International Journal of Computer Engineering and Information Technology

VOL. 8, NO. 5, May 2016, 71–78
Available online at: www.ijceit.org
E-ISSN 2412-8856 (Online)

Adoptive Approach of DSR and OLSR Routing Protocols using Optimal Probabilistic Logical Key Hierarchy in MANET

Harshit Prakash Patidar[1] and Mahesh Gocher[2]

[1, 2] Department of Computer Science Govt. Engineering College, Ajmer, Rajasthan

ABSTRACT

An ad hoc wireless network consists of mobile networks which prevents a fundamental architecture for communication without the support of traditional fixed-position routers. Nevertheless, the architecture must preserve communication routes although the hosts are mobile and they have restricted transmission range. There are different protocols for controlling the routing in the mobile 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 technology is growing daily, with such growth sooner or later it would not be practical or simply physically possible to have a fixed architecture for this kind of network. Ad hoc wireless network must be capable to self-organize and self-configure due to the fact that the mobile structure is moving all the time. Mobile hosts have a limited range and sending the message to another host, which is not in the sender's host transmission range, must be forwarded through the network using other hosts which will be operated as routers for delivering the message throughout the network. The mobile host must use broadcast for sending messages and should be in promiscuous mode for accepting any messages that it receives. In the ad hoc network there can be unidirectional hosts, that can transmit only to the one direction, so that the communication is not bi-directional as in the usual communication systems [6][5].

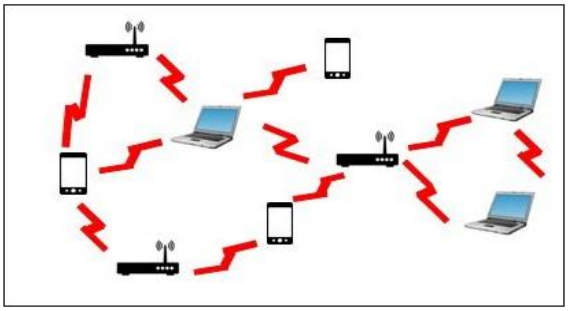

Fig.1. Infrastructure less network

The routing protocols for ad hoc wireless network should be capable to handle a very large number of hosts with limited resources, such as bandwidth and energy. The main challenge for the routing protocols is that they must also agreement with host mobility, meaning that hosts can appear and disappear in various locations. Thus, all hosts of the ad hoc network act as routers and must participate in the route discovery and maintenance of the routes to the other hosts. For ad hoc routing protocols it is essential to reduce routing messages overhead despite the growing number of hosts and their mobility. Keeping the routing table small is another important subject, because the increase of the routing table will disturb the control packets sent in the network and this in turn will disturb large link overheads [1][4].

2. OVERVIEW DSR AND OLSR ROUTING PROTOCOLS

Routing protocols are divided into two categories based on how and when routes are discovered, but both find the

shortest path to the destination. Proactive routing protocols are table-driven protocols, they always maintain recent up-to-date routing information by sending control messages periodically between the hosts which update their routing tables. When there are changes in the structure then the updates are propagated throughout the network. The proactive routing protocols use link-state routing algorithms which frequently flood the link information about its neighbours. Other routing protocols are on-demand routing protocols, in other arguments reactive, ones which generate routes when they are needed by the source host and these routes are maintained while they are needed. Such protocols use distance-vector routing algorithms, they have vectors containing information about the cost and the path to the destination. When nodes exchange vectors of information, each host transform own routing information when needed. The ad hoc routing protocols are usually classified as a pure proactive or a pure reactive protocol, but there are also hybrid protocols. This only concern flat routing protocols, but there are also hierarchical and graphic position assisted routing protocols [1].

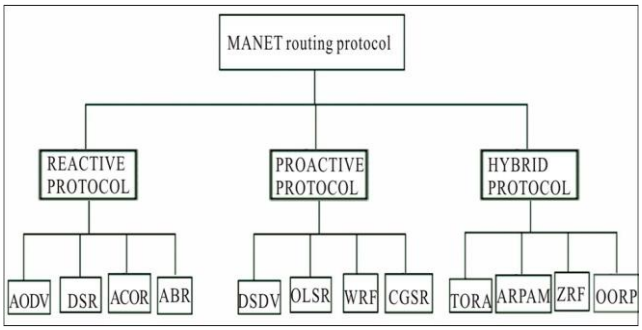

Fig. 2. Classification of Routing Protocols

2. 1 Proactive (Table driven) Routing Protocols

Each node in the network has routing table for the broadcast of the data packets and need to establish connection to other nodes in the network. These nodes record for all the presented destinations, number of hops mandatory to arrive at each destination in the routing table. The routing entry is labelled with a sequence number which is created by the destination node. To retain the stability, each station broadcasts and transforms its routing table from time to time. How many hops are mandatory to arrive that particular node and which stations are accessible is result of broadcasting of packets between nodes. Each node that broadcasts data will contain its new sequence number and for each new route, node contains the following information: [1][7]

- How many hops are compulsory to arrive that particular destination node
- Generation of new sequence number marked by the destination
- The destination address

The proactive protocols are suitable for less number of nodes in networks, as they need to inform node entries for each and every node in the routing table of every node. It results more Routing overhead problem. There is consumption of more bandwidth in routing table.
Example of Proactive Routing Protocol is (OLSR)[2]

OLSR:

Proactive routing protocol exchanges routing statistics with other nodes in the network. The key idea used in OLSR is of MPRs (Multi Point Relays). It is improved to decrease the number of control packets required for the data transmission using MPRs. To forward data traffic, a node picks its one hop symmetric neighbours, termed as MPR set that protections all nodes that are two hops away. In OLSR, only nodes, selected as MPRs are responsible for forwarding control traffic. The selected MPRs forward broadcast messages during the flooding process. Contrarily to the classical link state algorithm, where all nodes forward broadcast messages. So mobile nodes can reduce battery consumption in OLSR associated with other link state algorithms [1][2][7].

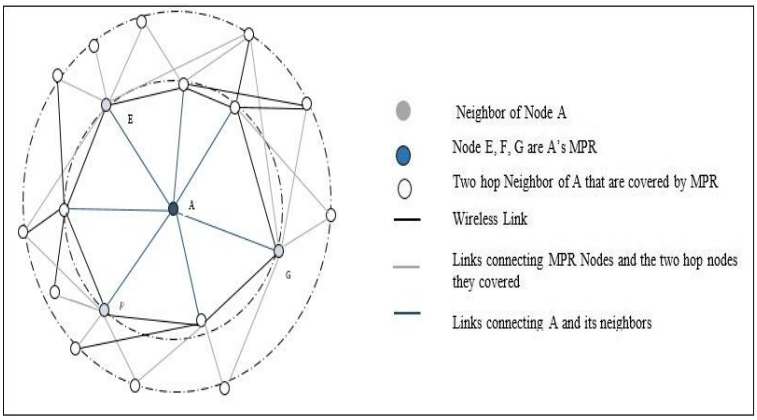

Fig.3. OLSR Routing Protocol

2.2 Reactive (On demand) Routing Protocol

Reactive Protocol has lesser overhead since routes are determined on demand. It employs flooding (global search) concept. Constantly updation of route tables with the newest route topology is not required in on demand concept.
Reactive protocol searches for the route in an on-demand manner and set the link in order to send out and accept the packet from a source node to destination node. Route discovery method is used in on demand routing by flooding the route request (RREQ) packets throughout the network.
Examples of reactive routing protocols are the dynamic

source Routing (DSR), ad hoc on-demand distance vector routing (AODV) [3].

Dynamic source routing protocol (DSR):

DSR uses source routing concept. When packets are flooded by a source node, the sender node caches complete hop-by-hop route to the receiver node. These route lists are caches in a route cache. The data packets carry the source route in the packet header. DSR uses Route Discovery method to send the data packets from sender to receiver node for which it does not previously know the route, it uses a route discovery process to dynamically determine such a route. In Route discovery DSR works by flooding the data packets in network with route request (RREQ) packets. RREQ packets are received by every neighbor nodes and continue this flooding process by retransmissions of RREQ packets, unless it gets destination or its route cache consists a route for destination .Such a node replies to the RREQ with a route reply (RREP) packet that is routed back to real source node. Source routing uses RREQ and RREP packets. The RREQ builds up the path traversed across the network. The RREP routes itself back to the source by traversing this path toward the back. The source caches backward route by RREP packets for upcoming use. If any connection on a source route is intoxicated, a route error (RERR) packet is notified to the source node [3].

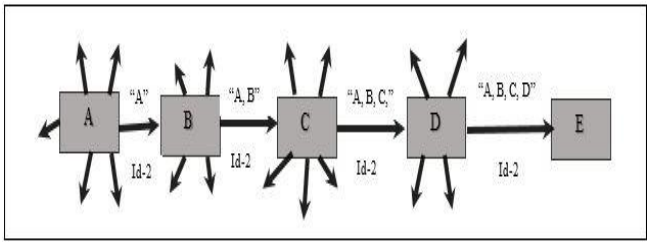

Fig.4. DSR Routing Protocol

3. DESCRIPTION OF MOBILITY MODEL

In mobility management, the random waypoint model is a random model for the movement of mobile users, and how their location, velocity and acceleration change over time. Mobility models are used for simulation purposes when fresh network protocols are estimated. The random waypoint model was first suggested by Johnson and Maltz. It is one of the most popular mobility models to evaluate mobile ad hoc network (MANET) routing protocols, because of its simplicity and wide availability.

In random-based mobility simulation models, the mobile nodes move randomly and freely without limitations. To be more specific, the destination, speed and way are all chosen randomly and independently of other nodes. This kind of model has been used in many simulation educations.

Two variants, the random walk model and the random direction model are variants of the random waypoint model [16].

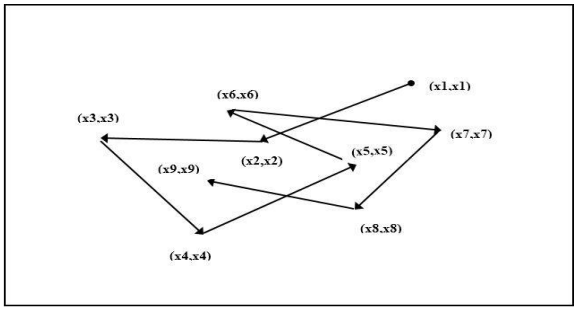

Fig. 5. Random Waypoint Model

4. ENERGY CONSUMPTION MODEL

We have calculated 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 energy consumption required to transmit a packet p then the energy E(p)=i*v*tp Joules, where i is new value, v the voltage, and tp the time occupied to transmit 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 with respect to members rekey probabilities as opposed to cumulative probability of PLKH. We focus on reducing number of rekeys that are caused due to member compromise or eviction. [10]

In tree when we introduced members as leaf nodes 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 descendents of M will have lesser probability. [11][12]

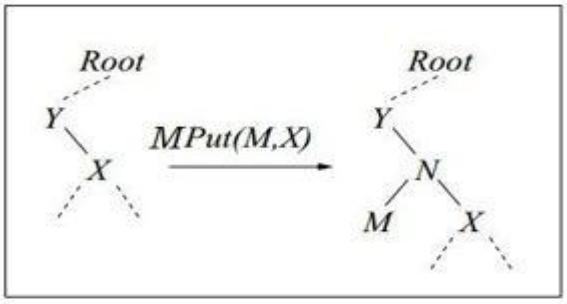

Fig.6. MPUT Operation

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 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]

From the development of the centralized key management, as in, the key-tree scheme is improved and reduce the cost of re-keying from Probability 0 (n) to 0 (log n) (where n is the group size).We 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 largely concentrated on minimizing the rekey cost of LKH based protocols by organizing 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 flexibility of assigning different weight and takes into an account a combined effect of the ideal degree, transmission power, mobility and battery power of the nodes. The modified WCA algorithm as follows:

Clusterhead Selection Technique

Step 1: Find the neighbors of each node v (i.e. nodes within its broadcast range). This gives the degree, dv, of this node. H is number of nodes a clusterhead can handle.

Step 2: Calculate the degree-difference, Dv = | dv – H|, for every node v.

Step 3: For every node, compute the sum of the distances, Sv, with all its neighbors.

Step 4: Calculate the running average of the speed for every node v. This provides the mobility of the nodes v and it denoted by Mv.

Step 5: Calculate consumed battery power, Tv. Since we assumed that consumption of battery power is more for a clusterhead than for an ordinary node.

Step 6: Calculate a combined weight Iv = c1 * Dv + c2 * Sv + c3 * Mv + c4 * Tv, for each node v.

The coefficients c1, c2, c3, c4 are the weighting factors for the corresponding system parameters.

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 Iv < AI and also corresponding rekey probability, RPv < ARP)

Then Calculate the new weight NIv = Iv * 0.001 + RPv.

Step 9: Choose the node with minimum NIv to be the cluster head.

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

(a) The clusterhead election procedure is not periodic and invoked as hardly as possible. This reduces system updates and hence computation and communication costs.

(b) Each clusterhead can ideally support a pre-defined system threshold nodes to ensure efficient MAC functioning. A high throughput of the system can be achieved by limiting or optimizing the number of node in each cluster.

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

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

7. SIMULATION RESULT AND ANALYSIS

We have simulate Optimal Probabilistic Logical Key in Mobile Ad hoc Network. Simulation is implement in C++ language. We 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 because of power exhaustion and some members may leave/join based on connection failure or availability. For each leave/join operation we have documented the numbers of rekeys generated, energy consumption for key generation and energy consumption at key-server.

In OPLKH approach, we have categorized three categories namely static, semi-dynamic and dynamic based on number of leaves and rekey probabilities. But in MANET we added some extra parameters to classify these categories. The additional parameters are pause time, node mobility and updating interval time. The additional parameter are listed in Table 1. In simulation for every updating interval time we have updated the node positions and routing tables.

Table 1: Simulation Parameter

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

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.

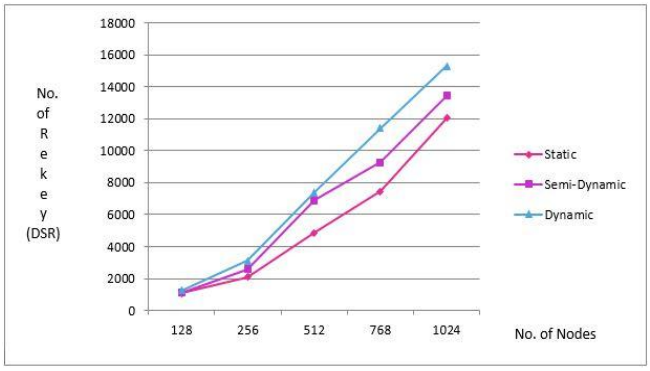

Fig.7. Graph between No. of Nodes and No. of Rekey in case of DSR

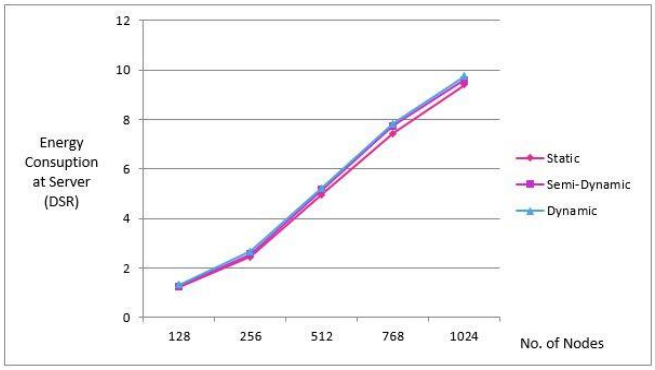

Fig.8. Graph between No.of Nodes and Energy Consumption At server in case of DSR

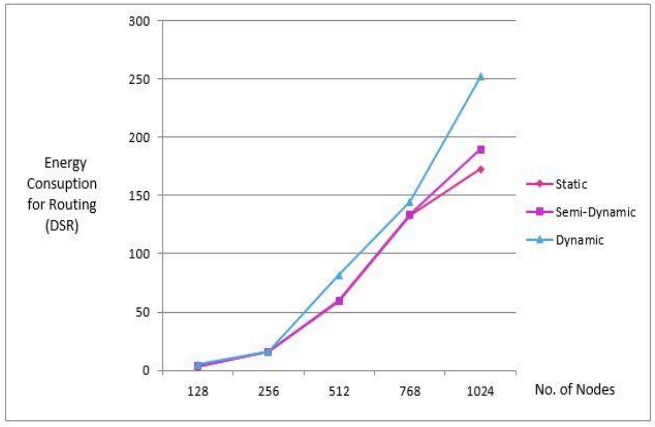

Fig.9. Graph between No. of Nodes and Energy Consumption for Routing in case of DSR

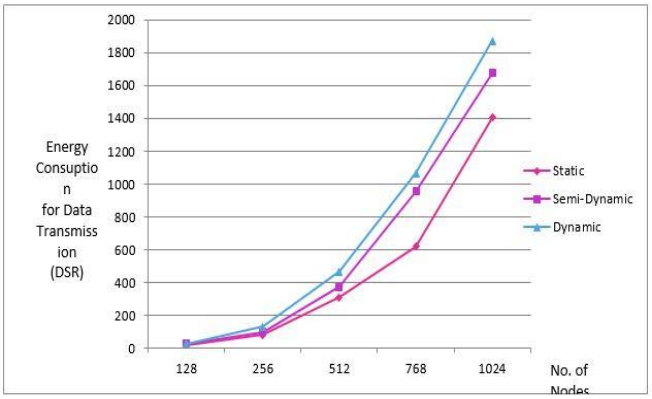

Fig.10.Graph between No. of Nodes and energy Consumption for data Transmission in case of DSR

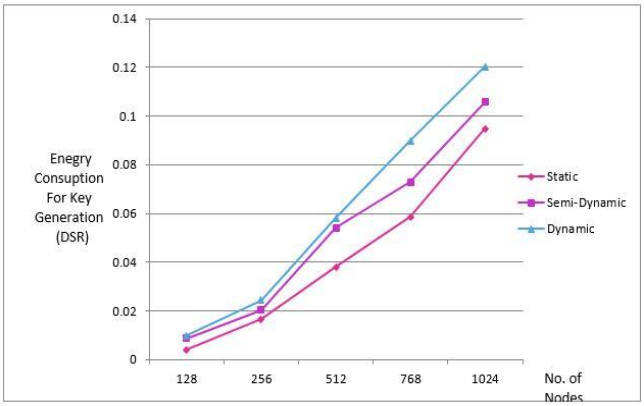

Fig. 11. Graph between No. of Nodes and energy Consumption for key Generation in case of DSR

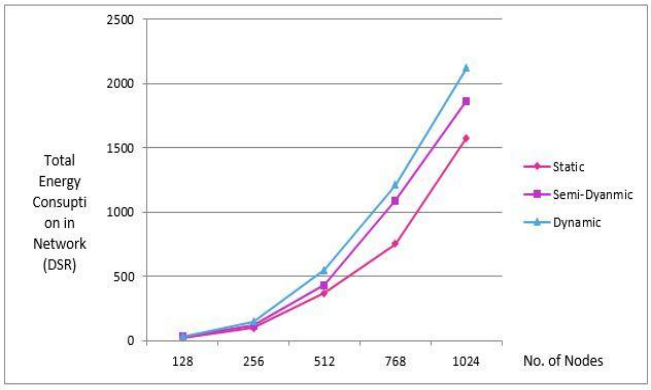

Fig.12. Graph between No. of Nodes and Total Energy Consumption in Network in case of DSR

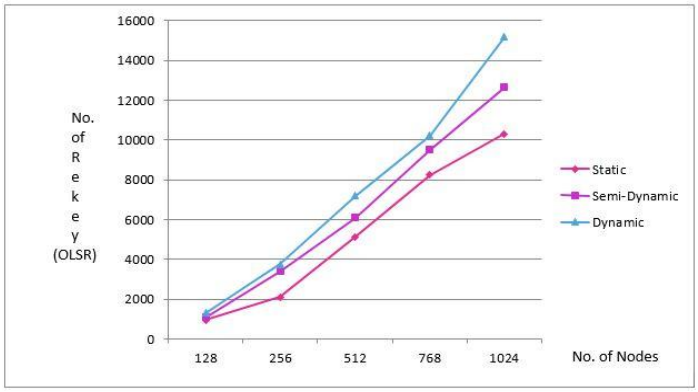

Fig.13. Graph between No. of Nodes and No. Of Rekey Cost in case of OLSR

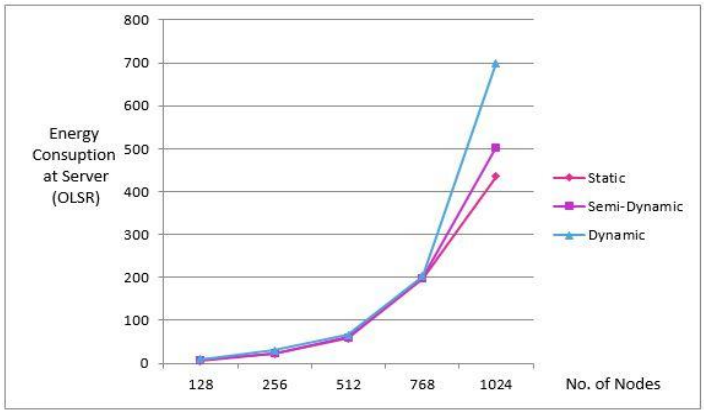

Fig.14. Graph between No. of Nodes and Energy Consumption at server in case of OLSR

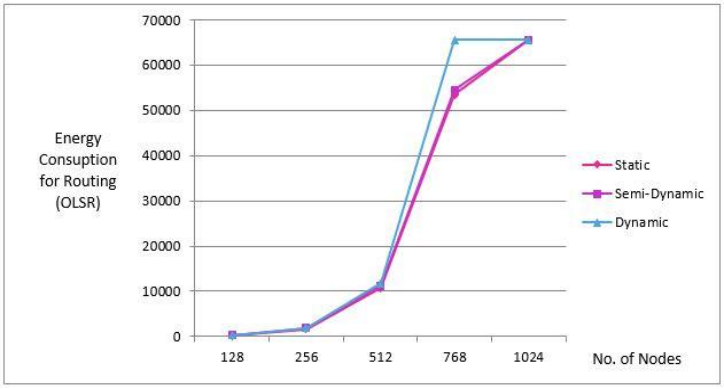

Fig.15. Graph between No. of Nodes and Energy Consumption for routing in case of OLSR

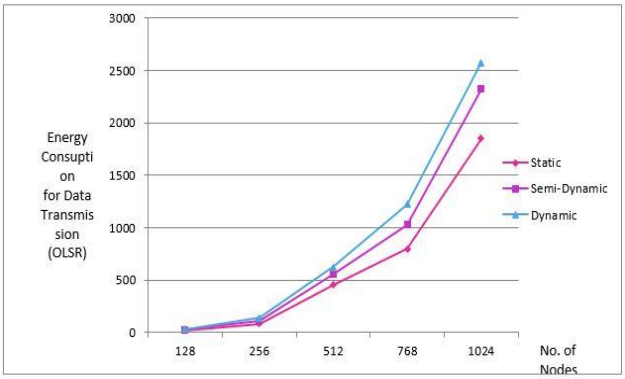

Fig.16. Graph between No. of Nodes and Energy Consumption for data Transmission in case of OLSR

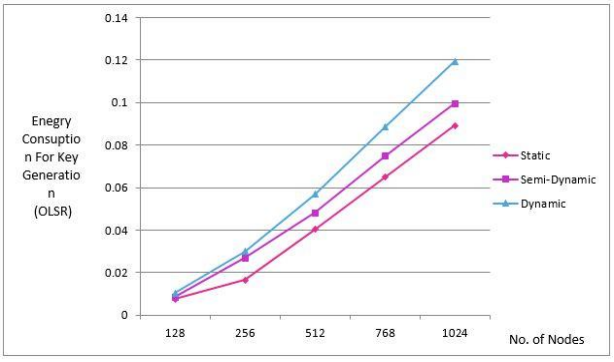

Fig.17. Graph between No. of Nodes and Energy Consumption for key Generation in case of OLSR

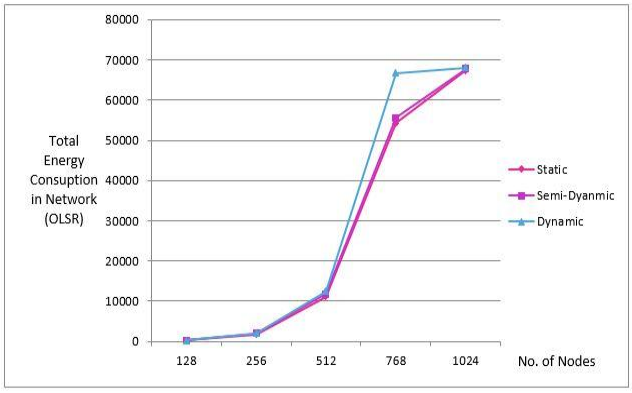

Fig.18. Graph between No. of Nodes and Total Energy Consumption In network in case of OLSR

8. CONCLUSION

In Mobile Ad-hoc Network, Secure Group Communication is a most Challenging Problem because of centralized administration, lack of fixed infrastructure and power Consumption. In Mobile Ad-hoc Network, node has limited power resource. We have Analysis Optimal probabilistic Logical Key Hierarchy logic which reduce rekey cost. Reducing Re-key cost means reducing the cost of Energy data transmission and Energy Consumption, which leads to long existence of Mobile Ad-hoc Network.

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