Journal of Theoretical and Applied Information Technology
31st March 2014. Vol. 61 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A HYBRID CLUSTER ENHANCED SECURE MULTICAST ROUTING SCHEME FOR MANET

[1]GEETHA G, [2]DR.N.J.R.MUNIRAJ,
[1]Research Scholar, Karpagam University, Coimbatore
[2] Principal, Tejaa Shakthi Insitute of Technology, Coimbatore
E-mail: [1]gopikagokul5@gmail.com

ABSTRACT

Mobile Ad hoc networks consist of mobile node without having any centralized access point. Due to dynamic nature, lack of Network integrity and authentication may likely to occur. To avoid this, several approaches have focused on authentication. In this research work, hybrid cluster enhanced Secure Multicast Routing Scheme is proposed to make network more secure. The main of the proposed work is to protect mobile nodes and its packets against attackers. In the presence of network attackers, performance will be degraded. The proposed scheme consists of three phases i.e. Cluster based Multicast routing, cluster head election and secret sharing scheme. The multicast routing is proposed to avoid misbehavior and route failures. Cluster head election is performed based on characteristics and behaviour of mobile nodes. Secret sharing scheme is used to provide node integrity and authentication. By using simulation results, HCSMR achieves better performance in terms of packet delivery ratio, delay, overhead, network lifetime, network integrity rate than the existing method EESMR, PLSS and LAER schemes.

Keywords: *MANET, Multicast Routing, Cluster Head Election, Secret Sharing Scheme, Authentication, Integrity, Mobility, Packet Delivery Ratio, Network Lifetime, Number Of Nodes, Throughput, Overhead And End To End Delay.*

1. INTRODUCTION

1.1. Multicast Routing in MANET

In Mobile Ad hoc networks, multicast packets are delivered to each member of a multicast group with the same best-efforts reliability and performance as unicast packets to members. Multicast groups may be of arbitrary size, may change membership dynamically, and may have either a global or local scope. The senders do not need to know membership groups, and needs not to be a member of that group.

The aim of multicasting is to deliver data to a set of selected receivers. There is no restriction on the location or number of members in a host group. Multicast can be classified into one to many or many to many communication applications. The important member identifications and functions are: group member, sources, destination, forwarding nodes, non-group member. The group membership is dynamic means that hosts may join and leave groups at any time.

1.2. Need for Wired and Wireless Multicasting

Mobile ad hoc networks characteristics can be considered while the design of multicast protocol [1], which are; limited Bandwidth, wireless links are error-prone, mobile hosts frequently handoff, and limited battery life of mobile device. On the other hand minimizing network resources consumptions and overheads are important for optimum design consideration. The movement and mobility of receivers or senders creates considerations that affect the network performance, the following are the considerations:

Routing Strategy: Tree construction, core placement, routing state maintenance, tunnelling, and network inactivity.

Destination behaviour: Join latency, packet loss, packet duplication, packet out of order, and leave latency.

Route Deployment consideration: packet delivery rate, quality of Service (QoS), scalability, interoperability, service pricing, and security.

The major use of multicast mechanisms is to overcome the above problems, however, there are tradeoffs, so a solution may add either overhead to the network or encounters delays. However, these

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

solutions try to solve specific problems and aims to the optimum routing efficiency.

2. RELATED WORK

In this paper [2], Entropy-based Stability QoS Routing with Priority scheduler is proposed using fuzzy controllers (ESQRP). This scheme produced significant improvements in data transmission rate, and average end-to-end delay. This algorithm is used to construct the new metric-entropy, select the stability path with the help of entropy metric and to reduce the number of route reconstruction

In this paper [3], Energy Efficient, Secure and Stable Routing Protocol is proposed to incorporate security and power features in ad hoc networks. It takes care of basic security needs and uses concept of Hash Key generation to attain the goal of security. Moreover, it uses route table entry for its power status.

In this paper [4], the aim is to find an efficient and secure communication in wireless ad hoc networks. This proposed scheme is used to generate stable link between source and destination. But no effort has been made to avoid tunneling attacks, selectively drop attacks.

In this paper [5], an efficient Trust based Multipath Route Discovery is focused with improved Route Lifetime. The algorithm is proposed to provide trust based solution for the Security attacks which affects the routing protocol performance. It considers the lifetime of the route, trust value of the route, as a metric for route discovery and also malicious node detection.

In this paper [6], an effective mechanism is proposed for AODV called modified AODV to detect and react to wormhole attacks and enhance the stability for MANETs. It is particularly a challenging attack to defend against wormhole attack. It was presented a mechanism for detecting and thus defending against wormhole attacks

In this paper [7], both link and node stability was considered. This technique is .expected to provide highly stable, reliable, robust node disjoint paths. As the paths are node disjoint, energy drain rate of the nodes is expected to be less and hence longer lifetime.

In this paper [8]. it was presented a route stability-based multipath QoS routing protocol for mobile ad hoc networks to support throughput and delay sensitive real-time applications in these networks. It incorporates a hop-by-hop ad mission control and a soft resource reservation scheme in a route discovery process to ensure QoS assurance to real-time applications.

In this paper [9], a multipath unicast routing algorithm is proposed with multiple constraints based on mobile agents. It uses mobile agents to collect information of all mobile nodes, and reduces the network delay and the overhead of control messages for routing. This algorithm has stronger routing stability and lower probability of link failure because it selects links with large link expiration time (LET) during route creating phase.

In this paper [10], the enhanced routing protocol is proposed that detect different attacks in a network using an advanced attack detection system (AADS) and switches to a particular protocol that can resist various attack for choose the optimal and secure path in network.

In this paper [11], new routing mechanism is developed to integrate a node selection with a stable and reliable link to establish and maintain trustworthy routes in the network. With the inclusion of this mechanism, it is expected that optimized stable and reliable routing protocol (OSRR) protocol would result in a higher percentage of successful data delivery inspite of mobility among nodes.

In this paper [12],a Local Intrusion Detection Security Routing (LIDSR) mechanism is proposed to detect Black Hole Attack (BHA) over the Ad hoc On Demand Distance Vector (AODV) MANET routing protocol. In the LIDSR mechanism, the intrusion detection is performed locally using the previous node from the attacker node instead of performing the intrusion detection via the source node as in the Source Intrusion Detection Security Routing (SIDSR) mechanism.

In this paper [13], Cross-layer based Secure Routing is developed in MANETs. It is a promising method to satisfy the network requirements which has gained its popularity during the recent years. It includes passing of the information from physical layer and MAC layer to the network layer. The route is selected based on the parameters obtained from the lower layers.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In this paper [14], Stability-Based Clustering (SBC) technique is developed to construct stable enough clusters to reduced maintenance overhead. It tends to construct more clusters in low-mobility situations and fewer clusters in high-mobility situations. The route finding mechanism combines both unicasting and broadcasting of route request packets.

In this paper [15], it was introduced that routing algorithm which enhances the stability and the continuity of communications. Communication stability is ensured by choosing the most stable route which bases on the computation of the Link Expiration Time.

In this paper [16], it was presented the design and implementation of declarative policy-based adaptive MANET routing protocols. This work builds upon declarative networking, a recent innovation for building extensible network architectures using declarative languages. Initially, it was demonstrated that traditional MANET protocols can be expressed in a compact fashion as declarative networks.

In this paper [17], a Link-Stability and Energy aware Routing protocol (LAER) was explored to make a balance between link stability and energy efficient. Each node broadcasts HELLO packets to all its neighbors that are in its communication range; each node in LAER maintains the table of its direct neighbors. When a node receives the HELLO packet, it updates the information of the neighbor, if neighbor ID is already present in table or adds a neighbor information, if it is a new neighbor. They have not considered on path, negihbor node stability.

In our previous works EESMRS [19] and PLSS [18], we have focused on energy consumption, link and path stability. In this research work, cluster head is chosen to provide network confidentiality. Secret sharing scheme is developed to achieve integrity and authentication.

The proposed work is organized as follows. The Section 1 describes introduction about multicast routing in MANET, need for wired and wireless multicast routing in MANET. Section 2 deals with the previous work which is related to the stability and authentication scheme. Section 3 is devoted for the implementation of proposed scheme. Section 4 describes the performance analysis and the last section concludes the work.

3. IMPLEMENTATION OF PROPOSED SCHEME

In this section, clustering methodology is used and cluster head is chosen based on certificate revocation list, weighting average. Secret sharing scheme is enhanced to provide integrity and authentication. The description of phases is given below.

3.1 Cluster based Multicast Routing

A network can contain one or several secret information sharing domains that involves a part of mobile nodes in the mobile ad hoc network. Assume that information sharing domain contains M security levels, and security level k (k= *1, 2, ..., M*) has superior security power over any other security level M that satisfies $M < K$. All mobile nodes of security level k build up security group SG_k.

It is represented as in terms of security power, the relationship among security groups SG_1, SG_2……SG_k, is subject to a cluster topology shown in Fig.1. Based on the definition of security group, M multicast groups (GM_k, k = 1, 2, ..., M), are constructed to provide multicast information broadcast among the cluster members of different security levels in an information sharing domain.

The design of multicast groups reflects the fact that the higher security groups have right to join and monitor the communication of lower security groups. If we use dynamic multicast, it is supposed that the number of GS_k mobile nodes is a random variable X_k, which is subject to Gaussian distribution with the mean of x_k and a small value of variance.

3.2 Cluster head Election

In the proposed hybrid cluster enhanced secure multicast routing scheme, cluster heads are responsible for cluster formation and maintain the network security. If cluster head discloses confidential information, it will imperil the security of the system. Including this, due to dynamic nature of the mobile nodes, their organization and dissociation to and from clusters trouble network stability and thus
reconfiguration of cluster heads is necessary.

Step1. Determine the level of convicted accusation. Each cluster member stores the accusation of insecure nodes in its Cluster member Certificate Revocation List (CRL), and then forwards the information of accusations to neighbors who store it in their CRL with a “suspect” accusation. The level of convicted accusation is S_u. Once the node gathers P accusations of a certain node, the “suspect” becomes “convicted.” The P is the value

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

in an (n, k) threshold cryptography scheme. The greater S_u indicates more insecure.

Step2. Estimate the convicted accusation S_u . If the S_u of the node u equals P, then node u is a malicious node. Consequently, the node u is eliminated from the election. Otherwise, the following procedures are to be implemented.

Step3. Value the reliable degree of node u. This study introduces the function of trust valuation in disclosed networks to evaluate direct trust relationships between two nodes. The combined value is calculated as

$$U_{comb} = 1 - \prod_{k=1}^{l} \sqrt[n_l]{\prod_{d=1}^{n_k}(1 - U_{k,d})} \quad (1)$$

Where $U_{k,d} \neq 0$

where $V_{k,d}$ denotes the value of the derivation of multiple direct trust relationships between two nodes;

V_{comb} represents the combined value of direct trust relationships in which k trusts d. In this scheme, after a period of operations, since each cluster member has the accused record of other nodes in its own CRL, the accused record indicates that the trust value between two cluster members and is shared among all members via RREQ messages, enabling the direct or recommended trust value to be derived.

Step4. Find the cluster neighbors of each member u which define its degree d_u as,

$$d_u = | M(u) | = \sum_{u' \in U, u' \neq u} \{ dist(u,u') < ty_{range} \} \quad (2)$$

Step5. Compute the degree difference $\Delta u = |d_u - \delta|$, for every node u. To ensure efficient Medium Access Control (MAC) functioning, each cluster head can support an optimum of δ, a pre-defined threshold of cluster members. This value exists to ensure that a cluster head does not become overloaded and the system efficiency is maintained at the expected level.

Step6. For every cluster member u, compute the sum of distances Du with all neighbors, as

$$D_u = \sum_{u' \in N(u)} \{ dist(u,u') \} \quad (3)$$

Step 7: Determine the operation average speed for every node until the current time is τ . Cluster members are assumed to have a Global Positioning System (GPS) since the GPS is primarily used to determine the geographical location of mobile nodes.

Step8. Compute the battery power consumption P_u, which is assumed to be more for a cluster head than an ordinary node.

Step9. Calculate the combined weight W_u for each cluster member u in cluster

Step10. Choose the node with the smallest W_u as the cluster head. All the neighbors of the chosen cluster head are no longer permitted to participate in the election procedure.

Step11. In the other clusters, repeat steps 1–10 to elect cluster heads for the remaining nodes not yet selected as a cluster head or assigned to a cluster.

Step12. Choose the cluster head with the smallest W_u as the root cluster head R_{ch}.

3.3 Secret Identification Scheme:

The secret identification phase involves an entity identifying itself by proving knowledge of a secret using a zero- knowledge proof; the protocol reveals no partial information whatsoever regarding the secret identification value(s) of P. P proves its identity to Q in t executions of a 3-pass protocol.

1. *Selection of system parameters*. A trusted center T publishes the common modulus $n = pq$ for all users, after selecting two secret primes p and q each congruent to 3 mod 4, and such that n is computationally infeasible to factor.

2. *Selection of per-entity secrets*. Each entity P does the following.

(a) Select k random integers $S_1, S_2, \ldots, S_k$ in the range $1 \leq S_i \leq n-1$, and k random bits $b_1, \ldots, b_k$. (For technical reasons, gcd (s_i, n) = 1 is required, but is almost surely guaranteed as its failure allows factorization of n.)

(b) Compute $v_i = (-1)^{b_i} \cdot (s_{2i})^{-1} \bmod n$ for $1 \leq i \leq k$. (This allows v_i to range over all integers co-prime to n with Jacobi symbol +1, a technical condition required to prove that no secret information is "leaked"; by choice of n, precisely one signed choice for v_i has a square root.

(c) P identifies itself by non-cryptographic means (e.g., photo id) to T , which thereafter registers A's public key ($v_1, \ldots, v_k$; n), while only A knows its private key ($s_1, \ldots, s_k$) and n. This completes the one-time set-up phase.

Protocol messages. Each of t rounds has three messages with form as follows.

Journal of Theoretical and Applied Information Technology
31st March 2014. Vol. 61 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$P \rightarrow Q : x(= \pm r^2 \bmod n) \quad (4)$$

$$P \rightarrow Q : (e_1, \ldots\ldots e_k), e_i \in \{0,1\} \quad (5)$$

$$P \rightarrow Q : y\left(= r.\prod_{e_j=1} s_j \bmod n\right) \quad (6)$$

Protocol actions. The following steps are executed t times; Q accepts P's identity if all t rounds succeed. Assume Q has P's authentic public key ($v_1, \ldots, v_k$; n); otherwise, a certificate may be sent in message (1), and used as in Protocol

(a) P chooses a random integer r, $1 \leq r \leq n-1$, and a random bit b; computes $x = (-1)^b \cdot r^2 \bmod n$; and sends x (the *witness*) to Q.

(b) Q sends to P (the *challenge*,) a random k-bit vector $(e_1, \ldots, e_k)$.

(c) P computes and sends to B.

(d) B computes and verifies the key.

3.4 Proposed Packet Format

Source ID	Destination ID	Key Verification	PI	Hop count	FCS
2	2	4	4	2	2

Fig.1 Proposed Packet format

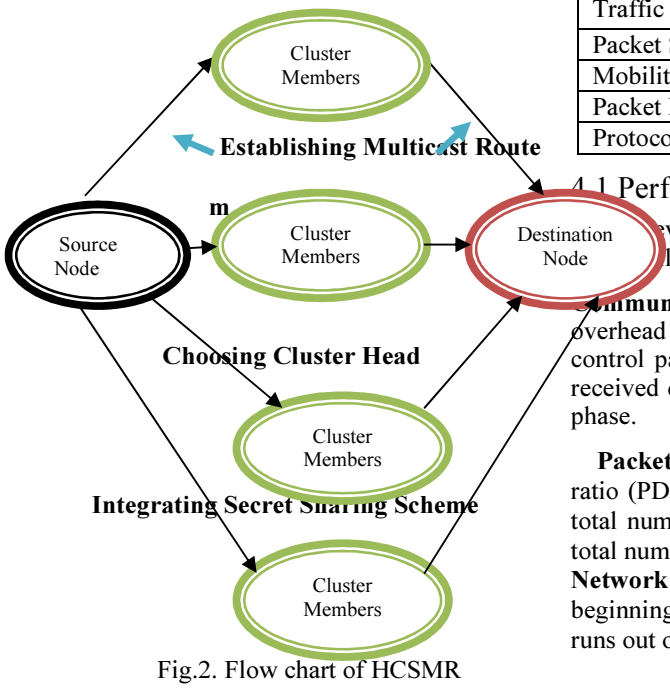


Fig.2. Flow chart of HCSMR

In fig. 1, the packet format of proposed algorithm is shown. Here the first two fields are source and destination address occupies 2 bytes. The third field is key verification used to store the verified keys that occupies 4 byte field. In next field, Packet Integrity fills 4 byte. Hop count occupies 2 byte field for calculating number of hops from cluster node. FCS is Frame Check Sequence used for error monitoring. Flowchart of HCSMR is shown in fig.2.

(3)

4. PERFORMANCE EVALUATION

The proposed scheme HCSMR is simulated with the help of object oriented discrete simulator. In this simulation, 101 mobile nodes move in a 1200 meter x 1200 meter square region for 100 seconds simulation time. All nodes have the same transmission range of 300 meters. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in table1.

Table1. Simulation and settings parameters

No. of Nodes	101
Area Size	1200 X 1200
Mac	802.11
Radio Range	300 m
Simulation Time	80 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Packet Rate	8 pkts/sec
Protocol	AODV

4.1 Performance Metrics

…valuate mainly the performance according …llowing metrics.

…mmunication overhead: The communication overhead is defined as the total number of routing control packets normalized by the total number of received data packets during the route maintenance phase.

Packet Delivery Ratio: The packet delivery ratio (PDR) of a network is defined as the ratio of total number of data packets actually received and total number of data packets transmitted by senders. **Network Lifetime:** It is defined as the time from beginning of simulation until first node in MANET runs out of energy.

End-to-End Delay: The End-to-End delay is defined as the difference between two time instances: one when packet is generated at the

Journal of Theoretical and Applied Information Technology
31st March 2014. Vol. 61 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

sender and the other, when packet is received by the receiving application.

Packet Integrity Rate: It is defined as how many packets are never corrupted by intruders.

The simulation results are presented here. It is compared that proposed scheme HCSMR with our previous scheme EESMRS, PLSS and existing scheme LAER [17] and in presence of stability environment.

Figure 3 shows the results of average end-to-end delay for varying the mobility from 20 to 100. From the results, we can see that scheme HCSMR has slightly lower delay than EESMRS, PLSS and LAER scheme because of stable routing.

Figure 4, presents the residual energy while varying the time. The Comparison of HCSMR, EESMRS, LAER and PLSS energy consumption is shown. It is clearly seen that energy consumed by HCSMR is less compared to EESMRS, LAER and PLSS.

Fig. 5, presents the comparison of communication overhead. It is clearly shown that the overhead of HCSMR has low overhead than EESMRS, PLSS and LAER scheme.

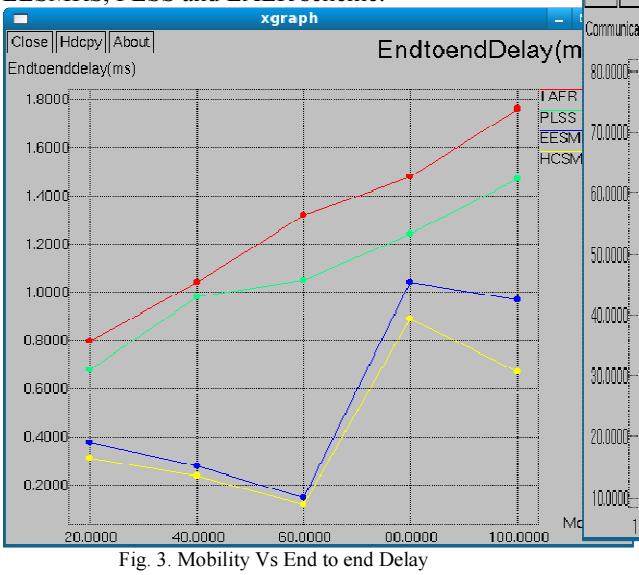


Fig. 3. Mobility Vs End to end Delay

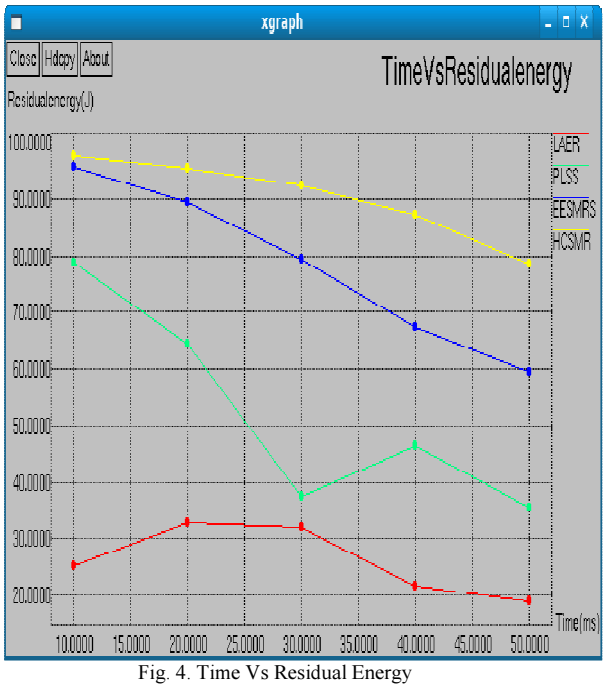


Fig. 4. Time Vs Residual Energy

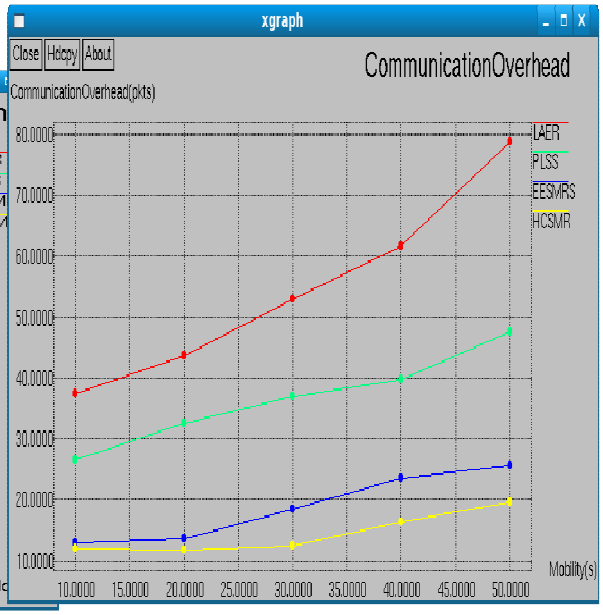
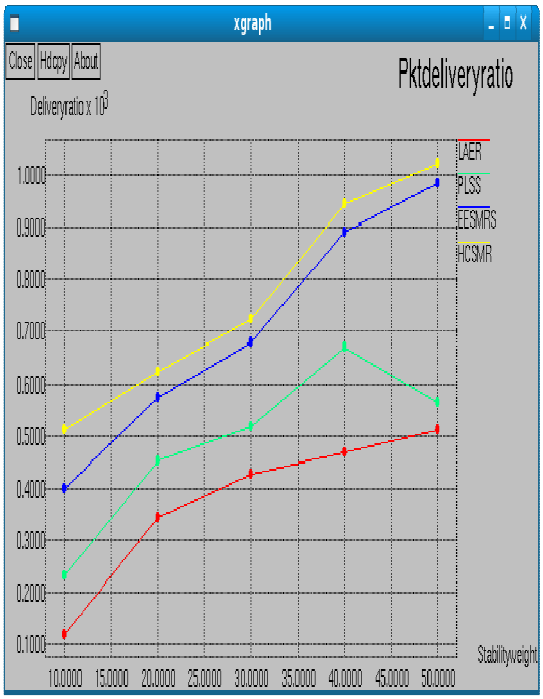


Fig. 5. Mobility Vs Communication Overhead

Journal of Theoretical and Applied Information Technology
31st March 2014. Vol. 61 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



.Fig.6. Stability Vs Packet Delivery Ratio

Figure 6 show the results of average packet delivery ratio for the stability weight 10, 20…50 for the 100 nodes scenario. Clearly our HCSMR scheme achieves more delivery ratio than EESMRS, PLSS and LAER scheme since it has both reliability and stability features.

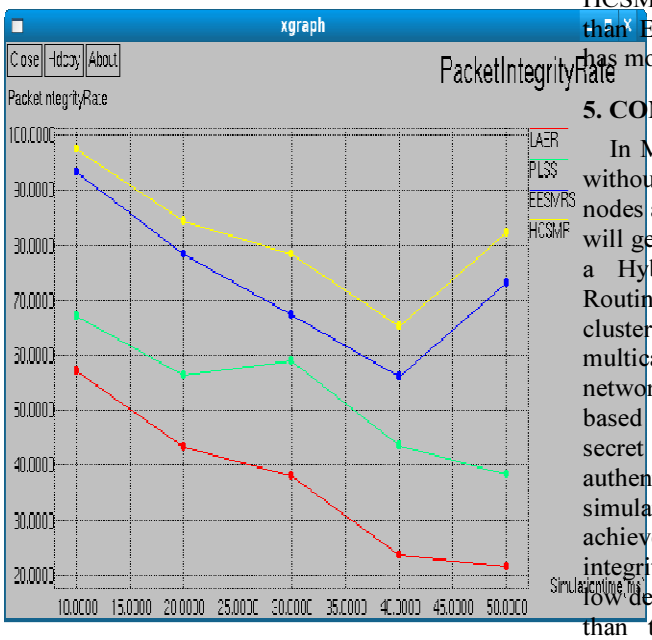


Fig.7. Simulation time Vs Packet Integrity Rate

Figure 7 show the results of packet integrity rate for the simulation time 10, 20…50 for the 100 nodes scenario. Clearly our HCSMR scheme achieves high link availability than EESMRS, PLSS and LAER scheme since it has both predicting stability features.

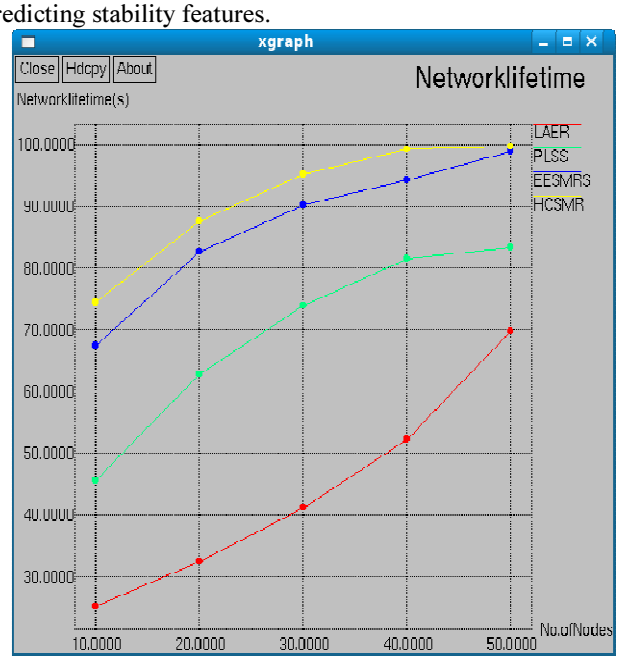


Fig.8. No.of Nodes Vs Network Lifetime

Figure 8 show the results of average network lifetime for the nodes from 10 to 50. Clearly our HCSMR scheme achieves more network lifetime than EESMRS, PLSS and LAER scheme since it has more residual energy.

5. CONCLUSION

In MANET, mobile nodes are moving randomly without any centralized administration. If these nodes are not having reliable secure routes, network will get degraded. In this paper, we have developed a Hybrid Cluster enhanced Secure Multicast Routing Scheme which attains integrity in between cluster groups. In the first phase of the scheme, multicast routing is developed to ensure high network lifetime. In second phase, cluster head is based on certificate revocation list. In third phase, secret identification phase to provide network authentication. Key is verified with each stage. By simulation results we have shown that the HCSMR achieves good packet delivery ratio, high packet integrity rate, more network lifetime while attaining low delay, overhead, minimum energy consumption than the existing scheme EESMRS,PLSS and LAER scheme while varying the number of nodes, node speed, throughput and simulation time.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES:

[1] C. Diot, B. Levine, B. Lyles, H. Kassem, and D. Balensiefen, 'Deployment Issues for the IP Multicast Service and architecture', *IEEE network,* Jan 2000.

[2] GUI Chao, "An entropy-based stability QoS routing with priority scheduler in MANET using fuzzy controllers", *Journal of Communication and Computer*, Vol.4, No.3, 2007, pp.52-54.

[3] Sunil Taneja & Ashwani Kush, "Energy Efficient, Secure and Stable Routing Protocol for MANET", *Global Journal of Computer Science and Technology*, Volume 12 Issue 10 Version 1.0 May 2012, pp.1-15.

[4] P.Kiran Rao and S.Vasundra , " Channel Aware Routing in MANET'S with Secure Hash Algorithm", *International Journal of Scientific and Research Algorithms*, Vol.2, No.1, 2012, pp.1-4.

[5] S. Priyadarsini, " TSRD-RL algorithm based Secured Route Discovery for MANET with improved Route Lifetime", *International Journal of Electronics and Electrical Engineering*, Vol.1, Issue 1, 2012, pp.52-67.

[6] Vijay Kumar and Ashwani Kush , "A New Scheme for Secured on Demand Routing", *Network and Complex Systems*, Vol.2, No.2, 2012, pp.1-9.

[7] Shuchita Upadhayaya, Charu Gandhi, "QOS Routing Using Link And Node Stability In Mobile Ad Hoc Networks", *Journal of Theoretical and Applied Information Technology*, 2012, pp.117-122.

[8] Nityananda Sarma and Sukumar Nandi, "A Multipath QoS Routing with Route Stability for Mobile Ad Hoc Networks", *IETE technical review*, Vol.27, Issue 5, 2010, 380-397.

[9] Bindhu.R, "Mobile Agent Based Routing Protocol with Security for MANET", *International Journal of Applied Engineering Research*, Vol.1, No.1, 2010, pp.92-101.

[10] Vinay Kumar Pandey, Dr. Harvir Singh and Sanjay Kumar, "Enhanced Secure Routing Model for MANET", *CS & IT*, 2012, pp.37-44.

[11] Ankit Verma and A.K.Vatsa, " Optimized Stable and Reliable Routing (OSRR) Mechanism in MANET", *International Journal of Science and Technology,* Volume 1 No. 9, 2012, pp.466-475.

[12] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Anton Satria, "Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol", *Australian Journal of Basic and Applied Sciences*, Vol.5, No.10, 2011, pp.1137-1145.

[13] Sreedhar C, Dr. S. Madhusudana Verma and Dr. N. Kasiviswanath, " Cross-Layer Based Secure Routing In Manets", *International Journal of Engineering Research and Applications*, Vol. 3, Issue 5, 2013, pp.725-731.

[14] Chun Chuan Yang and Yu- Chong Chang, "A Stability-Based Clustering Technique and Routing Protocol for Mobile Ad Hoc Networks", *Journal of Information Science and Engineering*, Vol.24, 2008, pp.469-481.

[15] Xi Hu, Jinkuan Wang and Cuirong Wang , "Mobility-adaptive Routing for Stable Transmission in Mobile Ad Hoc Networks", *Journal of Communications*, Vol. 6, No. 1, 2011, pp.79-86.

[16] Changbin Liu, Ricardo Correa, Xiaozhou Li, Prithwish Basu, Boon Thau Loo and Yun Mao, "Declarative Policy-based Adaptive MANET Routing", *IEEE Conferences*, 2011, pp.1-10.

[17] Floriano De Rango, Francesca Guerriero and Peppino Fazio, "Link-Stability and Energy Aware Routing Protocol in Distributed Wireless Networks", *IEEE Transactions on Parallel And Distributed Systems*, Vol. 23, No. 4, April 2012, pp.713-726.

[18] Geetha Nair1 and Dr.N.J.R.Muniraj2, "Prediction based Link Stability Scheme for Mobile Ad Hoc Networks", *International Journal of Computer Science Issues*, Vol. 9, Issue 6, No 3, 2012, pp.401-408.

[19] Geetha Nair1 and Dr.N.J.R.Muniraj, "Efficient Energy based Stable Multipath Routing Scheme for MANET", *International Journal of Computer Applications*, Vol.73, No.22, 2013, pp.13-19.