ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.5

An Alternative Data Security and Load Balancing in Multiprotocol Label Switching Wireless LAN

Dr.T.Pandikumar[1], Zeleke Wondimu[2]
Associate Professor[1], M.Tech [2]
Department of Information Technology
Defence University, College of Engineering, Debre Zeyit, Ethiopia

Abstract:
In this research thesis we propose a Multiprotocol Label Switching (MPLS) based architecture and load balancing to provide data security in multi-hop Wireless Local Area Networks (WLAN). Wireless Local Area Networks (WLANs) have been widely developed in the past two decades, due to their mobility and flexibility. During this period, IEEE 802.11 has become the dominant WLAN protocol. The application of MPLS technology in multi-hop WLAN is evolving. Therefore, next generation wireless networks are required to have IP mobility solutions with high reliability, low latency handoffs, and trustworthy security. Multi-Protocol Label Switching (MPLS) offers a suitable environment to implement multi-path routing algorithms and Traffic engineering, as multiple parallel Label Switched Paths (LSPs) may be established to carry each a portion of a traffic flow. MPLS will enable it to seamlessly interoperate with existing WLAN infrastructures. The proposed work focus on splitting of a packet to sub-packet and forward to multipath and applying Modified Round Robin algorithm at ingress router to schedule packet. The incoming traffic from mobile nodes partitioned among the number of next hops according to predefined values. The MPLS splitting and label assignment policy is defined to handle link or node failures and handle local restoration. This work is implemented on Network Simulation 2 (NS_2) tool. The simulation results show that our proposed approach scales well to fulfill fast handoff/handover performance while providing security for transmitted data with minor bandwidth overhead.

Keywords: WLAN, MPLS, Reliability, Handoff, Security, routing, LSP, LAN, LER

I. INTRODUCTION

1. BACKGROUND

Wireless Local Area Network technology is a fast growing industry. IEEE 802.11 based wireless LANs (WLANs) are one of the primary enablers of untethered access to the Internet. This trend is clear from the emergence of various wireless, portable devices such as Personal Digital Assistants (PDAs), laptops and cellular phones and smart phone. With the development of WLANs technology, WLANs have become an integral part of wired networks. To meet the increasing demand for mobile services, wireless providers are currently implementing fourth generation (4G) and fifth generation (5G) networking technologies that are heavily based on the Internet Protocol (IP). To support mobile applications, Mobile IP (MIP) was developed. MIP provides seamless mobility when a Mobile Node (MN) moves across IP subnets. However, MIP was not designed to support fast handovers and seamless mobility in a handover-intensive environment. With the rapid movement of mobile nodes in the WLANs, the Access Point (AP) radius continues to decrease. This can bring more handovers from one AP to another AP, because of frequent registration updates. In order to handle fast hand over and network resilience Multi-Protocol Label Switching (MPLS) is a good solution. Multi-protocol label switching (MPLS) technology (E.Rosen, et.al 2001) has emerged as a pioneering networking technology in which large investments have been made by many internet service providers (ISPs). Nowadays, networks infrastructure of most tier-1 ISPs support MPLS properties and services. MPLS technology is widely spread due to its appealing benefits. The scalability of a network can be significantly improved with MPLS core networks. In addition, MPLS technology adds the ability to provide the best data traffic engineering services (B.John Oommen, et.al 2007, Lai, et.al 2008). Certainly, one of the most noticeable applications of MPLS is MPLS virtual private networks (VPN). The VPN services can now be offered to customers with low cost and with minimum configuration overhead (Solano, et.al 2008). There are a number of benefits of enabling a multi-hop option for wireless access to the Internet. An obvious advantage of such an architecture is the increase in the wireless coverage area. WLANs indicate that in many cases multi-hop extensions can improve the data throughputs. One way to construct this multi-hop access infrastructure is to use a routing layer based solution. In fact, a number of on-demand routing protocols have been defined to provide network level connectivity between arbitrary pairs of wireless nodes in an ad-hoc wireless network, e.g. Dynamic Source Routing(DSR) , Ad-hoc On Demand Vector(AODV), Temporally Ordered Routing Algorithm (TORA) , Zone Routing Protocol(ZRP) , etc. While these protocols can be used to construct appropriate multi-hop paths from the wireless clients to the Access Points (APs) of an 802.11 WLAN.

1.2 Problem Description

These days the amount of data which user send and received on internet is becoming very large, such as multimedia and other user data, therefore in order to provide good quality of service with relatively low cost, implementing of Multi-Protocol Label Switching with enhanced security is very important solution. Splitting traffic packets to sub-packets and forward to multipath multi hop wireless local area network and dynamic load balancing in multipath wireless network increase quality of service, and good throughput, ensure end-to-end packet delivery. It is difficult to avoid QoS problems, research works should be done to minimize these problems. Many research works show that Multiprotocol label switching solves QoS problem in data communication and VoIP of wired networks and ordinary wireless networks, but regarding MPLS WLANs, there is a limitation of study to improve the performance of network and security. In this area more researches should be done to improve end to end packet delivery ratio, maximize throughput, minimize packet delay, and load balancing among the same cost links and good security. Our proposal of research work focus on splitting a packet to sub-packets and distribute to multipath multi hop wireless local area network for security purpose and load balancing, our proposed technique provide alternative method of data security.

1.2 Scope of the Study

The scope of our project is limited to improving security and QoS of extended service set multi hop WLANs so that the wireless node can communicate with its correspondent node. The study give attention to the traffic splitting and load balancing algorithm at ingress router and how to route label packet and forward the labeled packet with multiple disjoint paths called LSR between edge routers. Split incoming traffic IP/UDP packet to sub-packets, and sub-packets flows are dispersed into multiple available label switched paths to perform load balancing and link utilization, sub-packet forward to each path using modified round robin algorithm. The sub-packets assign packet id (PID) at ingress and packet reordering is done at the egress based on PID. At the receiving side how the egress router removes the label and forward to the destination end. Generally the scope of the study is limited to MPLS enabled LER, LSR, Access points and mobile nodes.

MPLS based APs forwards packet or switch packets by its label, routers never check routing table to forward packet, instead swapping of labels takes place. Applying of MPLS on multi hop wireless network improves performance of the network and increase in the wireless coverage area, but MPLS by its nature not designed for secured data communication. Wireless network is largely prone to attackers and sniffers, data can be easily captured due to open medium communication. Network Traffic splitting along a given network is one way of load balancing technique to enhance the performance of the network and improve the data security. Our proposed system split network traffic packets to sub-packets. The edge ingress router or Label Edge Router (LER) is responsible to split the packet to sub-packets. Sub-packets assign labels and forwarded to intermediate routers or switch, Label Switch Routers (LSR). When sub-packets reach at egress routers, the egress router reveal label, reassemble sub-packets and forward to destination address. Packet reordering at the destination router is done when sub-packets reach out of order.

1I. LITEARTURE REVIEW

The application of MPLS in wireless networks, compared to its application in wired IP networks, is relatively new and has been recently gaining increasing attention by researchers in both academia and the industry. The majority of research proposals on MPLS application in wireless networks focus on access networks. Initial work towards supporting mobile and wireless networks by MPLS was first proposed by (Yu, et.al 2000).The paper proposes a lightweight near-seamless handoff scheme to support terminal mobility over a MPLS-based Internet supporting performance guarantees. The handoff scheme is supported by: (1) A mobile label switched tree (MLST) architecture which provides dynamic mobility tracking and adaptive traffic rerouting during handoffs; and (2) An extended RSVP to enable fast and robust resource reservation during handoffs. This work does not address the required detailed adaptation information with MPLS RFC standards. However, to our best knowledge, this work is the first to tackle the MPLS integration with wireless networks. A number of MPLS mobile IP solutions have been proposed. (Kim, et.al 2001) examined the mobility-aware MPLS as a micro-mobility scheme to provide micro-mobility with continuous QoS support. It does so by combining the advantages of MPLS, such as IP QoS support, with the advantages of host-based micro-mobility schemes, such as low-latency handoffs. (K.Xie, et.al 2001) presents an overview of MPLS-based micro-mobility management that includes label switched path setup, packet forwarding, handoff processing, and paging. In order to prevent packet loss during handoff, they propose a medium access control (MAC) layer assisted packet recovery scheme. A MAC buffer in the old base station caches the packets dropped by the MAC layer and forwards these packets to the new base station. This solution adds considerable overhead such as path configuration set up. Also, this solution is not scalable when applied to core networks. The work in Ref. (Bisti, et.al 2011) has presented a Fast-Re-Routing enabled architecture that is optimized for wireless mesh networks and allows nodes to react to local node or link failures by activating a pre-configured alternate path to reach a two-hop neighbor using MPLS technology. MPLS Label switching/stacking and Label distribution protocol (LDP) are the main two protocols used to implement this solution. Also, Ref. (A.Sameh, et.al 2010) is another paper which proposes an interesting QoS architecture for wireless networks. This architecture involves requirements at the mobile terminal for initiating or hopping LSPs at the air interface, and allowing end to end interconnection to the backbone network. It is worth noting that research demand on MPLS applications is continuously growing, currently, there is ongoing research on MPLS application with multi-path routing in wireless mesh network (Y. Zheng, et.al 2012). Moreover, new research areas for the application of MPLS in Mobile IPv6, MANET clustering, and Vehicular Ad Hoc Networks (VANET) are proposed in references (Khan, et.al 2012, Q. Li, et.al 2012, Fathy, et.al 2012). Another research work that related to the proposed system is A New MPLS-Based Forwarding Paradigm for Multi-Radio Wireless Mesh Networks (Stefano Avallone et.al 2013), this paper introduce a novel mechanism, denoted as MPLS splitting policy. Such mechanism allows configuring multiple next hops at an intermediate node, so that the incoming traffic is partitioned among the next hops according to predefined coefficients named split ratios. The MPLS splitting policy has been designed to allow for load balancing and fast local restoration. With such a mechanism, it is crucial to properly determine the set of split ratios, as they determine how the traffic is routed across the network. This work presented an approach to compute a set of split ratios that guarantee high performance under different traffic loads. The paper was mainly focus on robustness and throughput of wireless mesh network, but it didn't consider data security and confidentiality. Another work was proposed "A splitting infrastructure for load balancing and security in an MPLS network" (Stavallo, et.al 2007) which was focused on multi path wireless back bone network and load balancing by splitting the incoming traffic to per packet splitting. This work was done by applying MPLS architecture and the output of this work was tested on kernel based testbed. The aim of this work was to secure data by load balancing and MPLS tunneling. But when data is traffic data is splitting per packet the data packet has information about the traffic, therefore the packet sniffer can get information.

III.DESIGN AND METHDOLOGY

3.1 Design

Multiprotocol label switching (MPLS) is a connection oriented protocol mainly designed for high speed wired network and wireless back bone networks. Today the need of high speed wireless network and requirement of high bandwidth wireless network MPLS is being used and implemented in the future generation wireless networks. The type network we proposed consist of heterogeneous topology and structure, i.e. mobile nodes, access nodes and core network at the back bone network. The core network of our proposed system and access nodes are multiprotocol label switched enabled nodes. The access nodes provide access (services) to mobile nodes that moves between the access routers of the same domain or not and connect the mobile node and wired node at the back bone. The core IP/MPLS provides administrative function such as seamless mobility with guaranteed quality of services, This is achieved by interconnecting the enterprise customers over wireless and wired access for Business to Business, Business to Customer and Machine to Machine network. More over as we propose the edge routers splitting and tunneling of the traffic packet to send to multipath core network and load balancing is achieved. In WLAN especially the ESS the network consists of multiple mobile nodes and access points for extended service of wireless networks. This can maximize the quality of service of a given network and the network coverage area of access points also maximized. Therefore we have consider the ESS WLAN to maximize QoS of our proposed system and apply the load balancing algorithm by splitting the incoming traffic packet.

3.2 Multipath *Forwarding Mechanism*

The basic idea for our implementation of MPLS technology in wireless network backbones is to enforce data splitting at the edge routers or nodes and then distribute the packets in multi-path routes. The important role of load distribution is engineered by the traffic splitting and path selection, which are the key components of multipath forwarding and the focus of this paper. Note that separately analyzing these two components of a multipath forwarding mechanism is one of our main contributions that are expected to help readers understand load distribution models. After having described the general multipath forwarding mechanism, different types of traffic units and different path selection schemes will be discussed.

3.2.1 Basic Multipath Forward

Functional components of multipath forwarding: traffic splitting and path selection. The traffic splitting component splits the traffic into traffic units (Sumet Prabhavat, et.al 2012), each of which independently takes a path, which is determined by the path selection component. If the forwarding processor is busy, each traffic unit is queued in the input queue attached at the output link as determined by the path selection. Various multipath forwarding models perform load distribution in different manners. Each model exhibits different advantages and shortcomings because of the difference in their internal functional components, i.e., traffic splitting and path selection.

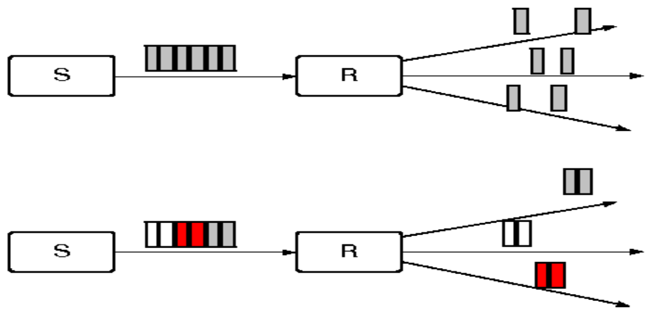

Figure 1. Traffic splitting and basic forwarding

3.2.2 Traffic Splitting

By the traffic splitting (Sumet Prabhavat, et.al 2012) component, aggregated traffic from traffic sources is split into several traffic units where the constitution of a traffic unit depends on the level of splitting granularity. In packet-level traffic splitting, traffic is split into the smallest possible scale, i.e., a single packet. Path selection is individually decided for each packet. A load distribution model with this kind of traffic splitting is referred to as a packet-based load distribution model. In flow-level traffic splitting, packet-identifiers determined rom destination addresses stored in packet headers, are taken into consideration in splitting. All packets heading for the same destinations are grouped together; each group is defined as a unit of flow with a unique flow identifier. Splitting traffic at this level can maintain packet ordering since path selection for all packets in the same flow is identical. The path selection for each flow is made independently. A load distribution model with this kind of traffic splitting is referred to as a flow based load distribution model. To further specify a particular flow, for example, packet header information such as source address, type of service, and protocol number can be used. In sub flow-level traffic splitting, a flow of packets heading for the same destination is allowed to be split into sub flows.

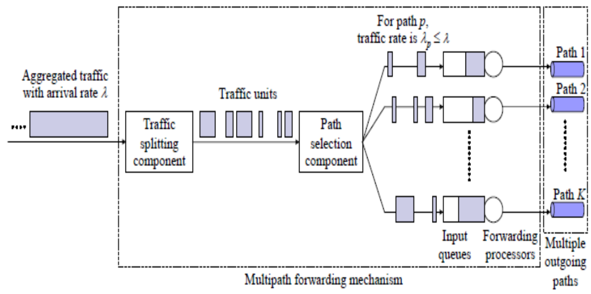

Figure.2. Path selection

3.3 Design and Implementation of MPLS Network Simulator

NS is an IP based simulator where a node consists of classifiers and agents. An agent is the sender/receiver object, while the classifier is the object that is responsible for classifying the arrived packets and then either forwarding them to the convenient nodes or delivering them to the local agent if the receiving node is the packet destination. Therefore, in order to construct an (Gaeil Ahn et.al 2001), MPLS node, a new classifier called « MPLS classifier » should be created in order to be able to classify the received packets, determines whether they are labeled or not, and treat them correspondingly. Also, a new agent « LDP agent » must be also inserted in the IP node in order to distribute labels with other MPLS nodes and construct the LSP paths. The architecture (Gaeil Ahn et.al 2001) of an MPLS node including the MPLS classifier and the LDP agent is shown in the figure 3:

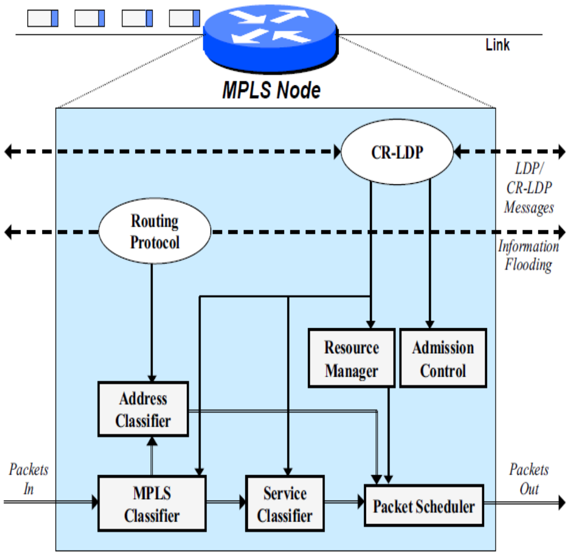

Figure .3. Conceptual model of MNS

When a node receives a packet, its MPLS classifier determines whether the received packet is labeled or not. If the received packet is labeled, the classifier will execute L2 switching. It replaces (swap) the label present in the MPLS header of the packet with the outgoing label corresponding to the packet's destination (FEC). And then transmits it to the next node. If the received packet is unlabeled and an LSP already exists for the packet destination (FEC), then the classifier will create an MPLS header, push an outgoing label in, and transmits the packet to the corresponding next hop. In case when the received packet is not Labeled and no LSP exist, the MPLS node will deliver the packet to the address classifier which execute ordinary L3 forwarding by examining the packet's destination address. The packet will be delivered to the port classifier when the receiving node is the destination of the packet. This port classifier will deliver the packet to the convenient agent. The LDP agent is used as we will see next to distribute labels and initiate LSPs based on the Label distribution protocol LDP. An MPLS node has three tables to manage the information related to the LSP and the label distribution. The three tables are the following:

3.3.1 The Label Information Base LIB table

This table is constructed and used to map the (Incoming Label, Incoming interface) couple to (Outgoing Label, Outgoing interface). It is then used when L2 operation is to be executed, that is when a labeled packet is received and a Label swap to be done or when an unlabeled packet is received and a label push is required. Therefore this table must contain the following five fields

- Incoming Label
- Incoming interface
- Outgoing Label
- Outgoing interface
- LIBptr (used in the PFT and ERB tables)

3,3,2 The Partial Forwarding PFT table

This table is used when an unlabeled packet arrives. The MPLS node will search this table for an entry where the FEC is the packet's destination address. The entry could either point to an entry in the LIB table to perform the convenient label push operation or point to NULL and as a result ordinary L3 forwarding is being done. Therefore this table must contain the following three fields:

- FEC
- PHB (per hop behavior)
- LIBptr (pointer to the LIB table)

3.3.3 The Explicit Routing information Base ERB table

This table is used only to keep the information for ER-LSP so it does not participate in the packet forwarding. The only thing to be done if an explicit route is desired is to insert a new entry with the same LIB pointer in the PFT table. Therefore this table must contain the following three fields:

- FEC
- LSPID
- LIBptr (pointer to the LIB table)

3.4 Packet Reordering

Reordered packets arriving the destination within a certain period of time, referred to as the timeout period, can be successfully recovered via the reordering buffer, at the expense of the increase of packet delay (V. Paxon et.al 1998, C. Demichlis et.al 2002). On the other hand, if reordered packets arrive after the timeout period is over, they are treated as lost packets, thus resulting in not only additional packet delay and but also inefficient network resource utilization for packet retransmissions. In other words, reordering can significantly affect the end-to-end performance as well as network performance. Although it is possible to reduce the occurrence of packet reordering by increasing the size of the reordering buffer, it comes with the price of a longer packet delay. Forwarding all packets bound for the same destination via the same path can completely prevent the reordering problem at the expense of load imbalance (S. Prabhavat, et.al 2009). These trade-offs need to be taken into account in mitigating the packet reordering issue.

IV. IMPLEMENTATION

This chapter deals about the detail implementation of the thesis project on NS2 simulator and results and analysis from implementation. In this stage we have include results from research. By reporting on the implementation, a clear picture is given of the research task and of the process through which we have sought to reach the goal of the research.

4.1 Proposed System

The proposed system is splitting traffic data and tunneling with tunnel id with in mpls domain so that possible attacks on traffic data can be reduced. The packets which transmit from correspondent node to mobile nodes is tunneled in mpls domain and send to mobile nodes through abroad foreign access routers. Mobile nodes send continuous control signals to its home agent routers to update its position, So that handoff delay and end to end delay can be reduced when mobile nodes move from one access router to another domain. Traffic data send from mobile nodes to correspondent is splitted at edge access routers and the ingress node send label request to the egress node, the egress router replies for available label and with suitable path, when the ingress node receive label it label the splitted data packet and transmit to egress node. Multiple mobile nodes can send data to a correspondent node simultaneously and a correspondent node can send to multiple mobile nodes. The splitting agent is attached to ingress node and splitting the incoming traffic to predefined payload data size. Once the data is splitted, the splitter agent pass the data to labeled, after data is labeled it pass to available path, in case of multiple paths available it selects suitable path based on the cost of the link. When labeled packet reach at egress the label removed from packet and forward to its destination address.

5.2 Implementation of the System

Table 1. Parameters used for simulation

Parameter type used	Value
Simulation start time	1.0sec
Simulation end time	12.0sec
Number of mobile nodes	10,20
Energy of nodes	100
Speed of mobile nodes	10, 25, 50, 100, 150, 200, 250, 300
Range of coverage	500m
Area	1000X1000
Interface queue length	1000
Interface queue type	Queue/WRR
mac	Mac/802_11
Packet size	512

In order to carry out some tests on the designed system, we have to implement it on a suitable language and platform. So we make a choice of the implementation language and implement it in a way that is convenient for simulation.

4.2 Network Animator (NAM)

NAM is a Tcl/TK based animation tool for viewing network simulation traces and real world packet traces. It supports topology layout, packet level animation, and various data inspection tools. It has a graphical interface, which can provide information such as number of packets drops at each link. The network animator "NAM" began in 1990 as a simple tool for animating packet trace data. Nam began at LBL. It has evolved substantially over the past few years. The NAM development effort was an ongoing collaboration with the VINT project. Currently, it is being developed as an open source project hosted at Source forge. This trace data is typically derived as output from a network simulator like ns or from real network measurements. We can either start NAM with the command **'nam <nam-file>'** where '<nam-file>' is the name of a NAM trace file that was generated by NS or one can execute it directly out of the Tcl simulation script for visualization of node movement.

4.2.1 Implementation of the protocol

The protocol implementation has two parts. The first part of the implementation is the implementation of the packet structure. It basically consists of different variables and elements of the protocol that are used in the agent. It is implemented in a struct type like to create the split packet.

```
struct hdr_split {
int cell_num;
int pkt_size;
…}
};
```

There are additional variables like packet type, seqno, components that are used for fulfilling the protocols functionalities. The second part of the protocol implementation is the agent class. A class called **SplitAgent()** is derived from the Agent base class. It consists of different functions that are needed for full operation of the protocol. The major functions in it include the following

void SplitAgent::recv(Packet* pkt, Handler*)

It is a function that is inherited from the base class Agent (). The function basically guides the protocol in taking appropriate action when an agent receives packets. Specifically this function will be invoked when one of the nodes (intermediate node, home agent or correspondent node) receives any of the messages. Once the message is received, the agent checks the type of message and responds appropriately. If the packet type is “PT_SPLIT” the node receive and reassemble, Otherwise node split the packet and send to the destination.

void PassAgent::recv(Packet* pkt, Handler*)

This function checks if the packet type which is received and if the packet type is “PT_SPLIT” it sends upward for reassemble, otherwise it forwards to destination address, it never split packet.

4.3 Simulation and Analysis of Results

After the implementation is done the system was tested for its performance. Based on the tests made, the results are obtained in trace files and manipulated accordingly to calculate the required parameters. Results made from our tests were used for making analysis of our system. The analysis is made for performance of the system.

4.3.1 Simulation Setup

In order to test our system we set our basic simulation setup and simulation parameters. The setup consists of the basic components of our system ESS WLAN, which are the mobile node, the home agent and correspondent nodes which are interconnected based on a way that represents real environment. Once the setup is created simulation parameters were set and the number of mobile nodes and speed was varied as it could occur in real world situation.

4.3.2 Simulation Topologies

The following various topologies are used to simulate our proposed system

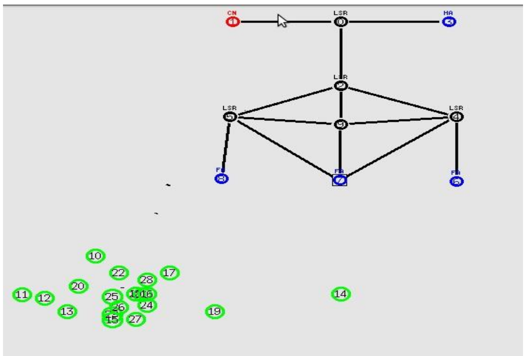

Figure.4. Single path 20 mobile nodes topology

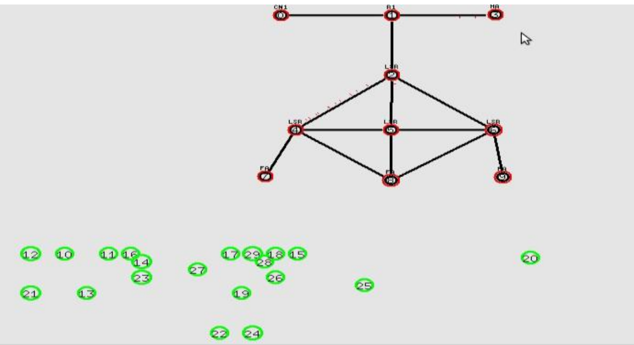

Figure 5. Multipath path 20 mobile nodes topology

V. CONCLUSION AND FUTURE WORK

5.1 CONCLUSION

In our analysis we have observed that the simulation generate huge amount of control packet that helps the mobile nodes and home agent communicate each other and update information about the position of mobile nodes. This control signal packets is very advantageous to keep communication going and are also helpful to minimize handoff delay since nodes registered to home agent and foreign agent can get information about the mobile nodes before it reaches to new access area. But mobile nodes sends this control packets continuously with some gap of time and this can affect the performance of the network by increasing packet processing delay of edge and intermediate nodes. The proposed system has very good performance in packet delivery ratio, Network throughput and average end-to-end delay. Packet delivery ratio of the proposed system for multipath network routing is 100%, and it has also very good packet delivery ratio for single path, by average 99.98%. Throughput of the proposed system is very high within a given range of node mobility. Average end-to-end delay of the proposed system with single path and multipath has a big difference, so that we can see average end-to-end delay can be minimized by using multipath network routing. The proposed system reduce end to end delay, maximize the throughput and has very good packet delivery ratio of future WLAN. The system enhance QoS and security for the future high speed WLAN. Application of multiprotocol label switching and load balancing helps the proposed system to enhance the QoS and security of the system. The multiple access points in ESS in WLAN helps to minimize the handoff delay as the mobile node move from one access router domain to others and availability of multiple access points helps the network to increase the throughput.

5.2 *Future Work*

This work is implemented with single path and multipath routing at the back bone of wireless local area network, packet transmission take place in multiple paths simultaneously. Packet send from mobile node to access node should be secured with cryptographic data security. To secure data communication on Local Wireless Network before the data transmission start the access router and mobile node should authenticate each other. Proper authentication should implemented in the future.

VI. REFERENCES

[1]. E. Rosen, A. Viswanathan, and R. Callon (2001) Multiprotocol Label Switching Architecture, IETF, RFC 3031.

[2].B. John Oommen, Sudip Misra, Ole-Christoffer Granmo. (2007). Routing Bandwidth-guaranteed paths in MPLS traffic engineering: A multiple race track learning approach, IEEE Transactions on Computers, pp. 959–976.

[3]. Lai, Wei Kuang, Zheng, Zhen Chang, & Tsai, Chen-Da. (2008). Fast reroute with pre-established bypass tunnel in MPLS’’. Computer Communications, 31(9), 1660–1671.

[4]. Solano, F., Fabregat, R., & Marzo, J. L. (2008). On optimal computation of MPLS label binding formultipoint-to-point connections. IEEE Transactions on Communications, 56(7), 1056–1059.

[5]. Langar, R., Bouabdallah, N., & Boutaba, R. (2008). A comprehensive analysis of mobility management in MPLS-based wireless access networks. IEEE/ACM Transactions on Networking, 16(4), 918–927.

[6].A.Taghizadeh, W.at-Chee,and R. Budiatro. (2010). MPLS assisted handover in ip-based mobility management schemes: A survey, second international conference on computer research and development, pp. 34–38.

[7]. Yu, O. T. W. (2000). Next generation MPLS-based wireless mobile network. IEEE Wireless Communications and Networking Conference, 3, 1193–1198.

[8].Kim, H., Wong, K., Chen, W., & Lau, C. (2001). Mobility-aware MPLS in IP-based wireless access networks. IEEE Globecom, 6, 3444–3448.

[9]. K. Xie, V. Wong, and V. Leung. (2003). Support of micromobility in MPLS-based wireless access networks, in Proc. Of IEEE WCNC, New Orleans, Louisiana, pp. 1242–1247.