Adaptive Approach for DSR and OLSR Routing Protocols using Optimal Probabilistic Logical Key Hierarchy in MANET

Mahesh Gochar
Depart. of Computer Science,
Govt. College of Engineering,
Ajmer, Rajasthan

Harshit Prakash Patidar
Depart. of Computer Science,
Govt. College of Engineering,
Ajmer, Rajasthan

Ravindar Singh
Depart. of Computer Science,
Govt. College of Engineering,
Ajmer, Rajasthan

ABSTRACT
wireless network with Ad hoc nature consists of mobile nodes which facilitates a fundamental architecture for communication without the support of traditional steady and fixed-positioned routers. However, the architecture must preserve communicating routes and the hosts have mobile nature and they have their restricted transmission range. There are various protocols for controlling the routing in the mobility environment. In MANET, the mobile nodes can perform the roles of both hosts and routers. Various MANET applications use for Military strategic communications and Disaster recovery mostly depended on secure node communication. For Secure Communication we use several Logical Hierarchy key protocol in Mobile Ad-hoc Network. But group key administration looks many problems because of unreliable media, less energy resources, mobile node failure. In this paper we analysis new logical key with Optimal Probabilistic Technique. In this key all node shaped in tree structure. OPLKH decreases the rekey cost and routing energy consumption in Mobile ad hoc network. In simulation we calculated the no. of rekeys cost, total energy consumption at server, key generation of energy consumption.

Keywords
Automatic-configuring infrastructure, Energy consumption, Rekey cost.

1. INTRODUCTION
Wireless communication technologies are not practical with fixed architecture for all wireless networks because of mobile nature of wireless nodes or devices. Wireless communication technologies are growing with high growth. Wireless networks with mobile nodes such as Ad hoc wireless networks must have capability to be self-organized and self-configured because of mobile nature of devices and networks.in these networks, mobile devices or hosts have a limited range to communicate with other hosts. If a host wants to send data to an another one host which is not in the range of source node then data must be expressed through the network using other nodes which can be played a role as routers for delivering the message all over the network. Broadcasting must be used for sending messages by the mobile hosts and host nodes should be in highly activate mode for accepting any message that it is been received. Hosts can be single directional that can transmit only to the one direction in the ad hoc network, so that the communicative system is not bidirectional as usually in communication systems. [5][6].

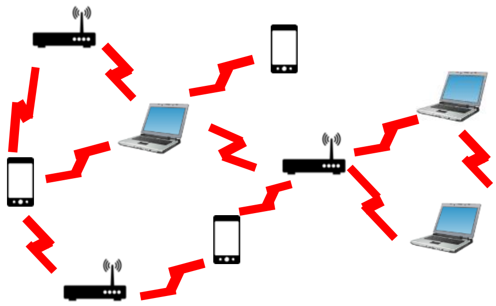


Fig.1. Infrastructure less network

Routing Protocols should have capability of handing big number of hosts with their limiting energy resources and limited bandwidths in a wireless ad hoc networks. Host mobility is the main challenge for routing protocols. by the agreement of mobility, hosts can appear and disappear at various locations. Although in ad hoc networks, all hosts of the network play their roles as routers and must have participation in route maintenance and route discovery of the routes for other nodes or hosts of the network.it is also essential for ad hoc routing protocols that reduce routing messages overhead and growing their mobility and number of hosts. Routing tables must keep smaller, because if increasing number of routing table size will also disturb control packets of host sent in the network and this disturbance increase large link overhead. [4][1].

2. OVERVIEW DSR AND OLSR ROUTING PROTOCOLS
Routing protocols finds source to destination‘s shortest path and routing protocols are categorized into 2 categories based on time of route discovery and when to discover the routes.one of main routing Protocols of Proactive routing protocol is OLSR.OLSR is a table-driven protocol. It’s one of major functionalities is, it maintains recent Reflecting latest routing information by sending control messages recurring at regular intervals between the hosts which bring up to date their routing tables. All the update forwarded all over the network, if there are any changes found in the structure. Link state routing algorithms are used by the proactive routing protocols to flood frequently the link information about its nearby nodes. On demand routing protocols are other routing protocols in which it generate routes when they have exigency of the source hosts and route maintenance is as it is required. Such protocols uses distance vector routing algorithms, these protocols have vectors that contain selective information of the path to the destination and the cost. Whenever nodes interchange vectors of their info. , each host transform possess routing information when they have exigency. As a purely

proactive or a purely reactive, the ad hoc routing protocols are also classified. But hybrid protocols are also there. [1]

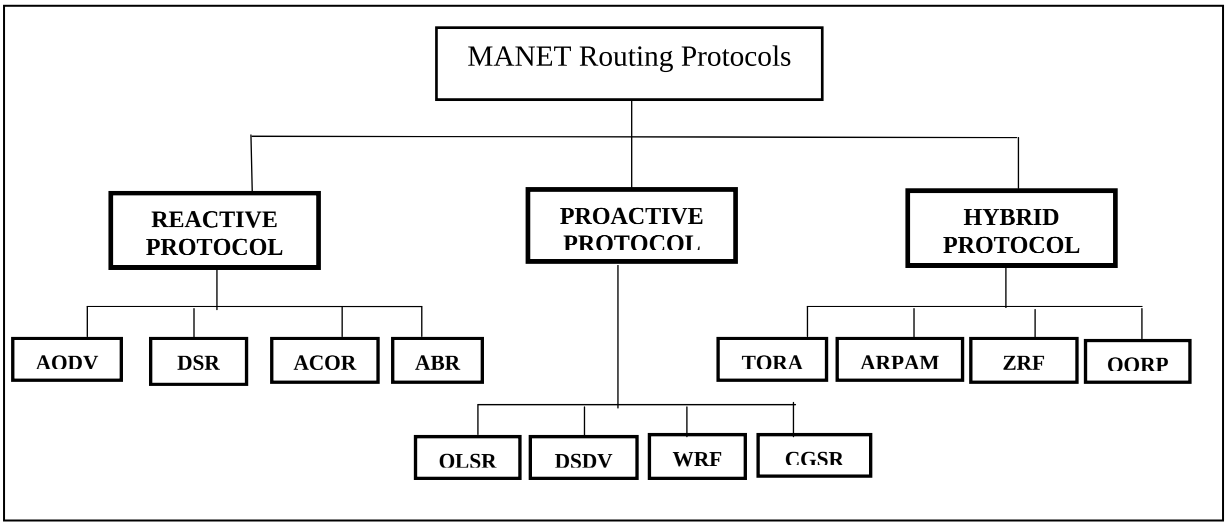


Fig. 2. Classification of Routing Protocols

2.1 Table driven (Proactive) routing protocols-

Proactive routing protocols are table driven routing protocols to broadcast the data-packets, every node has its routing table and every node need to step up connections to some other existing hosts of the networks .All the nodes of the network maintain their records related to all existing destination, required no. of hops mandatory to get in at every recorded destination in the tabular form. All the entries of routing table are labeled with a particular s. no. (Sequence number) that are produced by the destination nodes. For the stability retaining, every source node broadcasts and transforms its table of routing regularly. On the basis of routing table, how many no. of hops are required to reach a specific source node to a destination node, are calculated and which stations are receptacle measured as broadcasting of packets among the nodes. Every broadcasting data node, contain a new number with sequence and for every new route node maintain such information, given below. [1][7]

- Number of hops required to reach a particular destination node.
- New sequence no. for every destination.
- Contains destination address.

Basically, table driven protocols are more useful for the networks that contain less no. of hosts in the network. Because all the hosts need to inform their node entries to all other nodes of the network. There is more bandwidth

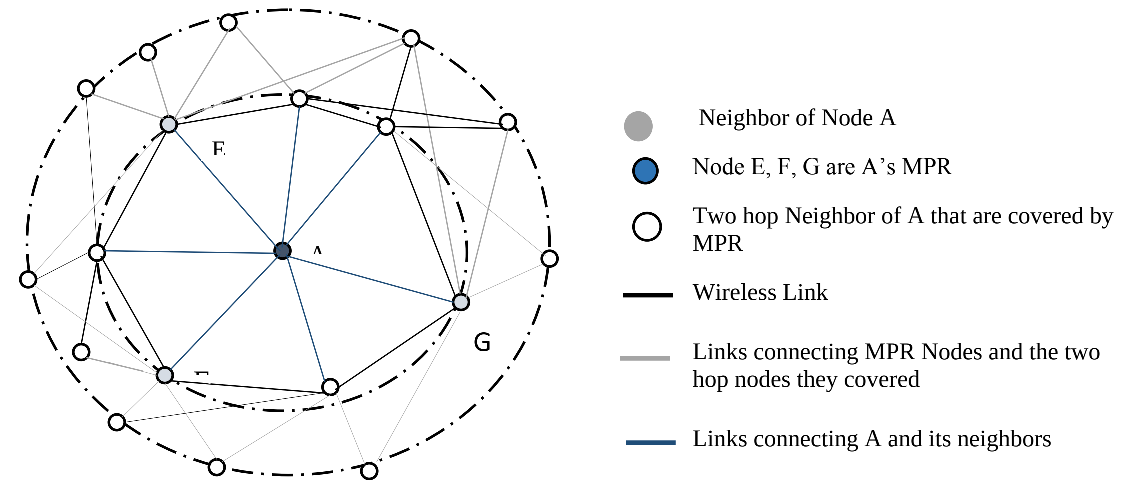
Consumption in routing table and higher routing overhead problem are resulted.

OLSR is the example of Proactive routing protocol [2]

Table Driven (proactive routing) routing protocol exchanges its routing information and statics with other existing hosts of the network.

2.1.1 OLSR-

Proactive routing protocol exchanges routing statics with other hosts in the network .Multi point Relays (MPRs) is the key idea use in OLSR.MPR is used to decrease the no. of control packets required for the data transmission. To forward traffic of data in network, a host picks its single hop symmetric neighbors termed as MPRs set that protects all hosts that are two hop away. MPR hosts or nodes have responsibility for forwarding control traffic in OLSR. While in the classical link state algorithm, all nodes forwards broadcast message. Battery consumptions can be reduced in OLSR using other existing link state algorithm [7][2][1].



OLSR: An illustration of multipoint relays

Fig.3. OLSR Routing Protocol

2.2 On Demand (Reactive Routing) Routing Protocol

On demand routing protocols determine routes on demand that's why the reactive protocol has less overhead problem as compared to proactive protocols. This type of protocols use global searching (flooding) conception. In On Demand concept, consistent updates in routing tables with newer rout topology is not required. In On Demand routing protocols, it looks for the routing in proactive method and create the link in order to send and accepting the packets from a source host or node to destination node, route discovery method is applied.by the flooding or oversupplying the RREQ(route request) packets all over the network. DSR and AODV are the example of Reactive routing protocols. [3]

2.2.1 Dynamic source routing protocol (DSR)-

DSR applies source routing concept, and DSR is one of on demand routing protocols when a source node floods packets, the transmitter node hives up hop-by-hop route to recipient node. The list of routes is cached in a source cache. Source route are kept in packet header by the data packets. Dynamic source routing applies route discovery method to send the data packets from sender node to receiver node for which it does not intimate discovery process to actively accretion such a route. In route discovery, DSR works by spreading the data packets in network with RREQ (route request) packets. In DSR, Periodic hello message transmission is not required. Dynamic Source Routing (DSR) is beaconless on demand routing protocol.

RREQ packets are found by all nearby node and continue the flood spreading process by retransmission of RREQ packets, unless it acquires destination host or its route cache consist a route for destination node. Such as a host reacts to the RREQ with a RREP (route reply) packet that is routed back to actual source node. Source routing applies route request RREQ and route reply RREP packets. The RREQ establish the path traversed all over the network. The route reply (RREP) packets routes itself back to the source by traversing this path toward the back. The source hives up backward route by RREP packets for upcoming use. If any connection on a source route is intoxicated, a route error (RERR) packet is apprised to the source host [3].

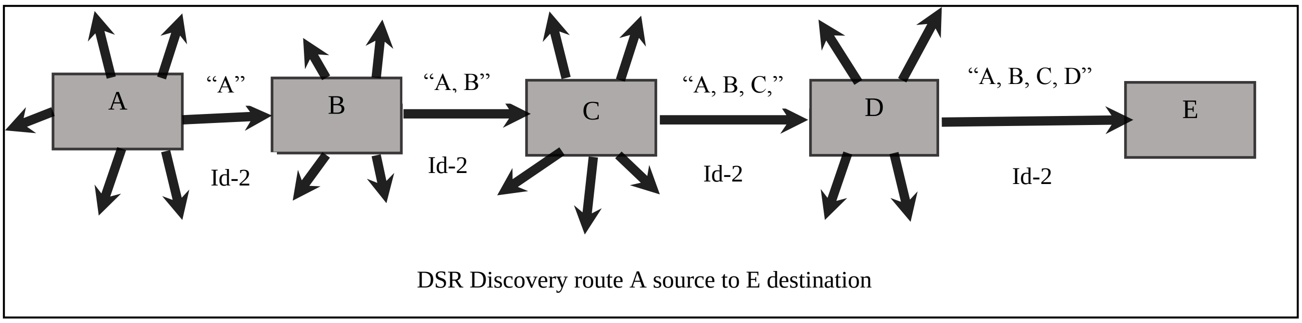


Fig.4. DSR Routing Protocol

3. DESCRIPTION OF MOBILITY MODEL

For the management of mobility, the random waypoint model (RWM) is a model of random mobility for the mobility of client users and tells about how velocity and acceleration and their location changes with respect to time. When the fresh network protocols are quantized and estimated, the random models are used for simulation purposes. Random waypoint model is one of prominent mobility model for the evaluation of mobile ad-hoc wireless network routing protocols, because of the header by the data absence of complications and widely availability. This model was firstly suggested by Jonson and

Maltz.

In randomized mobility simulation, models, the mobile nodes accelerates randomly and move freely without limitation. The destination, way and speed are all selected independently and randomly of the other nodes.

There are two variants of the random waypoint model, such as the random direction model and random walk model.[16]

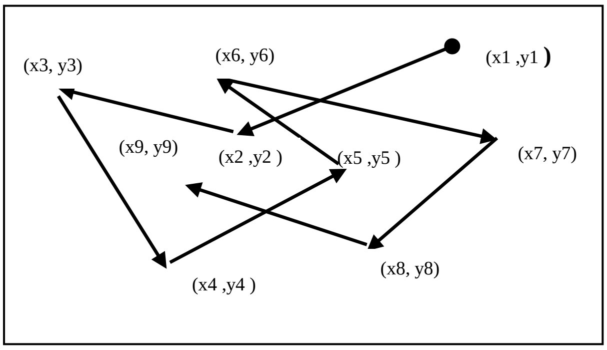


Fig. 5. Random Waypoint Model

4. ENERGY CONSUMPTION MODEL

We have computed the energy consumption for key generation proposed by Nachiketh(Nachiketh R. et. Al. 2003) and for data transmission and receiving are proposed by Dongkyun Kim (Dongkyun Kim. Et al. 2002).[7]

The required energy consumption to transmit a packet p then the energy $E(p)=i*v*t_p$ J, where, v the voltage, i is new value , J is the unit Joule and t_p the time occupied for transmission of the packet p. Energy consumption for the key setup phase using AES-128 bit key is 7.83 uJ/key. We use to simulate symmetric key of AES 128 bit length.

5. OUR APPROACH

We Analysis OPLKH [14] approaches which is the optimization for PLKH [15], which shrinkages rekey cost more. We establish the LKH tree regarding to members rekey probabilities as opposed to cumulative probability of PLKH. We focus on reduction of number rekeys that are caused due to member compromise or eviction. [10]

We have analyzed the OPLKH approaches [14] which is the optimized approach for PLHK [15], which shrinkage the rekey cost more. We establish the Logical Key Hierarchy (LKH) tree regarding to members rekey probabilities as opposed to cumulative probability of Probabilistic Logical Key Hierarchy (PLKH). We have main intention of minimizing number of rekeys that induced due to member eviction or compromise. [10].

In tree when we introduced members as leaf or ending nodes or hosts as in PLKH, we assemble for new insert-operation which place the members either as leaf node or as internal node in LKH tree based on their probabilities. When a new member M joins the group, we place member M in a position such that all ancestors of M will have higher probability and all descendants of M will have lesser probability. [11][12]

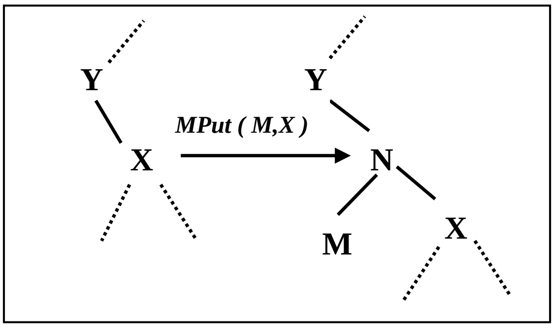


Fig.6. MPUT Operation

The LKH scheme purposes to reduce the cost of a negotiation recovery operation by adding extra encryption keys into the system. The members of the group are organized as leaves of a “logical” key tree which is preserved by the key manager. The internal nodes in this tree are rational entities which do not correspond to any real-life entities of the multicast group, but are used for key distribution purpose only. There is a key linked with each node in the tree, and each member holds a replica of every key on the path from its corresponding leaf node to the root of the tree.[14][15]

When a fellow leaves the group his related corresponding physical node is to be removed from the tree. The physical node may be an internal node or a leaf node based on how it injected and whether it has any dependent nodes at present. In OPLKH, delete procedure removes a physical node only if it’s a leaf node; otherwise, delete operation sets its type as consumable and refresh affected keys. [14][15]

By the development of the centralized key management, as in, the tree-key scheme is improved and reduce the cost of re-keying from Probability 0 (n) to 0 (log n), where n denotes the group size. It is accepted OPLKH method to MANET and analyzed the rekey cost and energy consumption for data transmission and routing in MANET.[12]

6. PROPOSED METHODOLOGY FOR THE MANET

In this method we, have concentrated on reducing the cost of rekey of LKH based protocols by organising the tree based on rekey probabilities of nodes.

As in OPLKH [14], we have implemented all the logical actions of OPLKH into MANET atmosphere. In MANET, we have chosen clusterhead as key-server because there is no key server. To select the clusterhead we have used weighted clustering algorithm (WCA) [13]. As rekey probability is one of the issues to cause re-clustering we have considered rekey probability to be another factor to WCA [13] algorithm.

The WCA has the flexibleness of taking combined effect of the degree and assigning different weights of ideality, node mobility battery power and transmission power. The modified WCA algorithm as follows:

Cluster head Selection Technique

Step 1: Find the nearby node of each node v (i.e. nodes within its broadcast range). This gives the degree, $\mathbf{d_v}$, of this node. **H** is number of nodes that can be handled by a clusterhead.

Step 2: Calculate the degree-difference, $\mathbf{D_v = | d_v – H|}$, for every node **v**.

Step 3: For every node, compute the sum of the distances, $\mathbf{S_v}$, with all its neighbors.

Step 4: Calculate the average running speed for every node v. This provides the mobility of the nodes **v** and it is denoted by $\mathbf{M_v}$.

Step 5: Calculate consumed battery power, $\mathbf{T_v}$. Since we have assumed that consumption of battery power is greater for a clusterhead than for an ordinary node.

Step 6: Calculate the combined weights $I_v = \mathbf{c_1 * D_v + c_2 * S_v + c_3 * M_v + c_4 * T_v}$, for each node **v**.

For the corresponding system parameters, these coefficients $\mathbf{c_1, c_2, c_3, c_4}$ are the weighting factors

Step 7: Calculate the average of all nodes weights, **AI,** and also compute the average of all nodes rekey probabilities, **ARP**.

Step 8: Now check for each node **v**,

If (weight $\mathbf{I_v < AI}$ and also corresponding rekey probability, $\mathbf{RP_v < ARP}$)

Then Calculate the new weight $\mathbf{NI_v = I_v} * 0.001 + \mathbf{RP_v}$.

Step 9: Choose the node of minimum $\mathbf{NI_v}$ to be the cluster head.

By using the modified WCA algorithm, primarily we choose the best node as clusterhead from the existing nodes to escape re-clustering. The following key features are considered in this weighted clustering algorithm [13].

(a) The clusterhead selection procedure is aperiodic and it is invoked as hardly as possible. It reduces system updates and reduces computational and communicational costs.

(b) To ensure efficient MAC functioning, each clusterhead can ideally support a pre-define system threshold nodes. By optimizing or limiting the number of node in each cluster, the system's high throughput can be achieved.

(c) The battery power can be professionally used within certain transmission range. If a node works as a clusterhead rather than an ordinary node, Consumption of the battery power is more.

(d) Mobility is a significant factor in deciding the clusterheads. Re-affiliation occurs when one of the ragular nodes moves out of a cluster and joins another existent cluster. [13]

7. SIMULATION RESULT AND ANALYSIS

We have simulated Optimal Probabilistic Logical Key in Mobile Ad hoc Network. Our Simulation is implemented on C++ platform. We have implemented experiment on groups of 128, 256, 512, 768, 1024 nodes. For each experiment, we have produced the joining/leaving of nodes randomly, in addition, some members may leave/join based on connection failure or availability and some members may leave because of power exhaustion. For each leave/join operation we have documented energy consumption for key generation, the numbers of rekeys generated and energy consumption at key-server .We have categorized three categories namely static, semi-dynamic and dynamic based on number of leaves and rekey probabilities in OPLKH approach. But in MANET we added some extra parameters to classify these categories. The additional parameters are pause time, updating interval time and node mobility.

The additional parameter are listed in Table 1. In simulation for every updating interval time we have updated the node positions and routing tables.

Simulation Results

In our simulation, we have calculated the numbers of rekeys and energy consumption for routing, data transmission and key generation in static, semi-dynamic and dynamic scenarios for each group size of 128, 256, 512, 768 and 1024.

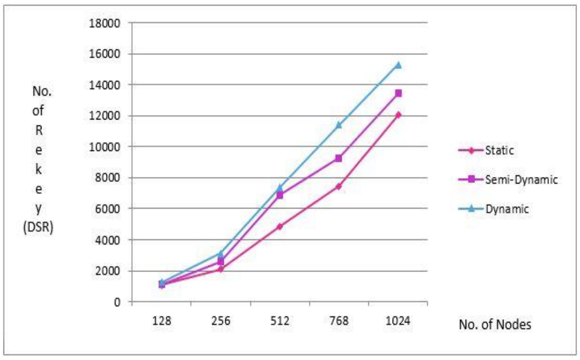


Table 1: Simulation Parameter and results

Simulation Parameters	Static	Semi-Dynamic	Dynamic
Mobility	0-5 m / s	0-10 m / s	0-20 m / s
Packet Size	256 bytes	256 bytes	256 bytes
Mobility Model	Random Waypoint	Random Waypoint	Random Waypoint
Pause Time	0-10 sec	0-5 sec	0 sec
Updating interval time	10 sec	5 sec	1 sec
No. of leaves	¼ of Group Size	½ of Group Size	¾ of Group Size
Area (in sq. m)	800x800	800x800	800x800
Energy	0-1000 J	0-1000 J	0-1000 J

Fig.7. Graph between No. of Nodes and No. of Rekey in case of DSR

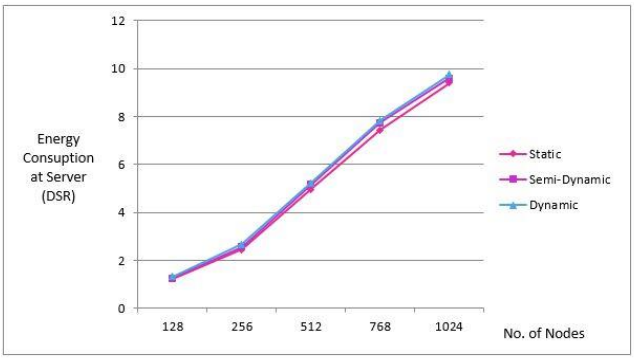


Fig.8. Graph between No.of Nodes and Energy Consuption At server in case of DSR

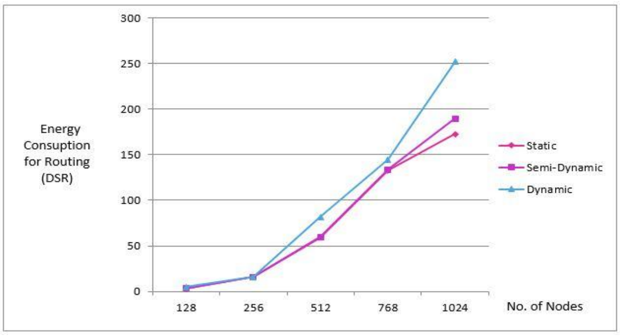


Fig.9. Graph between No. of Nodes and Energy Consumption for Routing in case of DSR

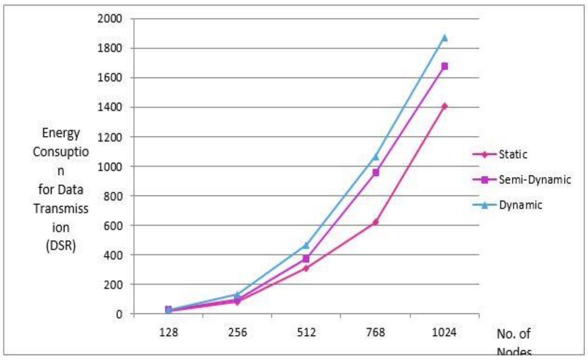


Fig.10.Graph between No. of Nodes and energy Consumption for data Transmission in case of DSR

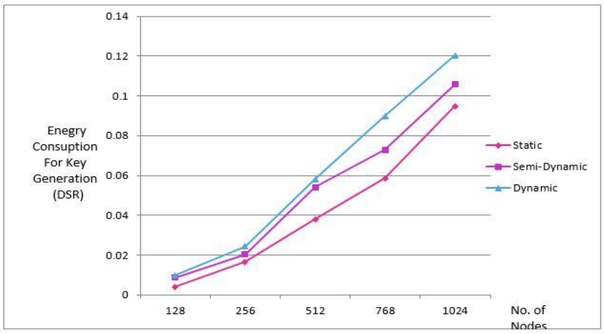


Fig. 11. Graph between No. of Nodes and energy Consumption for key Generation in case of DSR

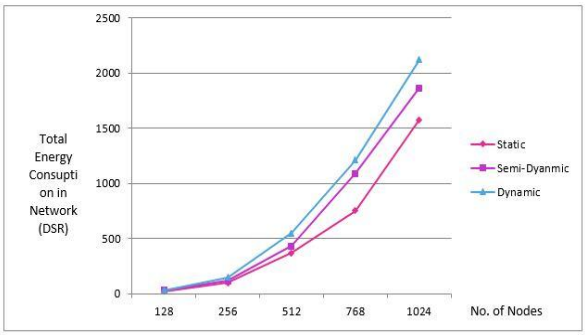


Fig.12. Graph between Total Energy Consumption and No. of Nodes in Network for DSR

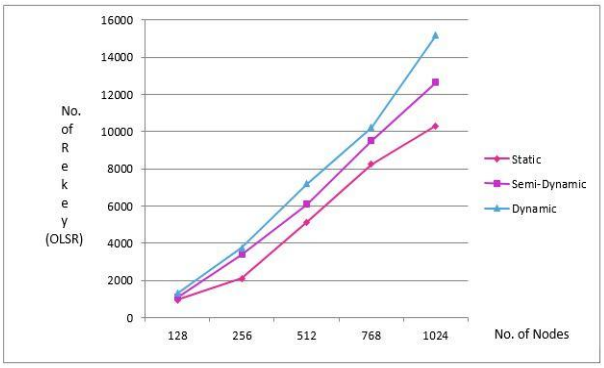


Fig.13. Graph between No. of Nodes and No. Of Rekey Cost in case of OLSR

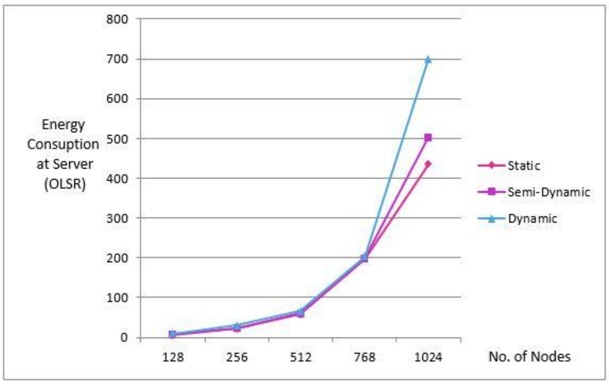


Fig.14. Graph between No. of Nodes and Energy Consumption at server in case of OLSR

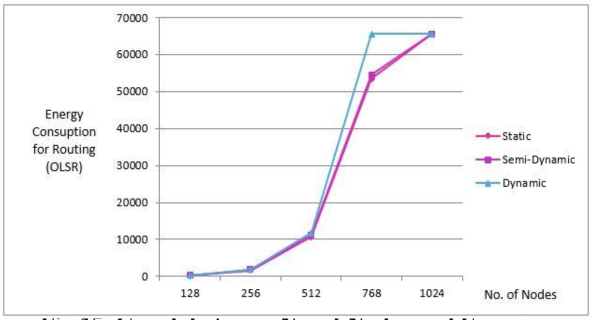


Fig.15. Graph between No. of Nodes and Energy Consumption for routing in case of OLSR

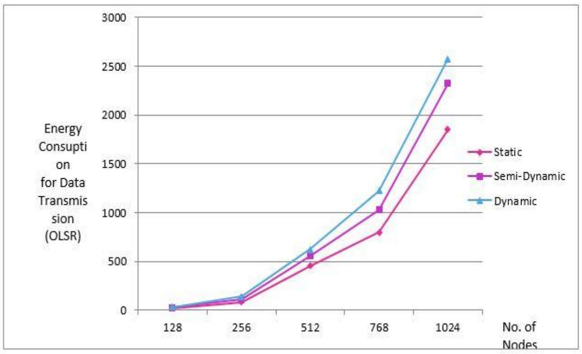


Fig.16. Graph between No. of Nodes and Energy Consumption for data Transmission in case of OLSR

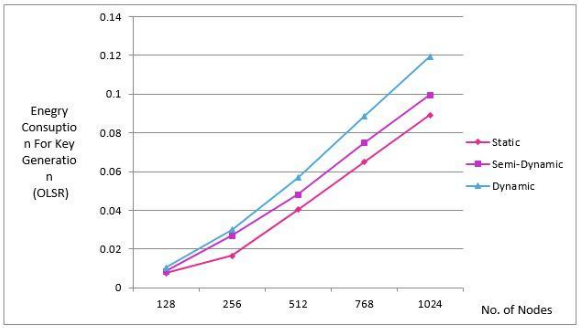


Fig.17. Graph between No. of Nodes and Energy Consumption for key Generation in case of OLSR

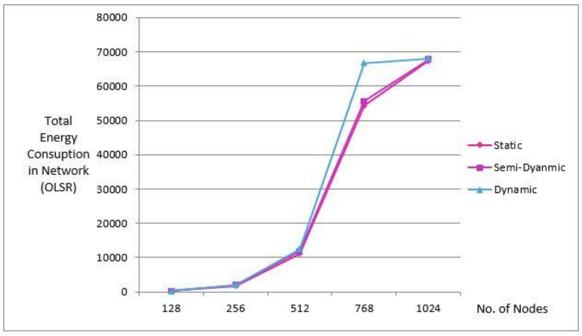


Fig.18. Graph between No. of Nodes and Total Energy Consumption In network in case of OLSR

8. CONCLUSION

In Mobile Ad-hoc Network, a most challenging problem is Secure Group Communication. Reasons behind this challenging problem are centralization of administration, power consumptions and lack of fixed infrastructure. Power resources are limited for nodes in Mobile Ad-hoc Networks. We have analyzed the logic of optimal probabilistic Logical Key Hierarchy logic, this reduces rekey cost. Reduction of rekey cost reduces the cost of energy data transmission and consumption of energy, which increases the long existence of Mobile Ad-hoc Network.

9. REFERENCES

[1] T. Clausen and P. Jacquet "Optimized Link State Routing Protocol (OLSR)." RFC 3626, IETF Network Working Group, October 2003.

[2] Ying Ge, Thomas Kunz and Louise Lamont "Quality of Service Routing in Ad-Hoc Networks Using OLSR."Proceeding of the 36th Hawaii International Conference on System Science (HICSS'03)

[3] COMPARISON OF EFFECTIVENESS OF AODV, DSDV AND DSR ROUTING PROTOCOLS IN MOBILE AD HOC NETWORKS by Sapna S. Kaushik & P.R. Deshmukh

[4] Xiaoyan Hong, Kaixin Xu and Mario Gerla "Scalable Routing Protocols for Mobile Ad Hoc Networks. "Computer Science Department, University of California, Los Angeles, August 2002.

[5] Koey Huishan, Chua Huimin and Koh Yeow Nam "Routing Protocols in Ad hoc Wireless Networks." National University of Singapore.

[6] Toa Lin, Scott F. Midkiff and Jahng S. Park "A Framework for Wireless Ad Hoc Routing Protocols. "Bradley Department of Electrical and Computer Engineering. Virginia Polytechnic Institute and State University. Blacksburg Virginia. 2003

[7] S. Corson and J. Macker "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations." RFC 2501, IETF Network Working Group, January 1999.

[8] P. Jacquet, P. Mühlethaler, T Clausen, A. Laouiti, A.Qayyum and L. Viennot "Optimized Link State Protocol for Ad Hoc Networks." IEEE INMIC Pakistan 2001.

[9] A. Laouti, P. Mühlethaler, A. Najid and E. Plakoo "Simulation Results of the OLSR Routing Protocol for Wireless Network." 1st Mediterranean Ad-Hoc Networks workshop (Med-Hoc-Net). Sardegna, Italy2002.

[10] P. Jacquet, A. Laouiti, P. Minet and L. Viennot "Performance of multipoint relaying in ad hoc mobile routing protocols." Networking 2002. Pise (Italy) 2002.

[11] Anne Marie Hegland et al., "Survey of key management in adhoc networks" , in Proc. IEEE communications surveys-2006.

[12] Jun Li, Guohua Cui, Xiaoqing Fu, Zhiyuan Liu, Li Su, "A Secure Group Key Management Scheme in Mobile Ad Hoc Networks", IEEE Computer Society Press, 2005.

[13] Jayanta Biswas, S. K. Nandy, "Efficient Key Management and Distribution for MANET", in Proc. ICC IEEE, 2006

[14] K.Gomathi, B.Parvathavarthini, "An Efficient Cluster based Key Management Scheme for MANET with Authentication", Trendz in Information Sciences & Computing (TISC), IEEE 2010.

[15] M. Chatterjee, S. K. Das, and D. Turgut, "An On-Demand Weighted Clustering Algorithm (WCA) for Ad hoc Networks", in Proc. of IEEE Globecom'00, 2000.

[16] Alwyn R. Pais, Shankar Joshi,"A new probabilistic rekeying method for secure multicast groups", in Proc. International Journal of Information Security- (2010) 9:275–286.

[17] Ali Aydın Selcuk, Deepinder Sidhu, "Probabilistic optimization techniques for multicast key management", in Proc Elsevier Science 2002.

[18] http://www.digplanet.com/wiki/Random_waypoint_model