*International Journal on Applications in Engineering and Technology*
*Volume 6 : Issue 1 : March 2020, pp 17 – 24 www.aetsjournal.com* ISSN (Online) : 2455 - 0523

# REALTIME MULTICASTING WITH NETWORK CODING AND HYBRID ALGORITHM IN MOBILE AD-HOC NETWORK

PRABAKARAN . S , GOVINDASAMY . R , GOPI . R ,

***Abstract***— The data transfer to the basis to the destination is more efficiently in the Mobile Ad-hoc Network, but the main thing in the MANET is the data should be reached the target with full format (without any packet loss). The package forwarding time between the sources to destination these are thinks should be managed using some techniques. A Network Coding based Real-time Multicast (NCRM) protocol is future for real-time multicast services in Mobile Ad-hoc Networks MANET. Through reducing the forwarding times for data packets in MANET, NCRM can not only lessen the energy consumption, but it also improves the throughput performance. NCRM outperforms Protocol for Unified Multicasting from end to end Announcement (PUMA) and Multicast Ad-hoc on-demand Distance Vector (MAODV) for increasing transmission reliability and energy use significantly. Hybrid algorithm is used for efficient data encryption and decryption for improving the security; stream cipher &block cipher are combined to get a secured HYBRID ciphertext.

***Keywords:*** Multicast Ad-hoc On-demand Distance Vector (MAODV), Protocol for Unified Multicasting throughout Announcement (PUMA), Network Coding based Real-time Multicast (NCRM)

## I. INTRODUCTION

A mobile ad hoc network (MANET) is defined as a network that has many free or autonomous nodes, often collected of mobile devices or other portable pieces that can arrange themselves in various ways and operate without strict top-down network administration. Each device in a MANET is free to go independently in any direction, and will, therefore, modify its links to further devices frequently. Each must forward traffic unrelated to its use, and thus be a router.

Prabakaran.S , Faculty of Information Technology, Dhanalakshmi Srinivasan Engineering College.
Govindasamy.R , Faculty of computer science and engineering, Dhanalakshmi Srinivasan Engineering College
Gopi.R , Faculty of Information Technology, Dhanalakshmi Srinivasan Engineering College.

The primary challenge in building a MANET is equipping each device always to maintain the information required to route traffic correctly. Such networks may operate by themselves or may be connected to the broader internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. "A collection of wireless mobile hosts forming a temporary network, without the aid of any federal administration or standard support services."

Mobile nodes have limited communication range, Reduces battery drain, Enables spatial reuse of limited bandwidth increased network capacity. To connect all nodes in the network, each node is a packet source , packet sink, router. Nodes must route packet for other nodes to keep the system fully connected. The ad-hoc architecture has many benefits, such as self-reconfiguration and adaptability to a highly variable mobile character such as power and transmission conditions, traffic distribution variations, and load balancing. However, such payback comes with some new challenges which mainly reside in the unpredictability of network topology due to the mobility of nodes, which coupled with the local broadcast capacity, cause a set of concerns in designing a message system on top of wireless ad hoc networks. These challenges include:

### *1)Routing*

Multicast routing is another challenge because the multicast tree is no longer static due to the random movement of nodes within the system. Routes between nodes may potentially contain multiple hops, which is new complex than the single hop communication. Multicast is a type of communication where multicast traffic addressed

for a group of devices on the network. IP multicast traffic is sent to a group and only members of that team receive and process the Multicast traffic. Tools which are interested in a particular Multicast traffic must join that Multicast group to receive the traffic.

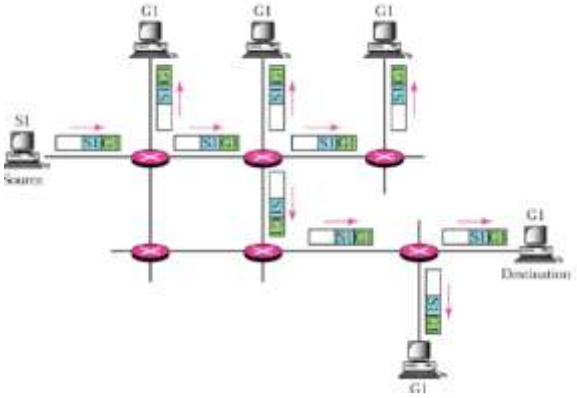


**Figure 1 Multicast Routing**

### *2) Security and Reliability*

In addition to the typical exposure of wireless connection, an ad hoc system has its particular safety problems due to, e.g., nasty neighbor relaying packets. The feature of distributed operation requires different schemes of verification and key management. Further, wireless link characteristics introduce also reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g., hidden terminal problem), mobility induced packet losses, and data transmission errors.

### *3) Quality of Service:*

Providing a diversity of repair levels in a continually changing setting will be a challenge. The characteristic stochastic feature of communications quality in a MANET makes it challenging to offer firm guarantees on the services provided to a device. An adaptive **QOS** must be implemented over the traditional source reservation to support the multimedia services.

### *4) Power Consumption:*

For most of the light-weight mobile terminals, the communication-related functions should be enhanced for lean power consumption. Protection of power and power-aware routing must be taken into consideration. Routing protocols can also be classified according to whether they find optimal (shortest) routes or sub-optimal routes. By not requiring courses to be optimal, it is possible to reduce the amount of control traffic (including routing updates) necessary to maintain the roads. However, optimal routes are desirable because they minimize delay and the number of resources (e.g., bandwidth and power) consumed.

## II. RELATED WORKS

Network coding has been successfully used in the past for efficient broadcasting in wireless multi-hop networks. Two coding approaches are suitable for mobile systems; random linear network coding (RLNC) and XOR-based coding. In this paper, we focus on the trouble of multiple source broadcasting in cellular ad hoc networks. We make the observation that RLNC provides increased resilience to packet losses compared with XOR-based coding. We develop an analytical model that justifies our intuition.

The Ad hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in ad-hoc mobile networks. Since of the difficulty of testing an ad hoc routing protocol in a real-world environment, a simulation was first created so that the protocol design could be tested in a variety of scenarios. Once simulation of the contract was nearly complete, [3,4] the simulation was used as the basis for an implementation in the Linux operating system.

Mobile Ad Hoc Networks (MANETs) is a self-configuring network of mobile nodes connected by wireless. These protocols have distinguishing features and use different mechanisms. Modified PUMA routing protocol improves the network performance regarding energy consumption and transmission failures. It reduces the load on wireless nodes by selecting the route with minimum energy with a maximum hop count. And also, SMAC is used to save the energy values of wireless nodes. In a multicast environment, by combing both of these techniques to increase the network performance regarding energy consumption,[5] transmission failures, packet dropping and an end-to-end delay.

A technique for secret communication using cryptography. Cryptography means data secure; it helps to ensure data privacy, maintain data integrity,

authenticate communicating parties, and prevent repudiation. It is a technique which is used to protect the critical data. The secret message is encrypted by a block cipher based on two cryptographic algorithms, the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA) which may be used by Federal organizations to protect sensitive data.[6]This Algorithm uniquely defines the mathematical steps required to transform data into a cryptographic cipher and also to changes the cipher back to the original form with a block length of 128 bits and a key length of 256 bits. Data Encryption Standard (DES) is the block cipher which takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bit line of the same length. It is a symmetric encryption technique which means both sender and receiver use a shared key to encrypt and decrypt the data.

Analysis of the effect of different parameters of the RC4 encryption algorithm where examined. Some experimental work was performed to illustrate the performance of this algorithm based on changing some of these settings. [7] The execution time as a function of the encryption key length and the file size was examined; this has been stated as complexity and security. Various data types were analyzed, and the role of the data type was also emphasized. The algorithm can be broken into two stages: initialization, and operation. In the initialization stage the 256-bit state table, S is populated, using the key, K as a seed. Once the state table is set up, it continues to be modified in a regular pattern as data is encrypted. Algorithm: Hybrid Multicast routing protocols, Source-Based Multicast Tree, Tree-based Multicast routing protocols.

## III. IMPLEMENTATION OF PROPOSED METHODOLOGY

Multicast routing is another challenge because the multicast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complicated than single hop communication. Multicast is a type of communication where multicast traffic is addressed for a group of devices on the network. IP multicast traffic is sent to a group, and only members of that team receive and process the Multicast traffic. Tools which are interested in a particular Multicast traffic must join that Multicast group to receive the traffic.

IP Multicast Groups are identified by Multicast In Multicast, the sender transmits only one copy of data, and it is delivered and processed. In real time, multi cast routing protocol is proposed. IP Multicast group are identified by Multicast IP Addresses (IPv4 Class D Addresses) In Multicast, the sender transmits only one copy of data, and it is delivered and who are interested in that traffic. The Proposed system mainly focused on Multicast routing, Packet forwarding time between the one node to other node and many nodes to any node. The main contributions of this paper are:

I. Through reducing the forwarding times for data packets in MANET, NCRM can not only decrease energy consumption but also improve the throughput performance.
II. To satisfy the maximum end-to-end delay deadline requirements for real-time services, NCRM adopts a mechanism with strict delay constraints. NCRM outperforms Those traditional protocols such as PUMA and MAODV regarding transmission reliability and energy consumption significantly.
III. Hybrid Algorithm (A stream cipher &block cipher are combined to get a secured Hybrid ciphertext for data encryption and decryption, here are many ways to connect cryptographic algorithms to the combination is increasing security.

Mobile Ad hoc Networks (MANETs) is the cooperative appointment of a collection of wireless mobile nodes that also performs as routers. Nodes in MANETs connect with each other through multi-hop transmission that does not need any current substructure or message supporting center. Topologies of MANETs [9] may change quickly. Nodes in MANETs often perform a given task with other nodes together. ZBMRP applies on-demand trials to dynamically establish mesh-based multicast routing zones along the path from the multicast source node to the multicast receivers. Control

packet flooding is employed inside multicast zones. Thus multicast above is vastly abridged, and excellent scalability can be achieved. It will also be easier to secure multicast routing. ZBMRP fits well for MANETs where bandwidth is limited, topology changes frequently, power is constrained, and security problem is severe. Simulation results are presented to support our claim.

Efficient use of the resources in mobile ad hoc networks (MANETs) is of great importance to maintain the required quality of service and to prolong the network lifetime. The utilization of the resources such as bandwidth and energy depends on some conditions such as network size, node density, and load distribution. These circumstances are uncontrollable and often vary throughout the operation of the network. To efficiently use the resources, the protocols that determine the behavior of the system should dynamically [10] adapt to these changing conditions. At the MAC layer, we develop an analytical model that reflects the relationships between protocol parameters and the overall performance of the protocol under various network conditions.

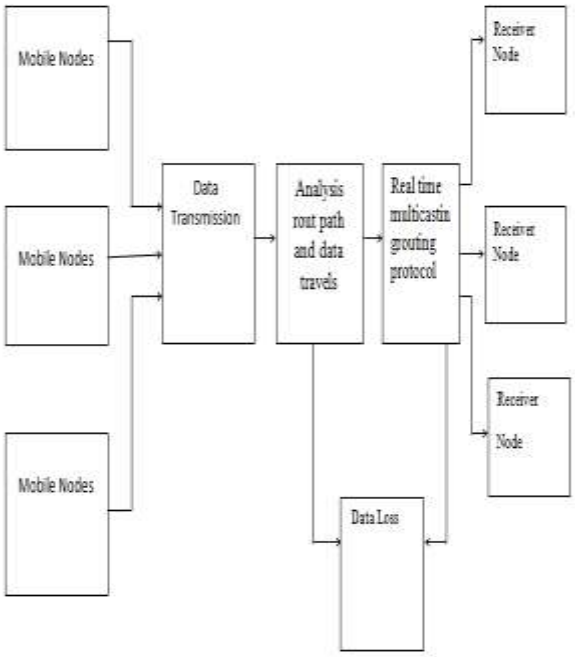



**Figure 2 proposed system architecture**

IP Multicast Groups are identified by Multicast In Multicast, the sender transmits only one copy of data, and it is delivered and processed. In the real time, multi cast routing protocol is propose d. IP Multicast group are identified by Multicast IP Addresses (IPv4 Class D Addresses)In Multicast, the sender transmits only one copy of data, and it is delivered and who are interested in that traffic. The Proposed system mainly focused on Multicast routing, Packet forwarding time between the one node to other node and many nodes to any node The new sub sink always has the higher priority for communication in the allocation of the overlapping time, which means that the mobile pan disconnects the communication link with current sub sink and turns to the new sub sink once it detects a new sub sink.

### *1) Multicast Ad-hoc On-demand Distance Vector (MAODV), Algorithm MAODV Protocol*

A set of techniques or mechanisms including the policies that can be applied in a network, to manage limited network resources such as bandwidth. These methods (MAODV) are intended to improve overall network performance and efficiency. They are also designed to provide for more predictability and orderliness in the event of network congestion.

Inputs: The ID and (x, y) coordinates of each node.

Outputs: Destination nodes receive data packets from sources nodes.

Begin

1. Select a center or near-center node in the initial network as the root node (RN).
2. The RN runs the Double-Flooding Algorithm (DFA) to create the location table (LT), sorts the LT by IDs in ascending order, and broadcasts the LT to each node in the network.
3. Each node uses the LT to generate its distance table (DT) concurrently. Then, each node marks any distance that is longer than the transmission range k in the DT as "∞" (infinity).
4. Each node calls the Algorithm to generate the one-to-all shortest-path table (SPT) concurrently
5. If a new node joined to the system, an existing node enthused out of the broadcast range of its any national nodes, or an existing node left-hand from the net, then it calls the Node-Reorganization Algorithm (NRA) to ask additional nodes to update (or mark as "new"

nodes if any) their LT for these changes consequently.

6. If some node needs to send packets via or to the above combined or enthused nodes, it has to (1) use the efficient LT in Step 5 to update its DT (or mark the "∞" distances if any); (2) track the procedure again to update its SPT; (3) reset all bulges in the LT to "old" nodes; and (4) shadows the trails in the new SPT to send packs to its terminus nodes.

7. If network topology changed again, repeat steps 5 and six until the whole network dismissed.

End of MAODV Protocol.

Throughput Performance is high

The techniques should also isolate faults and provide visibility into performance problems. Furthermore, traffic management is intended to increase the "throughput" traffic, based on the economic value and prevent the abuse of network resources.

### *2) Protocol for Unified Multicasting through Announcement (PUMA),*

Algorithm 1 Node I processing a Core Announce packet

This module is developed to topology design all node place particular distance. Without using any cables then fully wireless equipment based transmission and received packet data. Node and wireless between calculate sending and receiving packets. The sink is at the center of the circular sensing area.

1: Input:
2: announce incoming Core Announce
3: last Hop the node from which announce was received
4: Begin:
5: g announce: group
6: if coreIdg(i) = INVALID ADDRESS
OR coreIdg(i) _ announce:core
OR sequon( i) _ announce:seqNo then
7: Update local information:
Coleridge( i) announce:coreId
seadog( i) announce:seqNo
8: Invoke UpdatePUMAAndCostg (laptop;1; announce: cost; TRUE) 9: Update cost in the announcement packet:
announce: cost announced: cost + cost(i)
10: Rebroadcast announce
11: endif

Algorithm 2 Procedure Update PUMA

1: Parameters:
2: next neighbor ID indicating which PUMA table entry to be updated
3: height associated with this update
4: the cost of joining the group at a forwarding node of height via next5: lag indicating whether this update is deterministic
6: Begin:
7: if _g(i; next; height) is not de_ned then
8: _g(i; next; height) 0
9: end if
10: if detF lag = TRUE then
11: bestCostg(i; height) cost
12: _g(i; next; height) _g(i; next; height) + 1
13: else
14: if bestCostg(i; height) is not de_ned OR cost <bestCostg(i; height) then
15: bestCostg(i; height) cost
16: _g(i; next; height) 1 /* set intensity to max */
17: else
18: _g(i; next; height) _g(i; next; height) + 1
1+cost
19: endif
20: endif
21: _g(i; next; height) minf_g(i; next; height); 1)g /* PUMA intensity is at most one */

PUMA routing protocol improves the network performance regarding energy consumption and transmission failures. It reduces the load on wireless nodes by selecting the route with minimum energy with a maximum hop count.

### *3) Network Coding based Real-time Multicast (NCRM)*

Through lowering the forwarding times for data packets in MANET, NCRM can not only decrease the energy consumption but also improve the throughput performance.

1. Initialization: Create copies of the time-unwrapped graph. Initialize flow values on all edges of each figure to zero.
2. Set the number of edge-disjoint augmenting

paths.
Two repeat
3 .for do
4. Find the shortest augmenting path on the graph.
5 .Remove edges conflicting with edges in from all graphs.
6. Six end
7 .Increment a unit logical flow and reverse the edges along the augmenting paths for each graph. Increment by one.
8. specify multicast requirements on a directional graph G with: V (source)◊ a:{1,...,m} ν
9. a(2)=1 =o> vertex 1 sends information source 2 2V (set of sinks)◊ b:{1,...,m} ν
10. b(2)={5,6,7} =o> vertices 5,6 and 7 receive information source 2 h=[h1ν ...hm ] (information rate of sources)
11.The capacity of each link (i,j) between vertices i and j in graph G is Rij
12. characterize admissible rate ofo the network The fundamental literature of networko coding aims at characterizing the coding rate region R
13. The set of all admissible R for any type of G and any set of multicast requirements.
14. Repeat reach destination
End

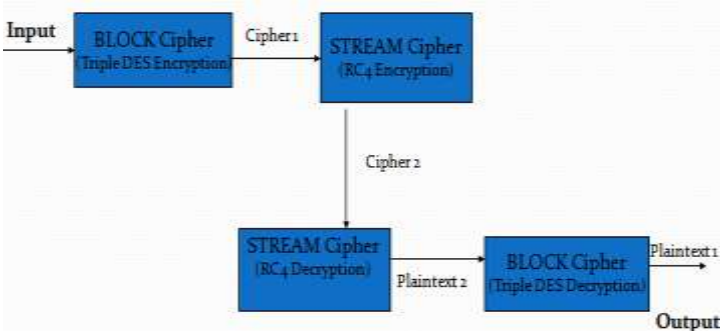
To satisfy the maximum end-to-end delay deadline requirements for real-time services, NCRM adopts a mechanism with strict delay constraints.

### *4) Hybrid Algorithm*

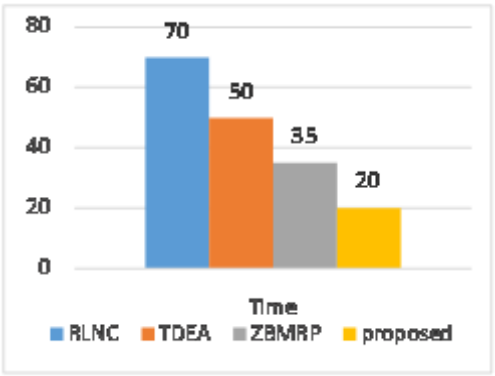
"A stream cipher & block cipher are combined to get a secured HYBRID ciphertext "

**Block Cipher-**In cryptography, a block cipher is a symmetric key cipher operating on fixed-length groups of bits called blocks, with a unvarying transformations. Might take 128-bit input and output 128-bit block of ciphertext. The key can be of any finite size. Decryption is the inverse function of encryption.

**Stream Cipher-**In cryptography, a stream cipher is a symmetric key cipher where plaintext bits are combined with a pseudorandom cipher bit stream (keystream), typically by an exclusive-or (XOR) operation. In a stream cipher, the plaintext digits are encrypted one at a time, and the transformation of successive digits varies during the encryption. An alternative name is a state cipher, as the encoding of each number is dependent on the current state. In practice, the digits are typically single bits or bytes. A stream cipher makes use of a much smaller and more convenient key 128 bits, for example. Based on this key, it generates a crucial pseudorandom stream which can be combined with the plaintext digits in a similar fashion to the one-time pad.




## IV. RESULTS AND DISCUSSION:



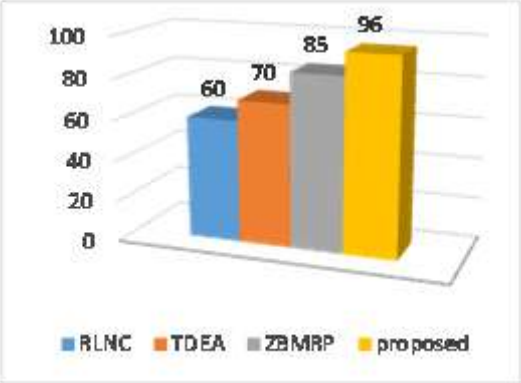

This module is developed for node creation, and more than 25 nodes placed particular distance. Wireless node put central area. Each node knows its location relative to the sink. The access point has to receive transmitted packets then send acknowledge to the transmitter. Nodes monitor the link status of next hops on the multicast tree. When a link break on the multicast tree is detected, the tree branch should be immediately repaired through the use of the RREQ/RREP/MACT messages. A multicast group leader is associated with each multicast group.The primary responsibility of this node is the initialization and maintenance of the group sequence number. A Group Hello message is periodically broadcast across the network by the multicast group the multicast group leader.

**Graph 1: Time complexity of proposed system**

Figure 1 shows the privacy level at the expansion of a connection that achieves lower time complexity compared to the existing system.

**Graph 2: shows the accuracy key log relational analysis.**

Graph 2 shows our evaluation results suggest that overall accuracy is well-suited for integration in existing systems since it incurs less than 5% overhead compared to existing semantically secure encryption modes.




Hybrid Algorithm (A stream cipher &block cipher are combined to get a secured Hybrid ciphertext for data encryption and decryption, There are many ways to connect cryptographic algorithms to get new algorithms. The impetus behind the combination is increasing security.

## V. CONCLUSION

Multicasting is used when the same message or the same stream of data must be forwarded to multiple destinations. Multicasting is an efficient data transmission method to support group-oriented (MAODV and PUMA) communications in one-to-many or many-to-many applications such as audio/video conferencing, collaborative works, and so on. In MANETs, the most challenging issue in multicast routing is to efficiently handle the frequent and unpredictable topology changes caused by host mobility, link breakage, and host failure. This paper provided a survey of most recent multicast routing (MAODV, PUMA) protocols for MANET. This study showed that MAODV and PUMA might improve network performance regarding delay, throughput, reliability or lifetime. Due to severe constraints of mobile wireless ad hoc networks such as host mobility, limited resources and very unreliable communication channel, single protocol or a set of protocols that can improve all these performance parameters is extremely hard to find. Security has become a very critical aspect of modern computing systems. The use of internet and network is growing rapidly. So the requirement to secure the data is necessary. To provide security, to network and data, different encryption methods can be used. In this paper, the Hybrid algorithm is used for Security purpose. It is based on Caesar cipher, Rijndael and Vernam algorithms. The author used this method for text files.

In our future work we can add various types of files in this method. Also we can add more algorithms to enhance the security. Using more algorithms provide a secure environment for data storage and retrieval.

## REFERENCES

[1] A. N. Mian, R. Baldoni, and R. Beraldi,(2009) “A survey of service discovery protocols in multihop mobile ad hoc networks,” IEEE Pervasive Comput., vol. 8, no. 1, pp. 66–74.

[2] N. Kadi and K. Al-Agha, (2008) "Optimized MPR-based flooding in ad-hoc wireless network using network coding," in Proc. 1st IFIP Wireless Days (WD), pp. 1–5.

[3] B. Vellambi, N. Rahnavard, and F. Fekri, (2010) "FTS: A distributed energy efficient broadcasting scheme using fountain codes for multihop wireless networks,” IEEE Trans. Commun., vol. 58, no. 12, pp. 3561–3572.

[4] C. N. Ververidis and G. C. Polyzos, (2008) “Service discovery for mobile ad hoc networks: A survey of issues and techniques,” IEEE Commun. Surveys Tuts., vol. 10, no. 3, pp. 30–45, 3rd Quart.

[5] P. Ostovari, J. Wu, and A. Khreishah, (2012) “Deadline-aware broadcasting in wireless networks with local network coding,” in Proc. IEEE Int. Conf.Comput. Netw. Commun. (ICNC), pp. 1123–1127.

[6] C. Reis, R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, (2006) "Measurement-based models of delivery and interference in static wireless networks,” vol. 36, no. 4.

[7] S. Agathos and E. Papapetrou, (2013)“On the set cover problem for broadcasting in wireless ad hoc networks,” IEEE Commun. Lett, vol. 17, no. 11, pp. 2192–2195.

[8] A. Khreishah, I. Khalil, and J. Wu, (2013) "Low complexity and provably efficient algorithm for joint inter and intrasession network coding in wireless networks," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 10, pp. 2015–2024.

[9] J. Krigslund, J. Hansen, M. Hundeboll, D. E. Lucani, and F. H. P. Fitzek, (2013) “CORE: COPE with MORE in wireless meshed networks,” in Proc.IEEE Veh. Technol. Conf. (VTC), pp. 1–6.

[10] Le Boudec J.-Y and M. Vojnovic, (2005) “Perfect simulation and stationarity of a class of mobility models,” in Proc. IEEE Int. Conf. Comput.Commun. (INFOCOM), pp. 2743–2754.

[11] Yu, J.Y., Chong, P.H.J.,2005. A survey of clustering schemes for mobile ad hoc networks, Communications Surveys &

Tutorials, IEEE Journals & Magazines Vol. 7, Issue 1, pp.32-48.

[12] H.Wu and X.Jia,2009. QoS multicast routing by using multiple paths/trees in wireless ad hoc networks, Ad hoc Networks.

[13] Mohammed AbuHajar, Ibrahim M.M. El Emary, Said AbuSha'ar, Ayman Murad,2009. Quality of Service Model for Dynamic Source Routing Protocol, World Applied Sciences Journal, Vol.7, Issue 4, pp.418-43.

[14] Kotecha, K.; Popat, S., "Multi-objective genetic algorithm based adaptive QoS routing in MANET," Evolutionary Computation, IEEE, pp.1423-1428, 2007.

[15] S. H. A. Wahab, M.Ould-Khaoua and S. Papanastasiou,2005. Performance Analysis of the LWQ QoS Model in MANETs", In Proc. of UKPEW, Newcastle, UK. Sec P. Rukmani and R. Ganesan / Procedia Engineering 64 ( 2013 ) 94 – 103

[16] Roja Kiran Basukala, Kyong-Heon Han, Dong-You Choi, Young Bai Kim, Seung Jo Han,2009. QoS Assurance of multimedia traffic in Residential Network with Hybrid Co ordination Function and Queuing Disciplines, Pacific Asia Conference on Circuits, Communications and System, IEEE.

[17] Sotirios Angelos Lenas, Stylianos Dimitriou, Fani Tsapeli, Vassilis Tsaoussidis,2010. Queue Management Architecture for Delay Tolerant Networking.

[18] Tetsuji Hirayama,2010. Analysis Of Multi class Feedback Queues And Its Application To A Packet Scheduling Problem, Journal of Industrial And Management Optimization, pp. 541-568.

[19] Jui Chi Chen.2012. Optimized Packet Scheduling Management: Maximizing Bandwidth Utilization for Next Generation Mobile Multimedia Communications, Wireless Pers Communication, pp.613-630.