International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.3, No.3, March 2014 DOI:10.15693/ijaist/2014.v3i3.40-49

A Cross Layer Based Secure Multipath Neighbour Routing Protocol in MANET

[1]DR.A.RAJARAM, ,
[1]Associate Professor, Department of Electronics and Communication Engineering, Karpagam Educational Institutions , Coimbatore, India.

[2]H.INDRAPRIYADARSINI
PG scholar
Karpagam University
Coimbatore, India
[2]indrapriya.ece@gmail.com

***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.

I.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.

II.PREVIOUS WORK

II.1 CROSS LAYER SECURITY FRAMEWORK FOR WIRELESS SENSOR NETWORKS [1]

The data collected by the nodes of WSN (Wireless Sensor Networks) are sensitive and vulnerable to attack, there is a need of making the Wireless Sensor Networks secure from the attacks. Most of the researchers have come up with security solution to WSN based on layered approach. Layered approach has noticeable flaws like 'redundant' security or 'inflexible' security solutions. In this work a new security scheme is proposed based on the concept of cross layer design methodology. The proposed approach doesn't claim to be immune to all the security attacks but this new approach certainly gives a new direction towards WSN security. The proposed security framework CLIFFs (Cross Layer Integrated Framework for Security), with the help of ISA (Intelligent Security Agent), is used as an adaptive security solution for different application scenario. The results obtained showed that CLIFFs, when provided with the right information regarding the application type, resulted in saving of energy to a large extent. There's a lot of scope of improvement for CLIFFs. ISA can be used to incorporate the concept of 'learning' during its phases of execution. A robust security can be realized if ISA, on itself, decide upon the level of security based on the deployment history of the WSN.CLIFFs can be further enhanced if it is incorporated with highly accepted 'Energy Efficient Routing Protocols and Keying techniques etc.

II.2 ENSURING DATA PRIVACY AND SECURITY IN MANET: CASE IN EMERGENCY RESCUE MISSION [2]

Mobile ad hoc networks (MANETs), which can be formed by groups of portable devices, cultivate new research trend in today's computing. MANET's unique features such as scalability, fault

tolerant and autonomous system allowed the network to be setup with or without any trusted authority. However, since this network is operated based on wireless environment, it is vulnerable to threats and intruders. Information flow in MANET can be intercepted and tampered and this raised a security issues in assured that information shared between nodes in emergency situation using MANET secure. Hence, a mechanism to ensure data privacy and security during emergency rescue mission is required. This scheme proposed the secure access architecture that incorporate access control model, which aims to ensure data travel between groups of secure and preserved the data integrity. The architecture consists of trust management, access control policy and cryptology protocols. With the architecture, a comprehensive access control model is constructed to support the access to data and information required during emergency rescue mission. Using the access control model, members will be verified using the cryptographic protocols such as encryption/decryption, hash function and digital signature. This will ensure that only authenticated member, belong to correct group get an access to the information requested. The used of tag which was created prior to network setup at the ERM(Emergency Rescue Mission), enabled members to be authenticated hence create trust between MG(Group leader) and M(Member). Beside this, the access policy embedded in the tag also able to distinguish the role between members of the group at the emergency rescue mission. This will eliminate wrongly data passing between members in the group at the ERM, hence ensuring data security and privacy is preserved between groups at ERM.

II.3CROSS LAYER INTEGRATED APPROACH FOR SECURED CLUSTER SELECTION IN AD HOC NETWORKS [3]

Mobile Ad hoc Network (MANET) basically, is a collection of mobile hosts incorporating wireless interfaces that forms a transitory autonomous network. They do not base on fixed infrastructure or central administration, rather work on the principle of self-organized interconnections among mobile nodes. Fundamentally, in MANET when nodes come inside the transmission range of neighboring nodes', they can be detected by each other and can communicate directly. However for communication outside this range they have to depend on some other nodes to relay the messages .This is where routing protocols have to play a very important role. Literature for improving the performance of routing protocol is available in abundance. Among these comes, the hierarchical/cluster-based routing protocols that claim to reduce control overheads. Clustering in Mobile Ad hoc Networks (MANETs) has proved to be advantageous compared to the traditional networks. However the highly dynamic and unstable nature of MANETs makes it intricate for the cluster based routing protocols to split a mobile network into clusters and determination of cluster heads for each cluster. Although much previous research has concentrated on cluster-head selection in MANETs, not much effort has been done on the security side of cluster-head selection. This scheme emphasize that secure cluster head selection in MANETs has an intense effect on network performance. Specifically, we stress that in ad hoc network where all the participants are self controlled, security is an essential aspect and the effective cluster-head selection can improve network throughput. A secure and effective cluster-head selection scheme using a cross-layer approach that integrates cluster-head discovery and selection functionality with network ad hoc routing mechanisms and the lower layer drivers built-in the system. Besides, this scheme handles the disconnections in ad hoc network due to the effects of topology changes and battery depletion. This scheme allows clients to switch to better cluster-head nodes as network topology changes. Hence, provides better performance to the network. One of the key requirements in an ad hoc network is for nodes to share and utilize each other resources. To use these resources the nodes in MANET needs to have knowledge, where these resources are existing in the network. Although much previous research has concentrated on Cluster-head selection in MANETs, not much effort has been made on the security side of Cluster-head selection. We propose an algorithm which selects a Cluster-head node who is trustworthy enough. Thus it secures the route discovery and maintenance system. Moreover this scheme handles the disconnections in ad hoc network due to the effects of topology changes. This algorithm put forward an effective cross-layer approach that integrates Cluster head discovery and selection functionality with network ad hoc routing mechanisms and the lower layer driver built-in the system. This scheme allows clients to switch to better Cluster-head nodes as network topology changes. Hence, provides better performance to network.

II.4 A DEFENSIVE MECHANISM CROSS LAYER ARCHITECTURE FOR MANETS TO IDENTIFY AND CORRECT MISBEHAVIOUR IN ROUTING [4]

The emerging mobile technology has brought revolutionized changes in the computer era.

One such technology of networking is Mobile Ad hoc Networks (MANETS), where the mobility and infrastructure less of the nodes takes predominant roles. These features make MANETS more vulnerable to attacks. As
the research continues several aspects can be explored in this area. At the very first it can be the problem of how to make the cross layer detection of attacks more efficient and work well. Since every layer in the network deals with different type of attacks, a possible viewpoint to those attack scenarios can be presented so that it can be extended in the later part. It becomes necessary to figure out the security solution architecture if there are different detection results generated by different layers. Secondly, there should be a measure of the network metrics to show increased performance. The scheme presents such a defensive mechanism cross layered architecture which strives to identify and correct misbehavior in MANETS especially with respect to routing layer. The evaluation of the scheme solution is also given with results obtained to show the performance of the network. Designing a clear line of defence in MANETS is a very tough task. Here a possible security solution in the form of cross layer architecture known as SSA. This SSA fulfils some of the main security requirements as mentioned, further it can be extended to more also. The security and encryption mechanisms can also be varied according to the simulation environments and applications. Ensuring that the routing technique mentioned namely TODV also works at the par to satisfy the MANET requirements. As the results shown with simulation experiments conducted states that the proposed approach guarantees the security objectives for MANETS and shows considerable enhancement in performance.

II.5 CROSS LAYER INTRUSION DETECTION SYSTEM FOR WIRELESS SENSOR NETWORK [5]

The wireless sensor networks (WSN) are particularly vulnerable to various attacks at different layers of the protocol stack. Many intrusion detection system (IDS) have been proposed to secure WSNs. But all these systems operate in a single layer of the OSI model, or do not consider the interaction and collaboration between these layers. Consequently these systems are mostly inefficient and would drain out the WSN. In this scenario a new intrusion detection system introduced based on cross layer interaction between the network, Mac and physical layers. Indeed address the problem of intrusion detection in a different way in which the concept of cross layer is widely used leading to the birth of a new type of IDS. Experimentally evaluated this system using the NS simulator to demonstrate its effectiveness in detecting different types of attacks at multiple layers of the OSI model. Taking security as main objective, introduced an intrusion wireless sensor networks. In this scenario the problem of intrusion detection is discussed in a new way in which the Cross layer single cross layer IDS to several layers of the OSI model instead of offering layer. The approach doesn't claim to be immune approach should give a new direction towards WSN security.

II.6 COST BASED POWER AWARE CROSS LAYER ROUTING PROTOCOL FOR MANET [6]

Mobile Ad-Hoc Networks (MANETs) are wireless networks consist a collection of mobile nodes with no fixed infrastructure, where some intermediate nodes should participate in forwarding data packets. So energy conservation is a critical issue in ad hoc wireless networks for node and network life. This issue is crucial in the design of new routing protocols. To design such protocols, look away from the traditional minimum hop routing schemes. In this scheme, developed a cost based power aware cross layer design to AODV. The discovery mechanism in this algorithm uses Battery Capacity of a node as a routing metric. This approach is based on intermediate nodes calculating cost based on Battery capacity .The intermediate node judges its ability to forward the RREQ packets or drop it. That is it integrates the routing decision of network layer with battery capacity estimation of MAC layer. Simulations are performed to study the performance of power aware cross layer AODV protocol using NS2. The simulation shows that the cross layer protocol improves packet delivery ratio & throughput and also nodes energy consumption is reduced by routing packets using energy optimal routes. The low power nodes are identified and rejected in RREQ flooding phase itself and not after facing any RREP transmission failures.

II.7 A NOVEL CROSS LAYER INTRUSION DETECTION SYSTEM IN MANET [7]

Intrusion detection System forms a vital component of internet security. To keep pace with the growing trends, there is a critical need to replace single layer detection technology with multi layer detection. Different types of Denial of Service (DoS) attacks thwart authorized users from gaining access to the networks and tried to detect as well as alleviate some of those attacks. In this scheme, a novel cross

layer intrusion detection architecture to discover the malicious nodes and different types of DoS attacks by exploiting the information available across different layers of protocol stack in order to improve the accuracy of detection. Hence, a better intrusion detection mechanism based on anomaly detection is presented for utilizing cluster data mining technique.

II.8 CURRENT TRENDS AND FUTURE ASPECTS IN CROSSLAYER DESIGN FOR THE WIRELESS NETWORKS [8]

Computer network today are becoming popular day by day in our day to day life. The users are looking forward to use wireless technologies such as Bluetooth, WLANs based on the IEEE 802.11 Standards etc. That allows them to share information via wireless media. The wireless network has several advantages over the wired technologies like flexibility, mobility, cheaper and faster deployment, easier maintenance and upgrade procedures. Cross-layer design refers to protocol design done by actively exploiting the dependence between the protocol layers to obtain better network performance in terms of throughput, average end to end delay etc. In this scheme, a survey of different cross-layer proposals for wireless networks taking in account the ongoing research in this hot area. The cross-layer design the architecture is updated or modified and it requires complete redesign and replacements. The cross-layer design creates interactions, some intended, and others unintended. Cross-layer design can be implemented for network security. When the channel is wireless then authentication of the wireless terminal is a serious issue which can be solved by proper authentication of the wireless terminal. Physical layer authentication in which the channel probing or channel estimation is used when integrated with the cross-layer design can enhance the security of the network.

II.9 CROSS LAYER BASED MISS DETECTION RATIO UNDER VARIABLE RATE FOR INTRUSION DETECTION IN WLAN [9]

The emphasis for the use of wireless LAN in industry is on robustness, reliability and security. Almost any given single security mechanism (such as MAC filtering) alone may be easily overcome by attackers. However, proper configuration and implementation of the maximum possible security mechanism must be used to form a multiple security layers, to provide the best possible wireless protection. The scenario deals with cross layer based miss detection ratio under variable rate for intrusion detection in WLAN. In cross layer based intrusions detection, the decision is based on the combine on weight value of two or more layer. So the decision is not based on single layer, it will reduce false positive rate. Two different layers, physical and MAC have been used in the present study and the results have been compared with existing technique. This technique is compared with the figure printing technique and the simulation result shows that the cross layer based intrusion detection system (CLBIDS) technique is better technique than the RFF (Radio Frequency Fingerprint) technique. It is concluded that the misdetection ratio is significantly less in the cross-layer scheme when compared with

RFF scheme, since it accurately detects the intrusion**.**

III.A CROSS LAYER BASED MULTIPATH NEIGHBOR ROUTING PROTOCOL

III.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. To decrease the energy consumption, the energy consumption model has been proposed. The experimental results shows more connectivity life time and less overhead.

Cross layer design is said to be the violation of layered communication architecture in the protocol design with respect to the original architecture. This design emphasizes on the network performance by enabling the different layers of the communication stack to share state information or to coordinate their actions in order to jointly optimize network performance.

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. Mobility causes changes for the physical layer (for e.g. interference levels), the data link layer (for e.g. link schedules), the routing layer (for e.g. new neighbouring nodes), and the transport layer (for e.g. connection timeouts). As such, a cross-layer based design enhances the capability of the node to manage its resources in the mobile environments Antenna arrays can also enable the reception of multiple packets simultaneously on the wireless channel and the data packets corresponding to several connections could also arrive simultaneously at a node. The cooperation of various layers such as routing, data link, and physical layer can ensure the forwarding of data for all the connections within time.

III.2 Need for Cross layer design

Cross layer design offers performance benefits for a particular system. In contrast, the architecture offers a model for sustained innovation in a system, so it offers long-term gains. The short-term performance gains of cross-layer design may be more significant for the network user to make efficient use of limited node resources.

The following issues raise the need for cross layer design:

- Due to multipath, the response of the wireless channel varies over time and space which leads to short-term fading. These variations may be caused due to either motion of the wireless device or changes in the surrounding physical environment, and lead to errors at the receiving end. This causes bursts of errors to occur during which packets cannot be successfully transmitted on the link. Furthermore, if very strong forward error correction codes at low error rates are employed to eliminate the burst errors then it reduces the spectral efficiency.
- There are also spatial and temporal variations on a much greater timescale due to the small scale variations. Large-scale channel variation means that the average channel response depends on user locations and the level of interference on the channel. This channel variation occurs because of some users may essentially demand more channel access time than others based on their location and/or mobile velocity, even if their data rate requirement is the same as or less than other users. The improvement in the channel characteristics can be improved if the strict physical and MAC layer boundaries can be made soft with the help of cross layer design.
- In MANET traditional approach, each layer of the IP protocol stack operates independently. The information is being shared between the adjacent layers only. Due to the dependencies between physical and upper layers, the traditional approach is not suitable for Mobile Ad hoc Networks. There is need to cross the normal layer boundaries to improve the performance of communication and hence better than the application layer performance. In Cross layer design, the data is shared between the different protocol layers dynamically.
- So that, the information can be exchanged between any different layers of the TCP/IP protocol stack. Figure 1 illustrates the cross layer design for information sharing across different layers.
- In Wireless network, physical layer, Media Access Control (MAC) layer and routing Layer is combined for network resource. At physical layer, transmission power and data rate is decided which affects MAC and routing decisions. The MAC layer is responsible for scheduling and allocating the wireless channel, it will determine the available transmitter bandwidth and the packet delay. Routing layer also depends on bandwidth and delay to select the link. The routing layer chooses the route to send the data packets to the destination.
- The routing decision will change the contention level at the MAC layer and accordingly the physical layer parameters. Because of adaptation of layers end to-end performance can be optimized. Any design changes in the protocol stack when adding interaction between different layers may have effect on the whole system. So cross layer design use with caution.

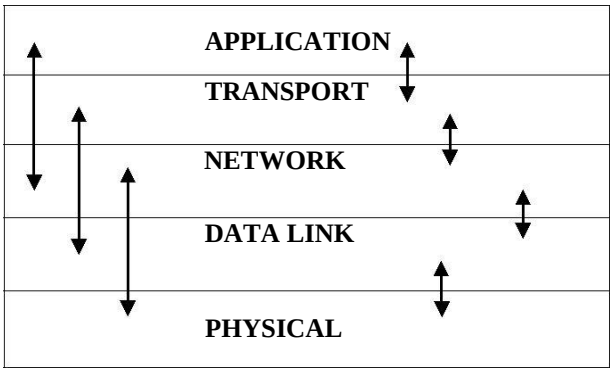


Figure:III.1 Cross layer design - Information sharing scheme

III.3 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 , 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 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 $\{P_l, P_m, \ldots\ldots P_n\}$ 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

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

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

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.

III.4 Energy Consumption Model

In MANETs, the topology is dynamic not static. Due to the dynamic topology, node consumes more energy while roaming. For this, the topology control approach has been introduced. In this approach, have considered two cases,

i) Energy consumption of the node and routes.

ii) Link stability and location stability.

Case i)

In first case, the dynamic and adaptive topology is proposed. It will adopt, according to the node moves with in the network. For this each node will keep on nearest level with in the cluster. The number of links connected to a node is very kept low. The link with the low transmission power is also taken in to the consideration for the energy consumption of the route.

Case ii)

For link stability and location stability, each node carrying link with highest density and efficient transmission power with adaptable location. The location stability which implies node is on the stable state which is ready state to send the number of packets to the intended destination node with degrading the network performance. While implementing these two cases, the energy consumption of the whole network can be effectively reduced.

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:

$E_{rr} = E_{elec} \times M$

III.5 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,

$$S'_k = S_k + \sum_{k=1}^{n} S_{lk}$$

After each PSS, all the shares will be changed, so that old shares become useless. In such case, since it is impossible to obtain new share from old share, a malicious node must collect at least t shares during the time between two executions of the PSS, which obviously makes his job more difficult.

In the proposed scheme periodically PSS occur at start first any share holder node (master node) send pss_start flag to all other share holders (master nodes) and all that nodes now send pss_start_ack to the share holder that initiated the PSS procedure. After receiving pss_start_ack from all share holder nodes the initiating share holder node send refresh flag to all share holder nodes. Now all node refresh its share and send the shares to other share holders using digital signature and encrypted with public key of destination node). After receiving share from all share holders the initiating share holder node now send pss_end flag to all other share holders and wait for ack. After receiving pss_end_ack from all share holders the initiating node now send refresh_end flag to all share holders. So now reach share holder can use these new share for further communication of MANET.

IV. PERFORMANCE ANALYSIS

We use Network Simulator (NS 2.34) to simulate our proposed NSEES algorithm. Network Simulator-2(NS2.34) is used in this work for simulation.NS2 is one of the best simulation tools available for Wireless sensor Networks. We can easily implement the designed protocols either by using the oTCL (Tool command Language) coding or by writing the C++ Program. In either way, the tool helps to prove our theory analytically.

In our simulation, 200 mobile nodes move in a 1300 meter x 1300 meter square region for 60 seconds simulation time. All nodes have the same transmission range of 500 meters. Our simulation settings and parameters are summarized in table 2.

IV .1 Performance Metrics

We evaluate mainly the performance according to the following metrics.

End-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Packet Delivery Ratio: It is defined as the ratio of packet received with respect to the packet sent.

Throughput: It is defined as the number of packets received at a particular point of time.

No. of Nodes	350
Area Size	1000 X 1000
Mac	802.11
Radio Range	500m
Simulation Time	60 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Transmitter Amplifier	150 pJ/bit/m^2
Package rate	4 pkt/s

Min Speed	1 m/s
Max Speed	5 m/s

Table1. Simulation settings and parameters of proposed algorithm.

➢ **MAC COLLISION RATE**

The average number of packets (including RREQ, route reply (RREP), RERR, and
CBR data packets) dropped resulting from the collisions at the MAC layer per second.

➢ **NORMALIZED ROUTING OVERHEAD**

The ratio of the total packet size of control packets (include RREQ, RREP,RERR, and Hello) to the total packet size of data packets delivered to the destinations. For the control packets sent over multiple hops, each single hop is counted as one transmission. To preserve fairness, use the size of RREQ packets instead of the number of RREQ packets, because the DPR and NCPR protocols include a neighbor list in the RREQ packet and its size is bigger than that of the original AODV.

➢ **PACKET DELIVERY RATIO**

The ratio of the number of data packets successfully received by the CBR destinations to the number of data packets generated by the CBR sources.

➢ **AVERAGE END-TO-END DELAY**

The average delay of successfully delivered CBR packets from source to destination node. It includes all possible delays from the CBR sources to destinations. The experiments are divided to three parts, and in each part evaluate the impact of one of the following parameters on the performance of routing protocols.

IV.2 SIMULATION RESULTS

Compare to the existing scheme CLMNR our proposed scheme CLSMRSCA achieves better performance in terms of following QOS parameters and network parameters.

- Mobility VS Overhead
- Throughput Vs Network Lifetime
- End to End delay Vs Speed
- No.of nodes Vs path reliability rate
- Simulation time Vs energy consumption

➢ **Mobility VS Overhead**

It is very important to reduce the redundant rebroadcast and packet drops caused by collisions to improve the routing performance. Compared with the conventional CLMNR protocol, the CLSMRSCA protocol reduces the MAC collision rate by about 92.8 percent on the average. Under the same network conditions, the MAC collision rate is reduced by about 61.6 percent when the CLSMRSCA protocol is compared with the CLMNR protocol. This is the main reason that the CLSMRSCA protocol could improve the routing performance.

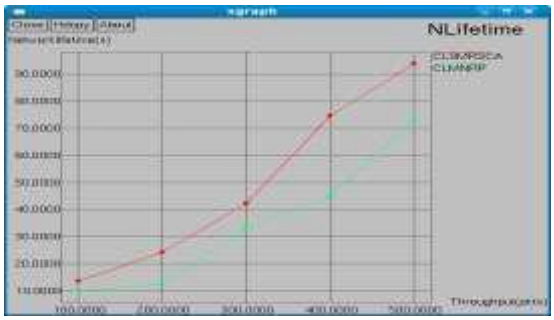
Fig.IV.1 shows the the comparison of overhead and mobility. It is clearly shown that the overhead of CLSMRSCA has low overhead than the CLMNRP protocol while varying mobility range from 20.0000 to 100.0000.

.

Figure IV.1 Mobility Vs Overhead

➢ **Throughput Vs Network Lifetime.**

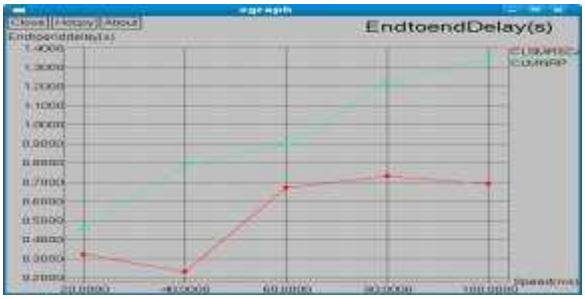
Figure IV.2 shows the results of Throughput Vs Network Lifetime. From the results, we can see that CLSMRSCA scheme has higher Network Lifetime than the CLMNRP while varying the Throughput from 100.0000 to 500.0000(pkts).



FigureIV.2ThroughputVsNetwork Lifetime

- **End to End delay Vs Speed**

  Figure IV.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 IV.3: End to End delay Vs Speed**

- **No.of nodes Vs path reliability rate**

Figure IV.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.

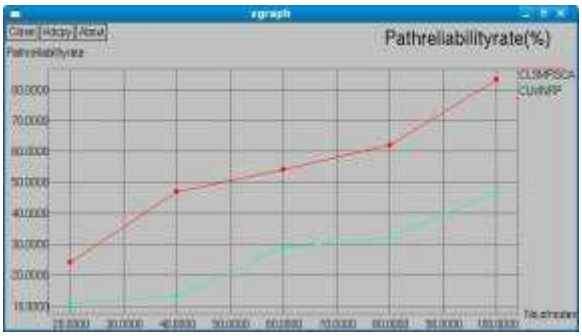


Figure IV.4: No.of nodes Vs path reliability rate

- **Simulation time Vs energy consumption**
  Figure 5.6 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.

.

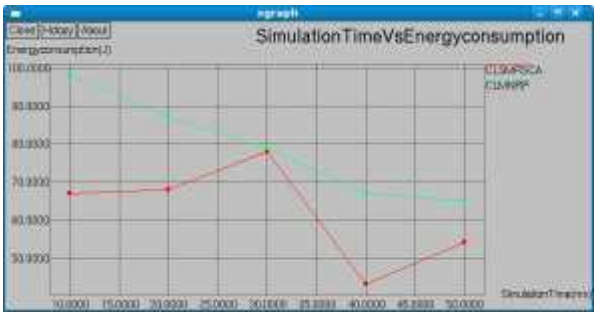


Figure IV.4: Simulation Time Vs Energy Consumption

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

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 InternationalJournalofComputerand

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.

[5] Djallel Eddine Boubiche and Azeddine Bilami,(2012),'Cross Layer Intrusion Detection System for Wireless Sensor Network', proceeding of International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, pp.No.1-18.

[6] Rekha Patil and Dr.A.Damodaram,(2008),'Cost Based Power Aware Cross Layer Routing Protocol For MANET', proceeding of IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp.No.1-6.

[7] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi and Seung-Jo Han,(2010),'A Novel Cross Layer Intrusion Detection System in MANET', proceeding of 24th IEEE International Conference on Advanced Information Networking and Applications, pp.No.1-8.

[8] Sandeep Sharma, Rajesh Mishra and Karan Singh,(2010),'Current Trends and Future Aspects in Cross Layer Design for The Wireless Networks', pp.No.1-14.

[9] Ravneet Kaur,(2011),' Cross layer based miss detection ratio under variable
rate for intrusion detection in WLAN', proceeding of International Journal of Computer Engineering Research Vol. 2(5), pp. 75-81.

AUTHORS PROFILE :

Dr.A. Rajaram received the **B.E.** degree in Electronics and Communication Engineering from the Government College of Technology, Coimbatore, Anna University, Chennai, India, in 2006, the **M.E.** degree in Electronics and Communication Engineering (Applied Electronics) from the Government College of Technology, Anna University, Chennai, India, in 2008 and he received the **Full Time Ph.D.** degree in Electronics and Communication Engineering from the Anna University of Technology, Coimbatore, India in March 2011. He is currently working as a Associate Professor, ECE Department in Karpagam College of Engineering, Coimbatore, India. His research interests include Mobile Ad Hoc networks, wireless communication networks **(WiFi, WiMax HighSlot GSM),** novel **VLSI NOC** Design approaches to address issues such as low-power, cross-talk, hardware acceleration,Design issues includes **OFDM MIMO** and noise Suppression in **MAI** Systems, **ASIC** design, Control systems, Fuzzy logic and Networks, **AI**, Sensor Networks.He has published 11 international journals including 4 impact factor referred journals, 1 National Journal, 2 International Conferences, 9 National Conferences.

H.Indrapriyadarshini received the B.E. degree in Electronics and Communication Engineering from the Anna University of Technology, Coimbatore, India, in 2009.She is currently pursuing M.E. degree in Electronics and Communication Engineering in Karpagam University, Coimbatore, India. She is currently working as a Lecturer, ECE Department in Karpagam Institute of Technology, Coimbatore, India. Her research interest Mobile Ad Hoc networks, wireless communication networks and Embedded.