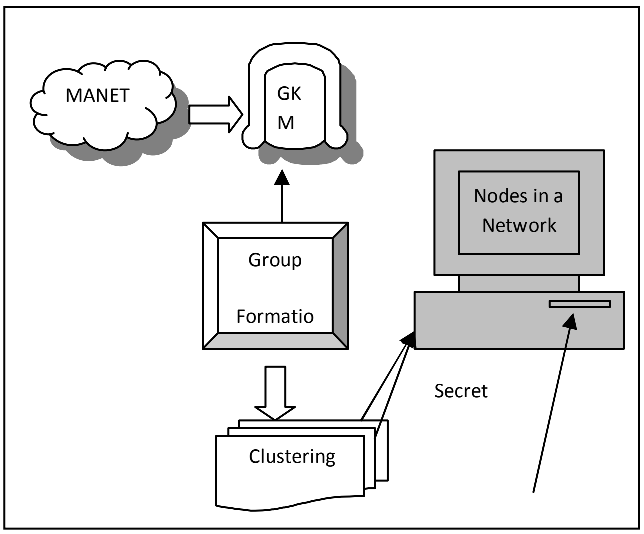


Fig 3.4 Architecture diagram of CBM based on FKRS in MANET

Based on clustering, which is performing using the nodes has fair key and minimal resource consumption, the secure social network communication is activated through multicasting.

## 4. Experimental Evaluation

Broad experimental amend is conducted to observe the proposed Energy and Bandwidth-based Fair Queue Scheduling algorithm (EBFQS) and Cluster Based Multicasting (CBM) using Fair Key and Resource scheduler (FKRS) in MANET. It is implemented within the ns-2 simulator. The radio model is based on the viable hardware with a wireless transmission range of 270 meters and channel capacity of 3Mbps. Each simulation runs for 270 seconds and the results are compared. The applications of interest include, FTP-driven TCP traffic, CBR-driven (constant bit rate) UDP traffic, audio-driven UDP traffic and video-driven UDP traffic. All packets are set to be of 512 bytes, except that video traffic has varying packet sizes based on the actual traces. The performance of the proposed EBFQS and CBM using FKRS is measured in terms of

i) Usage of Energy
ii) Bandwidth
iii) Network Transmission Delay,
iv) Communication Overhead
v) Security
vi) Clustering Effectiveness

## 5. Results and Discussion

In this work, it shows how the social network communication is done effectively and securely using EBFQS and CBM which is done through Fair Key and Resource Scheduler. The existing work described only the adaptive multicast routing to handle multicast delivery schemes for DTNs, so the proposed work described the process of multicasting for an effective communication in MANET even when the topology of the network changes. The table and the performance graph show the effectiveness of the proposed EBFQS and CBM using FKRS for an effective communication.

| Load Factor (L) | Energy Usage (Joules) | |
|---|---|---|
| | Proposed EBFQS using FKRS | Existing Adaptive Multicast Routing |
| 0.2 | 1.0 | 3.2 |
| 0.4 | 1.3 | 3.8 |
| 0.6 | 1.5 | 4.3 |
| 0.8 | 2.0 | 4.9 |
| 1.0 | 2.7 | 5.4 |

Table 5.1 Load Factor vs. Energy Usage

The above table (Table 5.1) described the energy usage by load factor in MANET. The energy usage of the proposed technique is compared with an existing Adaptive Multicast Routing in MANET.

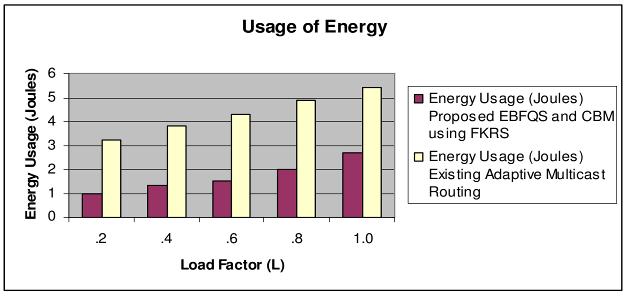


Fig 5.1 Load Factor vs. Energy Usage

Fig 5.1, described the communication overhead of nodes obtainable in MANET. In the proposed EBFQS and CBM using FKRS technique, the nodes in the MANET consumes less energy performs well with the less time consumption to transmit a message from source to destination compared to an existing method.The variance in the communication overhead for MANET would be 55-65% low in the proposed technique.

| No. of packets (p) | Bandwidth | |
|---|---|---|
| | Proposed EBFQS using FKRS | Existing Adaptive Multicast Routing |
| 20 | 210 | 280 |
| 40 | 220 | 300 |
| 60 | 233 | 320 |
| 80 | 241 | 340 |
| 100 | 250 | 355 |

Table 5.2 Packet Flow vs. Bandwidth

The above table (Table 5.2) described the bandwidth usage in MANET. The bandwidth reduces in the proposed EBFQS and CBM using FKRS technique than an existing system in MANET.

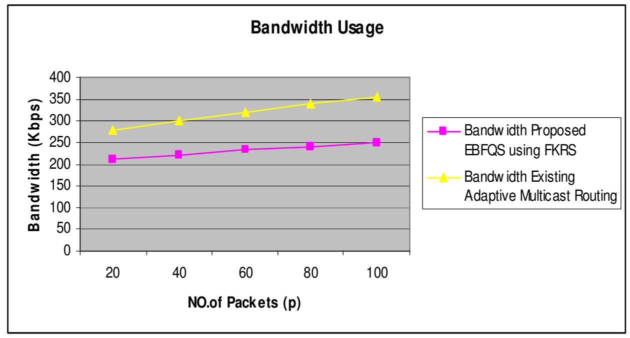


Fig 5.2 Packet Flow vs. Bandwidth

Fig 5.2, described the bandwidth level of communication available in MANET. In the proposed EBFQS and CBM using FKRS technique, the nodes in the MANET consumes the lesser bandwidth to transmit a message from source to destination compared to an existing Adaptive Multicast Routing. The bandwidth usage is 20-30 % less in the proposed technique.

| No. of packets (p) | Network Transmission Delay | |
|---|---|---|
| | Proposed EBFQS and CBM using FKRS | Existing Adaptive Multicast Routing |
| 5 | 0.6 | 1.3 |
| 10 | 1.3 | 1.8 |
| 15 | 2.0 | 2.8 |
| 20 | 2.5 | 3.1 |
| 25 | 3.1 | 3.6 |

Table 5.3 No. of nodes vs. Network transmission delay

The above table (Table 5.3) describes the network transmission delay when number of packets increases in MANET environment. The table describes the comparison of the proposed EBFQS and CBM using FKRS with an existing multicast routing in MANET.

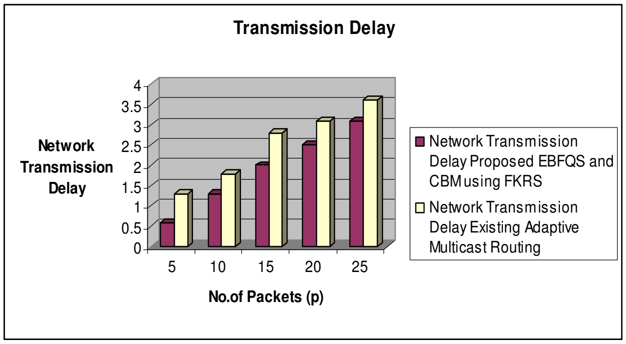


Fig 5.3 No. of nodes vs. Network transmission delay

Fig 5.3 describes the network transmission delay for sensing the packet data from source clustered node to destination clusterd node in MANET. Comparison result of the proposed with an existing Adaptive Multicast Routing in MANET based on network transmission delay. When number of packets in the nodes in the MANET increases, the network transmission delay for sending the packets from source to destination is 13- 20 % less in the proposed EBFQS and CBM using FKRS contrast to an exisitng Adaptive multicast in MANET.

| No. of nodes (n) | Communication Overhead (%) | |
|---|---|---|
| | Proposed EBFQS and CBM using FKRS | Existing Adaptive Multicast Routing |
| 25 | 13 | 25 |
| 50 | 21 | 42 |
| 75 | 33 | 53 |
| 100 | 47 | 76 |
| 125 | 62 | 85 |

Table 5.4 No. of nodes vs. Communication Overhead

The above table (Table 5.4) described the communication overhead of nodes in MANET. The communication overhead arises in the proposed EBFQS and CBM using FKRS technique is low compared with an existing system in MANET.

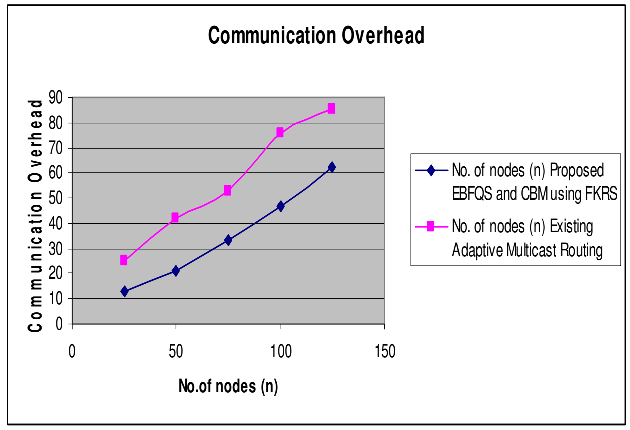


Fig 5.4 No. of nodes vs. Communication Overhead

Fig 5.4, described the communication overhead of nodes obtainable in MANET. In the proposed EBFQS and CBM using FKRS technique, the nodes in the MANET consumes less bandwidth resource, performs well in the process of communication overhead and consumes less time to transmit a message from source to destination compared to an existing method.The variance in the communication overhead for MANET would be 30-40% low in the proposed technique.

| Methods | Security level (%) |
|---|---|
| Proposed EBFQS and CBM using FKRS | 90 |
| Existing Adaptive Multicast Routing | 60 |

Table 5.5 security level

The above Table (table 5.5) described the security level of nodes for communication in MANET. The level of security in the proposed EBFQS and CBM using FKRS technique is high compared with an existing system

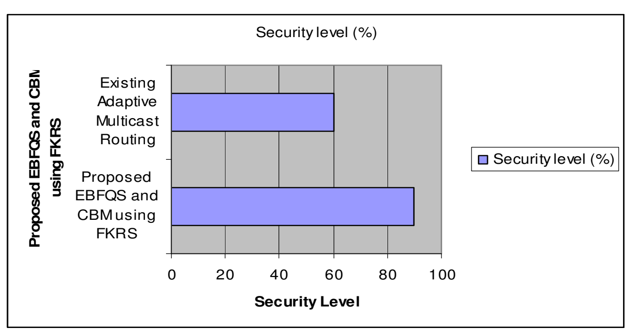


Fig 5.5 security level

Fig 5.5, described the security level of communication available in MANET. In the proposed EBFQS and CBM using FKRS technique, the nodes in the MANET has higher security level to transmit a message from source to destination compared to an existing Adaptive Multicast Routing.

| No. of nodes (n) | Clustering efficiency | |
|---|---|---|
| | Proposed EBFQS and CBM using FKRS | Existing Adaptive Multicast Routing |
| 5 | 0.5 | 1.2 |
| 10 | 1.2 | 1.9 |
| 15 | 2.1 | 2.8 |
| 20 | 2.6 | 3.3 |
| 25 | 3.2 | 3.8 |

Table 5.6 No. of nodes vs. Clustering efficiency

The above table (Table 5.6) described the efficiency of clustering process for nodes in MANET. The efficiency of cluster using the proposed technique is compared with an existing Adaptive Multicast Routing in MANET.

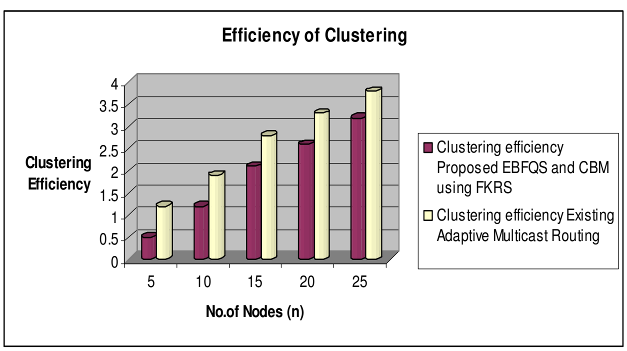


Fig 5.6 No. of nodes vs. Clustering efficiency

Fig 5.6, described the efficiency of clustering process for nodes available in MANET. In the proposed EBFQS and CBM using FKRS technique, the clustering process is done for the nodes which has fair key in MANET and the clustering process is compared to an existing system. Comparison result of the proposed technique with an existing adaptive multicast routing shows that the technique perform 20-25% high in the process of clustering the nodes based on fair key and minimal resource consumption.

## 6. Conclusion

In this paper, the proposed Energy and Bandwidth-based Fair Queue Scheduling algorithm (EBFQS) and Cluster Based Multicasting (CBM) using Fair Key and Resource scheduler (FKRS) in social networking communication MANET by gratifying the application efficient energy, bandwidth usage and security. In synopsis, the proposed EBFQS and CBM using FKRS approach has some advantageous features: 1) targeting the packet scheduling process and explore avenues for making it energy attentive and bandwidth, 2) it presented an effective method to cluster the nodes based on fair key and negligible resource expenditure, 3) it professionally done the fair key mechanism through GKM, 4) it consumes less time for clustering process and provides an effective communication. Compared to the existing techniques the proposed EBFQS and CBR using FKRS technique fro secure social networking communication outperforms well and the level of security is 75-85 % high.

## References

[1] U. Lee, S.-Y. Oh, K.-W. Lee, and M. Gerla. Scalable multicast routing in delay tolerant networks Proc. ICNP, 2008.

[2] S. Ioannidis, A. Chaintreau, and L. Massoulie Optimal and scalable distribution of content updates over a mobile social network Proc. INFOCOM, 2009.

[3] M. Andrews, A. Fernandez Anta, L. Zhang, and W. Zhao., "Routing and scheduling for energy and delay minimization in the power down model "IEEE INFOCOM '10, March 2010.

[4] A. Wierman, L. L. H. Andrew, and A. Tang., "Power-aware speed scaling in processor sharing systems " In IEEE INFOCOM '09, pages 2007– 2015, 2009.

[5] A. Renuka, and K. C. Shet, "Cluster Based Group Key Management in Mobile Ad hoc Networks," IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 4, pp. 42-49, 2009.

[6] Yi-Hong Chu, et. Al., " Density Conscious subspace Clustering for High-Dimensional Data", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 22, NO. 1, JANUARY 2010

[7] Mohamed-Salah Bouassida, Isabelle Chrisment, and Olivier Festor, "Group Key Management in MANETs," International Journal of Network Security, vol. 6, no. 1, pp. 67-79, 2008.

[8] Renchu Guan et. Al., " Text Clustering with Seeds Affinity Propagation", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 23, NO. 4, APRIL 2011.

[9] Yun Yang and Ke Chen, " Temporal Data Clustering via Weighted Clustering Ensemble with Different Representations", IEEE TRANSACTIONS ON

KNOWLEDGE AND DATA ENGINEERING, VOL. 23, NO. 2, FEBRUARY 2011.

[10] Chadi Maghmoumi, Hafid Abouaissa, Jaafar Gaber, and Pascal Lorenz, "A Clustering-Based Scalable Key Management Protocol for Ad Hoc Networks," ctrq, 2009 Second International Conference on Communication Theory, Reliability, and Quality of Service, pp.42-45, 2009.

[11] Rony H. Rahman, and Lutfar Rahman, " A New Group Key Management Protocol for Wireless Ad-Hoc Networks," International Journal of Computer and Information Science and Engineering, vol. 2, no. 2, pp. 74-79, 2008.

[12] Eric Hsueh-Chan Lu, et.Al., "Mining Cluster-Based Temporal Mobile Sequential Patterns in Location-Based Service Environments", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 23, NO. 6, JUNE 2011.