International Conference on Systems, Science, Control, Communication, Engineering and Technology 2015 [ICSSCCET 2015]

ISBN	978-81-929866-1-6	**VOL**	01
Website	icssccet.org	**eMail**	icssccet@asdf.res.in
Received	10 - July - 2015	**Accepted**	31- July - 2015
Article ID	ICSSCCET037	**eAID**	ICSSCCET.2015.037

A Cross Layer Based Secure Multipath Neighbor Routing Protocol in MANET

H INDRAPRIYADARSINI[1], T ARTHI[2]
[1, 2] Assistant Professors, Department of Electronics and Communication Engineering,
Karpagam Institute of Technology, Coimbatore.

Abstract: *A mobile ad hoc network is a collection of mobile nodes forming an ad hoc network without the assistance of any centralised structures or administration. It is a wireless network and a self-configuring one. Due to high mobility of nodes in mobile ad hoc networks (MANETs), there exist frequent link breakages which lead to frequent path failures and route discoveries. The overhead of a route discovery cannot be neglected. In a route discovery, broadcasting is a fundamental and effective data dissemination mechanism, where a mobile node blindly rebroadcasts the first received route request packets unless it has a route to the destination, and thus it causes the broadcast storm problem. In this phase, cross layer is deployed to improve lifetime and quality of service (QoS). By deploying secret sharing scheme have provided message integrity and authentication. By using the experimental result of CLSMRSCA achieves more path reliability rate, lifetime, end to end delay and less overhead than the existing scheme CLMNRP.*

Keywords: CLSMRSCA -Cross Layer Based Secure Multipath Routing Scheme for Collision Avoidance, CLMNRP -Cross Layer Based Multipath Neighbor Routing Protocol.

1. INTRODUCTION

Mobile Ad Hoc Network

Mobile Ad Hoc Network (MANET) is a self-configuring system of mobile routers linked by wireless links which consequently combine to form an arbitrary topology. Thus, the network's wireless topology may alter rapidly and unpredictably. However, due to the lack of any fixed infrastructure, it becomes complicated to exploit the present routing techniques for network services, and this provides some huge challenges in providing the security of the communication, which is not done effortlessly as the number of demands of network security conflict with the demands of mobile networks, largely due to the nature of the mobile devices .e.g. low power consumption, low processing load.

Cite this article as: H INDRAPRIYADARSINI, T ARTHI. "A Cross Layer Based Secure Multipath Neighbor Routing Protocol in MANET." *International Conference on Systems, Science, Control, Communication, Engineering and Technology (2015)*: 170-174. Print.

II.A CROSS LAYER BASED MULTIPATH NEIGHBOR ROUTING PROTOCOL

II.1 Cross layer design

A cross layer based multipath neighbor routing protocol is developed to attain network connectivity. Here this protocol is deployed to overcome the link and path breakages. Cross layer design is said to be the violation of layered communication architecture in the protocol design with respect to the original architecture. Distributed algorithms can exploit a cross-layer design to enable each node to perform fine-grained optimizations locally whenever it detects changes in network state.

II.2 Multipath Routing

Multipath routing has been explored in several different contexts. Traditional circuit switched telephone networks used a type of multipath routing called alternate path routing. In alternate path routing, each source node and destination node have a set of paths (or multipaths) which consist of a primary path and one or more alternate paths. Alternate path routing was proposed in order to decrease the call blocking probability and increase overall network utilization.

In alternate path routing, the shortest path between exchanges is typically one hop across the backbone network; the network core consists of a fully connected set of switches. When the shortest path for a particular source destination pair becomes unavailable (due to either link failure or full capacity), rather than blocking a connection, an alternate path, which is typically two hops, is used. Multipath routing increases fault-tolerance and reliability. The router can split the same label traffic flow into different paths with the given traffic engineering constraint. QoS constraints like minimum delay and maximum bandwidth are considered for splitting a given flow dynamically into

these multiple paths. The steps for achieving load distribution through the multipath routing is follows.

Step 1: Calculate the ℓ, a set of disjoint path from source to destination. The path is considered as a loop less path.

Step 2: Find the path χ from ℓ based on the bandwidth and (least hop) shortest path distance i.e.

$Bw(p_m) = Bw(p_k)$ and the distance $S_d(m) = S_d(l)$.

Step 3: If (Path failure occurs)

Choose the alternative backup path form the set ℓ $\{P_l, P_m, \ldots\ldots\ldots P_n\}$ with least hop distance. If the source is l and the destination n.

Else

Stop the transfer of the data form source to destination.

Step 4:

Select the path from the maximum number of edge disjoint paths which satisfies the bandwidth and delay requirements

$BW(p_l) + BW(p_m) + \ldots\ldots\ldots BW(p_k) = BW_t(P_T)$

$DE(p_l) + DE(p_m) + \ldots\ldots\ldots DE(p_k) = DE_t(P_T)$

Step 5:

Establishing the multipath routing among all the mobile nodes in the network.

Step 6:

Achieving the load balancing to improve the throughput and network connectivity.

Cite this article as: H INDRAPRIYADARSINI, T ARTHI. "A Cross Layer Based Secure Multipath Neighbor Routing Protocol in MANET." *International Conference on Systems, Science, Control, Communication, Engineering and Technology (2015)*: 170-174. Print.

II.3 Energy Consumption Model

In MANETs, the topology is dynamic not static. Due to the dynamic topology, node consumes more energy while roaming.The energy model of proposed algorithm is given below. In this model energy consumption for transmitting M bit is equal to:

$E_{tr}(M, d) = E_{elec} \times M + \delta_{amp} \times M \times d^2 - E_{wast}(P_{drop})$
M = bit contain some information like current energy level of the node, data label, node's location and hop count.
E_{elec} = Energy to be Transmitted and Received electronic device module (75 nJ/bit).
δ_{amp} = Transmitter Amplifier (150 pJ/bit/m^2)
d = distance between the two nodes.
$E_{wast}(P_{drop})$ = Energy wasted on packet dropping.
And the energy for receiving K bit is equal to:
$E_{rr} = E_{elec} \times M$

II.4 Secret Sharing Scheme

Use the concept of Proactive Secret Sharing (PSS) to provide data authenticity and confidentiality. In the PSS implementation, each share holder randomly generates own sub-shares (e.g., (s_{i1}, s_{i2}, . . . , s_{in}) on node i), and each sub-share is mutually exchanged to refresh own share. More precisely, the PSS procedure can be performed in the following steps:

1) Let (s_1, s_2, . . . , s_n) be an (n, t) sharing of the secret key S of the service, with node *l* having S_l.
2) Node *l* (i {1 . . . n}) randomly generates s_l's sub shares (s_{l1}, s_{l2}, . . . , s_{ln}) for an (n, t) sharing.
3) Every sub-share s_{lk} (k {1 . . . n}) is distributed to node k through secure link.
4) When node k gets the sub-shares (s_{1k}, s_{2k}, . . . , s_{nk}), it computes a new share from these sub-shares and its old share with an equation,

$$s'_k = s_k + \sum_{k=1}^{n} s_{lk}$$

III. RESULTS

In our simulation, 350 mobile nodes move in a 1000 meter x 1000 meter square region for 60 seconds simulation time. All nodes have the same transmission range of 500 meters.

Fig.1 shows the the comparison of overhead and mobility. It is clearly shown that the overhead of CLSMRSCA has low overhead than the CLMNRP protocol while varying mobility range from 20.0000 to 100.0000.
Figure.2 shows the results of Throughput Vs Network Lifetime. From the results, we can see that CLSMRSCA scheme has higher Network Lifetime than the CLMNRP while varying the Throughput from 100.0000 to 500.0000(pkts).
Figure.3 presents the comparison of End to end delay while varying the Speed from 20.0000 to 100.0000. It is clearly shown that the delay of CLSMRSCA lower than the CLMNRP protocol.

Figure.4 presents the comparison of No.of nodes Vs path reliability rate while varying the No.of nodes from 20.0000 to 100.0000. It is clearly shown that the path reliability rate of CLSMRSCA higher than the CLMNRP protocol.

Figure 5. presents the comparison of Simulation time Vs energy consumption while varying the time from 10.0000 to 50.0000. It is clearly shown that the energy consumption of CLSMRSCA lower than the CLMNRP protocol.

Cite this article as: H INDRAPRIYADARSINI, T ARTHI. "A Cross Layer Based Secure Multipath Neighbor Routing Protocol in MANET." *International Conference on Systems, Science, Control, Communication, Engineering and Technology (2015)*: 170-174. Print.

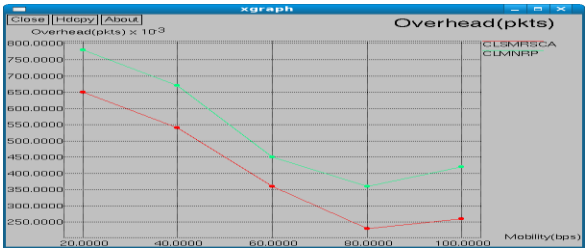

Figure.1 Mobility Vs Overhead

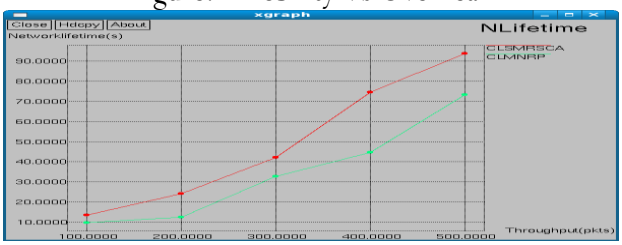

Figure.2ThroughputVsNetwork Lifetime

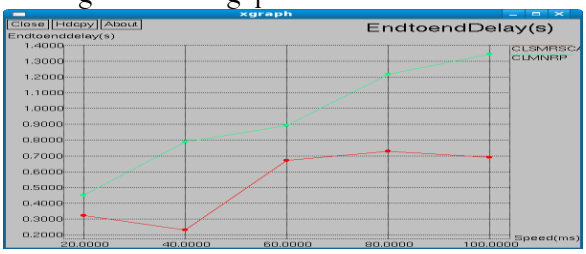

Figure.3: End to End delay Vs Speed

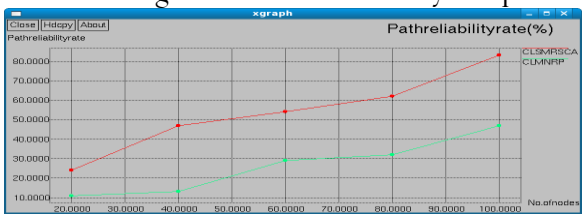

Figure.4: No.of nodes Vs path reliability rate

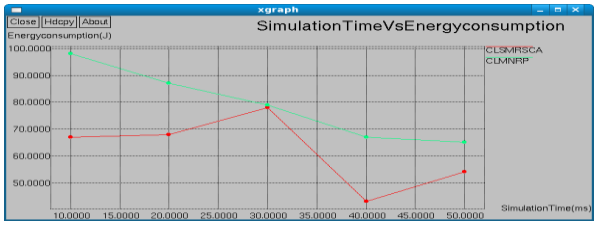

Figure 5: Simulation Time Vs Energy Consumption

V.CONCLUSION AND FUTURE WORK

In this project, a cross layer based secure multipath routing scheme has been proposed for mobile ad hoc networks. This cross layer increases additional network lifetime. Here, secure multipath routing is deployed to overcome the failures of links and paths as well as provide security from the intruders. For reducing the effect of attackers secret sharing scheme provides authentication. The simulation results also show that the proposed scheme has good performance and achieves more connectivity, lifetime, less overhead, path reliability rate and energy consumption.In future, integration of symmetric key cryptography model with energy consumption can be implemented. Efficient link aware scheduling can be done with authentication scheme to achieve high integrity and authentication

Cite this article as: H INDRAPRIYADARSINI, T ARTHI. "A Cross Layer Based Secure Multipath Neighbor Routing Protocol in MANET." *International Conference on Systems, Science, Control, Communication, Engineering and Technology (2015)*: 170-174. Print.

REFERENCES

[1] Kalpana Sharma and M.K. Ghose,(2011),' Cross Layer Security Framework for Wireless Sensor Networks' proceeding of International Journal of Security and Its Applications Vol. 5 No. 1, pp.No.1-14.
[2] Asmidar Abu Bakar , Roslan Ismail , Abdul Rahim Ahmad and Jamalul-Lail Abd Manan,(2012),' Ensuring Data Privacy and Security in MANET: Case in Emergency Rescue Mission' proceeding of International Conference on Information and Knowledge Management (ICIKM 2012) IPCSIT vol.45, pp.No.1-5.
[3] D. N. Goswami and Anshu Chaturvedi,(2012),' Cross Layer Integrated Approach for Secured Cluster Selection in Ad Hoc Networks', proceeding of International Journal of Computer and Communication Engineering, Vol. 1, No. 3, pp.No.1-4.
[4] G. S. Mamatha,(2012),' A Defensive Mechanism Cross Layer Architecture for MANETs to Identify and Correct Misbehavior in Routing', proceeding of International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, pp.No.1-10.

Cite this article as: H INDRAPRIYADARSINI, T ARTHI. "A Cross Layer Based Secure Multipath Neighbor Routing Protocol in MANET." *International Conference on Systems, Science, Control, Communication, Engineering and Technology (2015)*: 170-174. Print.