A Review on Strategies to Optimize and Enhance the performance of WLAN and Wireless Networks

Rosslin Robles and Maricel O. Balitanas

Western Visayas College of Science and Technology
rosslin_john@yahoo.com, jhe_c1756@yahoo.com

Abstract

WLAN is a type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. In this paper, we propose strategy for internetworking of WLAN and MANET. MANET and WLAN are based on IEEE 802.11 for MAC layer protocol while they adopt different mode, such as infrastructure and ad-hoc. An optimize Performance Improvement Scheme of Transmission Protocol over Wireless Networks is also discussed.

Keywords: *Networks, WLAN, LAN, Wireless Protocols*

1. Introduction

MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. They are also a type of mesh network, but many mesh networks are not mobile or not wireless. Wireless LANs have gained strong popularity in a number of vertical markets, including the health-care, retail, manufacturing, warehousing, and academia. These industries have profited from the productivity gains of using hand-held terminals and notebook computers to transmit real-time information to centralized hosts for processing.

Today wireless LANs are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers. In the next sections, We present MANET and WLAN more briefly and presents Review on Strategies to Optimize and Enhance the performance of WLAN and Wireless Networks.

2. WLAN

A wireless local area network (LAN) is a flexible data communications system implemented as an extension to, or as an alternative for, a wired LAN. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections. Thus, wireless LANs combine data connectivity with user mobility. [1]

Wireless LANs have gained strong popularity in a number of vertical markets, including the health-care, retail, manufacturing, warehousing, and academia. These industries have profited from the productivity gains of using hand-held terminals and notebook computers to transmit real-time information to centralized hosts for processing. Today wireless LANs are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers.

The widespread reliance on networking in business and the meteoric growth of the Internet and online services are strong testimonies to the benefits of shared data and shared resources. With wireless LANs, users can access shared information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires. Wireless LANs offer the following productivity, convenience, and cost advantages over traditional wired networks:

- Mobility: Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.
- Installation Speed and Simplicity: Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- Installation Flexibility: Wireless technology allows the network to go where wire cannot go.
- Reduced Cost-of-Ownership: While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.
- Scalability: Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area.

Wireless LANs frequently augment rather than replace wired LAN networks-often providing the final few meters of connectivity between a wired network and the mobile user. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs: [1]

- Trade show and branch office workers minimize setup requirements by installing pre-configured wireless LANs needing no local MIS support.
- Warehouse workers use wireless LANs to exchange information with central databases, thereby increasing productivity.
- Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.
- Senior executives in meetings make quicker decisions because they have real-time information at their fingertips.
- Doctors and nurses in hospitals are more productive because hand-held or notebook computers with wireless LAN capability deliver patient information instantly.
- Consulting or accounting audit teams or small workgroups increase productivity with quick network setup.
- Students holding class on a campus greensward access the Internet to consult the catalog of the Library of Congress.

- Network managers in dynamic environments minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.
- Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.
- Network managers installing networked computers in older buildings find that wireless LANs are a cost-effective network infrastructure solution.

2.1 Autonomous Architecture

In the autonomous architecture, the WTPs completely implement and terminate the 802.11 function so that frames on the wired LAN are 802.3 frames. Each WTP can be independently managed as a separate network entity on the network. The access point in such a network is often called a “Fat AP” as shown in Figure 1. [2]

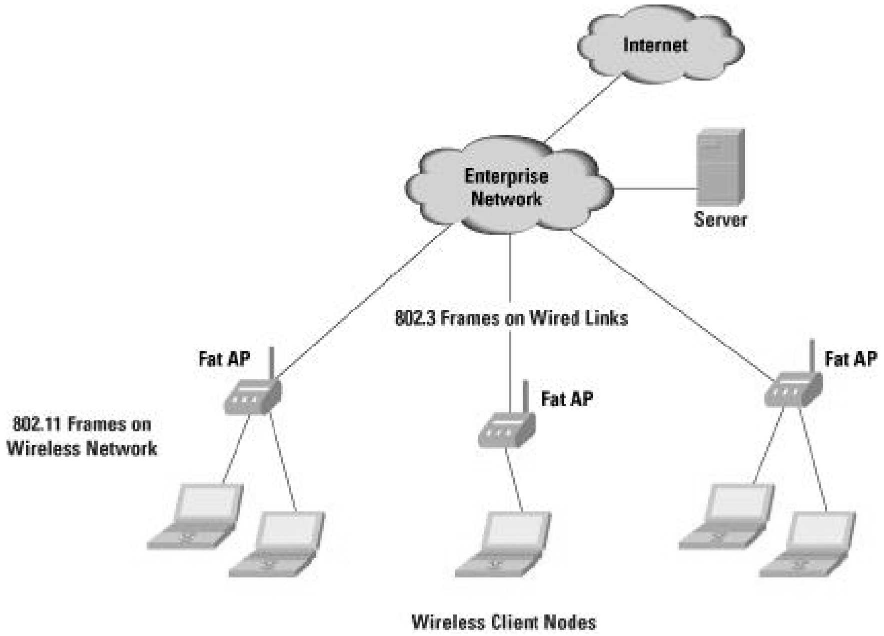

Figure 1. Autonomous WLAN Network Architecture

During the initial stages of WLAN deployment, most APs were autonomous APs, and manageable as independent entities in the network. During the past few years, centralized architectures (discussed next) with ACs and WTPs have gained popularity. The primary advantage of the centralized architecture is that it provides network administrators with a structured and hierarchical mode of control for multiple WTPs in the enterprise. [2]

2.2 Centralized Architecture

The centralized architecture is a hierarchical architecture that involves a WLAN controller that is responsible for configuration, control, and management of several WTPs. The WLAN controller is also known as the Access Controller (AC). The 802.11 function is split between the WTP and the AC. Because the WTPs in this model have a reduced function as compared to the autonomous architecture, they are also known as “Thin APs.” Some of the functions on the APs are variable, as discussed in the following section as shown in Figure 2. [2]

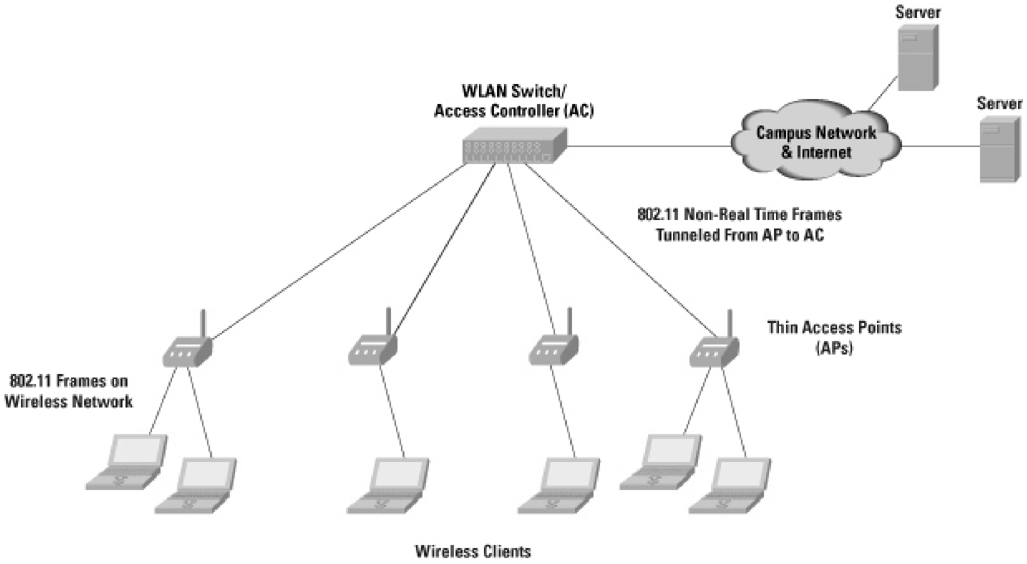

Figure 2. Centralized WLAN Network Architecture

2.3 Distributed Architecture

In the distributed architecture, the various WTPs can form distributed networks with other WTPs through wired or wireless connections. A mesh network of WTPs is one example of such architecture. The WTPs in the mesh can be linked with 802.11 links or wired 802.3 links. This architecture is often used in municipal networks and other deployments where an “outdoor” component is involved. This article does not address the distributed architecture. [2]

3. MANET

A MANET (mobile ad hoc network), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links.[3]

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

MANETs are a kind of wireless ad hoc networks that usually has a routeable networking environment on top of a Link Layer ad hoc network. They are also a type of mesh network, but many mesh networks are not mobile or not wireless.

The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid- to late 1990s. Many academic papers evaluate protocols and abilities assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other and usually with nodes sending data at a constant rate. Different protocols are then evaluated based on the packet drop rate, the overhead introduced by the routing protocol, and other measures. [4]

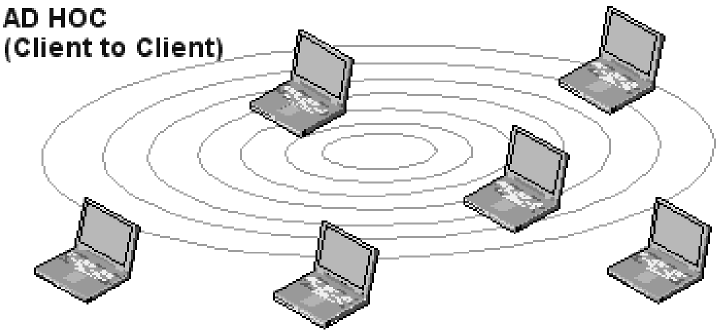

Figure 3. A Wireless Mesh. When laptops are set up to transmit in "ad hoc" mode, they create a wireless mesh network.

3.1 Vehicular Ad-Hoc Network or VANET

The main goal of VANET is providing safety and comfort for passengers. To this end a special electronic device will be placed inside each vehicle which will provide Ad-Hoc Network connectivity for the passengers. This network tends to operate without any infra-structure or legacy client and server communication. Each vehicle equipped with VANET device will be a node in the Ad-Hoc network and can receive and relay others messages through the wireless network. Collision warning, road sign alarms and in-place traffic view will give the driver essential tools to decide the best path along the way. [6]

There are also multimedia and internet connectivity facilities for passengers, all provided within the wireless coverage of each car. Automatic payment for parking lots and toll collection are other examples of possibilities inside VANET.

Most of the concerns of interest to MANets are of interest in VANets, but the details differ. Rather than moving at random, vehicles tend to move in an organized fashion. The interactions with roadside equipment can likewise be characterized fairly accurately. And finally, most vehicles are restricted in their range of motion, for example by being constrained to follow a paved highway. In addition, in the year 2006 the term MANet mostly describes an academic area of research, and the term VANet perhaps its most promising area of application.

InVANET, or Intelligent Vehicular Ad-Hoc Networking, defines an Intelligent way of using Vehicular Networking. InVANET integrates on multiple ad-hoc networking technologies such as WiFi IEEE 802.11 b/g, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee for easy, accurate, effective and simple communication between vehicles on dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well methods to track the automotive vehicles is also preferred. InVANET helps in defining safety measures in vehicles, streaming communication between vehicles, infotainment and telematics.

Vehicular Ad-hoc Networks are expected to implement variety of wireless technologies such as Dedicated Short Range Communications (DSRC) which is a type of WiFi. Other candidate wireless technologies are Cellular, Satellite, and WiMAX. Vehicular Ad-hoc Networks can be viewed as component of the Intelligent Transportation Systems (ITS).

Vehicular Networks are an envision of the Intelligent Transportation Systems (ITS). Vehicles communicate with each other via Inter-Vehicle Communication (IVC) as well as with roadside base stations via Roadside-to-Vehicle Communication (RVC). The optimal goal is that vehicular networks will contribute to safer and more efficient roads in the future by providing timely information to drivers and concerned authorities.

The main goal of VANET is providing safety and comfort for passengers. To this end a special electronic device will be placed inside each vehicle which will provide Ad-Hoc Network connectivity for the passengers. This network tends to operate without any infrastructure or legacy client and server communication. Each vehicle equipped with VANET device will be a node in the Ad-Hoc network and can receive and relay others messages through the wireless network. Collision warning, road sign alarms and in-place traffic view will give the driver essential tools to decide the best path along the way.[5]

3.2 Intelligent Vehicular ad-hoc Network

Intelligent vehicular ad hoc networks (InVANETs) use WiFi IEEE 802.11 and WiMAX IEEE 802.16 for easy and effective communication between vehicles with dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well methods to track automotive vehicles. InVANET is not foreseen to replace current mobile (cellular phone) communication standards . "Older" designs within the IEEE 802.11 scope may refer just to IEEE 802.11b/g. More recent designs refer to the latest issues of IEEE 802.11p (WAVE, draft status). Due to inherent lag times, only the latter one in the IEEE 802.11 scope is capable of coping with the typical dynamics of vehicle operation. [7]

Automotive vehicular information can be viewed on electronic maps using the Internet or specialized software. The advantage of WiFi based navigation system function is that it can effectively locate a vehicle which is inside big campuses like universities, airports, and tunnels. InVANET can be used as part of automotive electronics, which has to identify an optimally minimal path for navigation with minimal traffic intensity. The system can also be used as a city guide to locate and identify landmarks in a new city. Communication capabilities in vehicles are the basis of an envisioned InVANET or intelligent transportation systems (ITS). Vehicles are enabled to communicate among themselves (vehicle-to-vehicle, V2V) and via roadside access points (vehicle-to-roadside, V2R). Vehicular communication is expected to contribute to safer and more efficient roads by providing timely information to drivers, and also to make travel more convenient. The integration of V2V and V2R communication is beneficial because V2R provides better service sparse networks and long distance communication, whereas V2V enables direct communication for small to medium distances/areas and at locations where roadside access points are not available. [7]

Providing vehicle-to-vehicle and vehicle-to-roadside communication can considerably improve traffic safety and comfort of driving and traveling. For communication in vehicular ad hoc networks, position-based routing has emerged as a promising candidate. For Internet access, Mobile IPv6 is a widely accepted solution to provide session continuity and reachability to the Internet for mobile nodes. While integrated solutions for usage of Mobile IPv6 in (non-vehicular) mobile ad hoc networks exist, a solution has been proposed that, built upon on a Mobile IPv6 proxy-based architecture, selects the optimal communication mode (direct in-vehicle, vehicle-to-vehicle, and vehicle-to-roadside communication) and provides dynamic switching between vehicle-to-vehicle and vehicle-to-roadside communication mode during a communication session in case that more than one communication mode is simultaneously available. Currently there is ongoing research in the field of InVANETs for several scenarios. The main interest is in applications for traffic scenarios, mobile phone systems, sensor networks and future combat systems. Recent research has focused on topology related problems such as range optimization, routing mechanisms, or address systems, as well as security issues like traceability or encryption. In addition, there are very specific research interests such as the effects of directional antennas for InVANETs and minimal power consumption for sensor networks. Most of this research aims either at a general approach to wireless networks in a broad setting or focus on an extremely specific issue. [7]

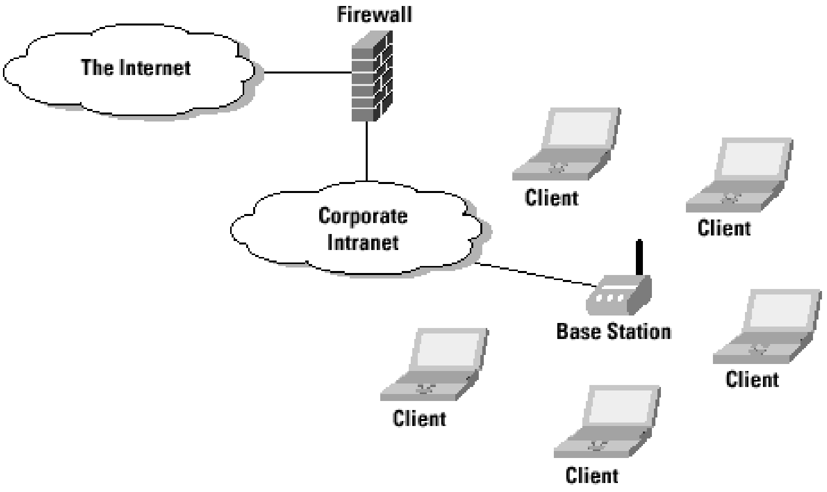

Figure 4. Typical IEEE 802.11 Configuration

4. Related Studies

4.1 IEEE 802.11

Networks in IEEE 802.11 are classified into two structures, such as infrastructure and ad hoc [8]. In infrastructured structure, access point (AP) is easily found in a network, as shown Fig ure 4. Basic unit for infrastructured structure is Basic Service Set (BSS), where station group communicates each other with no help from AP or others. The Extended Service Set (ESS) is the set of BSS. The ad-hoc network is Independent Basic Service Set (IBSS), where no AP is found, and mobile stations communicate each other as peer-to-peer.

4.2 OLSR (Optimized Link State Routing)

OLSR is optimized link state algorithm for mobile ad hoc networks. OLSR belongs to a proactive routing protocol [9] and helps nodes to keep all routing information in network. The unique point of OLSR is the set of selected nodes to forward broadcast control message, MPRs. A node in network selects MPRs among its one hop neighbors, and only MPRs flood control traffic. OSLR employs such hierarchical model to configure a network, which minimizes the overhead from flooding of control traffic to all nodes in the network. Basic requirement for MPR selection is whether there is bi-directional link between a given node and MPR, which avoids problems from data transfer over uni-directional link. To build the route from a given node to any destination in the network, the MPRs are also used [10].

In OLSR, three message types are defined; HNA, Hello and Topology Control (TC) messages. Main functions of OLSR are summarized as neighbor discovery and topology dissemination. For neighbor discovery, each node in network exchanges Hello message periodically. This Hello message contains the list of neighbors. The Hello message is only processed within all one-hop neighbors, not forwarded to others. The Hello message enables every node to discover one-hop and two-hop neighbors. MANET Gateway periodically broadcasts HNA message which contains

prefix information for address configuration and subnet information where the Gateway belongs. This message will notify other nodes in network that the Gateway is the door to public network.

4.3 IP Mobility

Mobile IP (or IP mobility) is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address. Mobile IPv4 is described in IETF RFC 3344 (Obsoleting both RFC 3220 and RFC 2002), and updates are added in IETF RFC 4721. Mobile IPv6 is described in IETF RFC 3775.

The Mobile IP protocol allows location-independent routing of IP datagrams on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet. While away from its home network, a mobile node is associated with a care-of address which identifies its current location and its home address is associated with the local endpoint of a tunnel to its home agent. Mobile IP specifies how a mobile node registers with its home agent and how the home agent routes datagrams to the mobile node through the tunnel.

Mobile IP provides an efficient, scalable mechanism for roaming within the Internet. Using Mobile IP, nodes may change their point-of-attachment to the Internet without changing their home IP address. This allows them to maintain transport and higher-layer connections while roaming. Node mobility is realized without the need to propagate host-specific routes throughout the Internet routing fabric.

Mobile IP is most often found in wired and wireless environments where users need to carry their mobile devices across multiple LAN subnets. It may for example be used in roaming between overlapping wireless systems, for example IP over DVB, WLAN, WiMAX and BWA. Currently, Mobile IP is not required within cellular systems such as 3G, to provide transparency when Internet users migrate between cellular towers, since these systems provide their own data link layer handover and roaming mechanisms. However, it is often used in 3G systems to allow seamless IP mobility between different Packet Data Serving Node (PDSN) domains.

A mobile node can have two addresses - a permanent home address and a care of address (CoA), which is associated with the network the mobile node is visiting. There are two kinds of entities in Mobile IP:

- A home agent stores information about mobile nodes whose permanent home address is in the home agent's network.
- A foreign agent stores information about mobile nodes visiting its network. Foreign agents also advertise care-of addresses, which are used by Mobile IP.

A node wanting to communicate with the mobile node uses the permanent home address of the mobile node as the destination address to send packets to. Because the home address logically belongs to the network associated with the home agent, normal IP routing mechanisms forward these packets to the home agent. Instead of forwarding these packets to a destination that is physically in the same network as the home agent, the home agent redirects these packets towards the foreign agent through an IP tunnel by encapsulating the datagram with a new IP header using the care of address of the mobile node.

When acting as transmitter, a mobile node sends packets directly to the other communicating node through the foreign agent, without sending the packets through the home agent, using its permanent home address as the source address for the IP packets. This is known as triangular routing. If needed, the foreign agent could employ reverse tunneling by tunneling the mobile node's packets to the home agent, which in turn forwards them to the communicating node. This is needed in networks whose gateway routers have ingress filtering enabled and hence the source IP address of the mobile host would need to belong to the subnet of the foreign network or else the packets will be discarded by the router. The Mobile IP protocol defines the following:

- an authenticated registration procedure by which a mobile node informs its home agent(s) of its care-of-address"(es);
- an extension to ICMP Router Discovery, which allows mobile nodes to discover prospective home agents and foreign agents; and
- the rules for routing packets to and from mobile nodes, including the specification of one mandatory tunneling mechanism and several optional tunneling mechanisms.

4. Strategies to Optimize and Enhance the performance of WLAN and Wireless Networks

In this section we review the Strategies to Optimize and Enhance the performance of WLAN and Wireless Networks

4.1 Optimized Internetworking Strategy of MANET and WLAN [12]

This was designed to integrate the architecture of MANET and MIPv6. When a mobile node moves and enters into dead spot, where it sensors only ad-hoc network, not public network, connection to public network is supported by MANET Gateway. The mobile node is able to listen to any IEEE 802.11 frame format, but no standards for handoff between ad-hoc and infrastructure are present while handoffs between adhoc modes or between infrastructure modes are present. For internetworking between MANET and MIPv6, handoff mechanism between different modes is required.

MIPv6 protocol is employed for mobile devices within public network, and OLSR is employed in MANET. The OLSR protocol holds all networks routing information, and optimization is performed via MPRs, which is very good for large and dense networks. OLSR accepts original IP packet format, and no change is required, so OLSR seems to be very adequate for integration of MANET and MIPv6. [12]

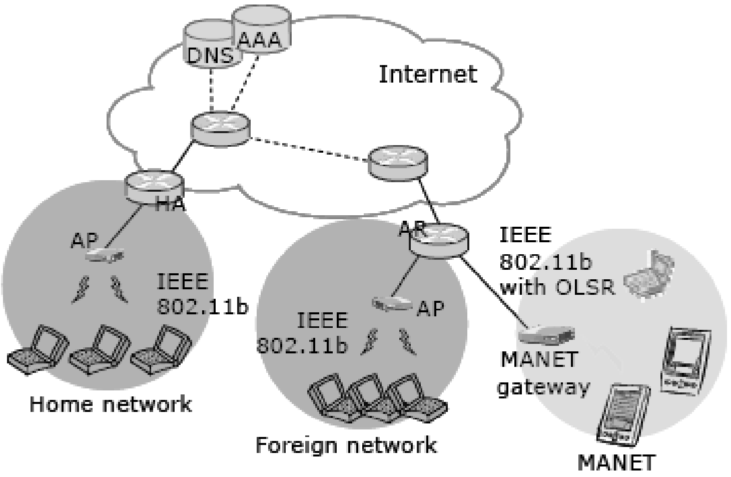

Figure 5. Internetworking between WLAN and MANET

This architecture is shown in Figure 5. The network is divided into three parts; WLANs based on MIPv6, MANET and Internet, mainly wired public networks. As shown in Fig. 2, WLAN is directly connected to public networks, while MANET is connected to public networks via MANET Gateway. The MANET Gateway is a link between MANET and WLAN. In OLSR-based MANET, two new node types are defined, as follows:

− MANET Gateway: A static node provides connection to nodes in MANET into WLAN. The MANET Gateway periodically broadcasts HNA message into network. Its main function is to notify foreign nodes in MANET of outside subnet information where it is attached and prefix information.

− MANET Router: General OLSR-enabled nodes are simply called MANET Router. MANET Router may be assigned with more than one address. From MIPv6's angle, MANET is regarded as foreign network. Once a mobile node enters pollution area, where it receives different kinds of IEEE 802.11 MAC frames with higher signal strength than threshold, it may keep its current network connection or change into the different mode, depending on the switching algorithm specified below. As the mobile node determines to change mode, new care-of address is required. A periodical HNA message from MANET Gateway informs the mobile node of prefix information and its subnet routing information. From this message, the mobile node knows the MANET Gateway is the door to Internet. Now, the mobile node builds care-of address, and starts registration process with home agent. Besides, this mobile node will join in MANET. The mobile node exchanges Hello message with its neighbored nodes. When the mobile node keeps moving and goes away from the MANET Gateway by several hops, packets originated from the mobile node and destined to some node out of MANET will be delivered to MANET Gateway using OLSR, and the Gateway will forward it to AR using MIPv6 protocol.

4.2 Snoop Protocol

The snoop is a TCP aware link layer protocol. Snoop was designed so that the wired infrastructure of the network would need no changes. Since Snoop protocol does not require changing wired network, it is good candidate for our system [13]. So, we modified snoop protocol for SCTP which means it supports multi-homing and multi-stream.[13]

To support the multi-homing and the multi-streaming of SCTP, SCTP-Snoop agent executes followings: SCTP interchanges INIT Chunk and INIT-ACK Chunk, which are needed information for multi-homing and multi-streaming, during association establishment. In the process of exchange, SCTP-Snoop agent gets and stores addresses of Sender and receiver included INIT Chunk and INIT-ACK Chunk. If the packet losses have occurred by receiver, SCTP-Snoop agent will judge a problem by a transmission path. So, SCTP Snoop transfers lost packets by selecting one of transmission paths. Also, SCTP Snoop checks lost chunks through Gap Ack Block field of SCTP SACK-Chunk, and retransmits lost chunks stored in buffer.

The snoop module has two linked procedures, snoop_data() and snoop_ack(). Snoop_data() processes and caches packets intended for the mobile host(MH) while snoop_ack() processes acknowledgments (ACKs) coming from the MH and drives local retransmissions from the base station to the mobile host. The flowcharts summarizing the algorithms for snoop_data() and snoop_ack() are shown in Figure 6 and Figure 7 , and their working details are described in brief below.

In Figure 6, when the data chunk packet is received by base station with snoop agent, if it is not the new data chunk which is adjudged through the Transmission Sequence Number (TSN) of SCTP, the agent forwards it to the receiver without storing to buffer.

If it is the new data chunk and an out-of-sequence, the agent forwards it to the receiver after marking packet loss by congestion. If it is the new SCTP packet and in order, it copies into buffer and forwards it to the receiver. At that time, if the new SCTP packet is INIT-Chunk or INIT-ACK chunk, Snoop agent could store addresses into buffers after verification address parameters. And Snoop agent stores INITChunk and INIT-ACK chunk into buffers and forwards to MH. In Figure 6, when the SCTP sack chunk is received by base station, if it is the new sack chunk, the agent removes it from the buffer and modifies retransmission timer by measuring RTT to reflect new RTT, while if it is the first duplicate sack chunk, it means packet loss in wireless networks. So, Snoop agent retransmits lost chunks after verification Gap Ack block of SCTP SACK-Chunk and dumps the duplicate sack chunk. However, if it is not the first duplicate sack chunk but the duplicate sack chunk, the agent dumps the duplicate sack chunk.

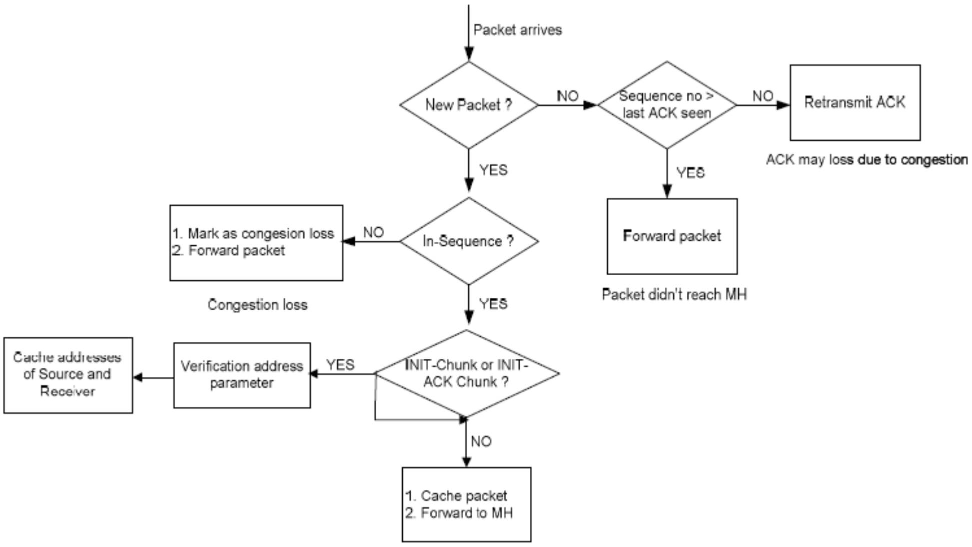
Packet arrives
New Packet ?
NO
Sequence no > last ACK seen
NO
Retransmit ACK
ACK may loss due to congestion
YES
YES
Forward packet
Packet didn't reach MH
1. Mark as congesion loss
2. Forward packet
NO
In-Sequence ?
Congestion loss
YES
Cache addresses of Source and Receiver
Verification address parameter
YES
INIT-Chunk or INIT-ACK Chunk ?
NO
1. Cache packet
2. Forward to MH

Figure 6. Snoop_data()

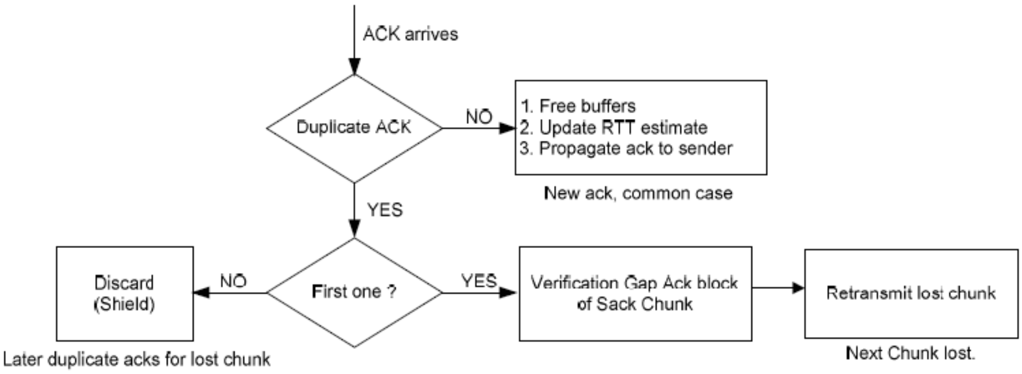

Figure 7. Snoop_ack()

4.3 VLAN Access Control Scheme

VACS (VLAN Access Control Scheme) is defined to control the communication session between the devices in different asymmetric VLAN. This scheme helps to communicate a device as if they are same VLAN on condition that a client has a access right. In addition, the authority levels are decided by network administrator. To begin with doing this, Filtering DB keeps a tuple of Destination MAC, Source MAC, and VLAN ID information for each device.

The function of VACS are described as below

• The Filtering DB sent the rank information set by manager(administrator) decides the authority to access specific devices when extending to asymmetric VLAN (a , b)

• Deny access the network originally. (1 , 2) The first function can solve the problem that original asymmetric VLAN

forward the frames according to Destination MAC, PVID by storing Destination MAC, Source MAC, PVID tuple in filtering DB.

a : Any client, which want to be a member of a different VLAN, requests theright to admission of approach the shared devices.

b : The manager (Administrator) updates the current VLAN information. If an unauthorized client tries to connect A (shared device), switch #2 will not forward the frames to A. There is no information about an unauthorized client in FTDB.

The second function is directly implemented using VACS.

1 : The manager who has monitored VLAN information commands a policy to block a illegal client.

2 : VACS will send blocking frames added client's VID. There are two cases to block a client. One thing is to block the client being already a member of network. The other is to block the client using network in VLAN the access network originally.

VACS automatically collect network information to establish Filtering DB and block illegal host in real time. The collected information about network

resource, such as VLAN ID, MAC address, etc, is sent to manager. The manager system gives a right to communicate a device in different VLAN and a protection to reach an important server using information received from VACS. VACS component applied with dynamic access control schemeThere are three types of VACS component modules. The essential function of VACS is monitoring VLAN frame, VLAN frame creation and Authentication. Also, VACS must be a VLAN-aware device to analysis entire VLAN frame.

Additionally VACS can have ability to block a client regardless of DHCP or Static environment. If unauthorized client try to be a member of network, VACS can protect network resources.

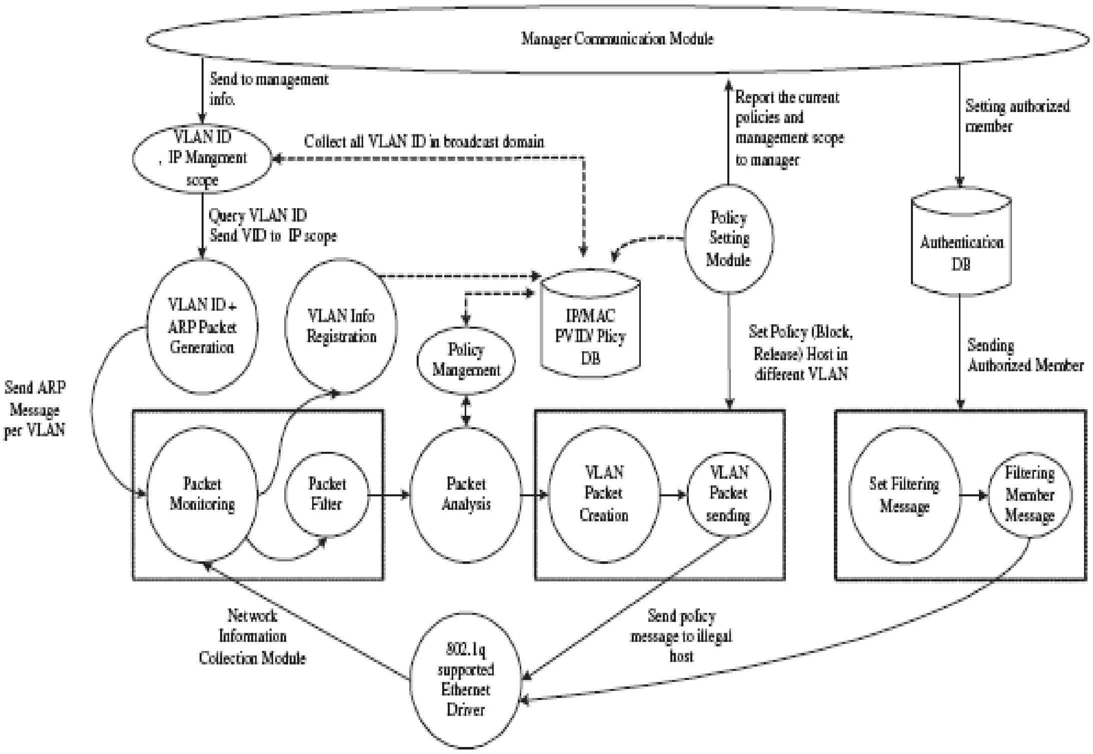
Manager Communication Module
Send to management info.
VLAN ID , IP Mangment scope
Collect all VLAN ID in broadcast domain
Report the current policies and management scope to manager
Setting authorized member
Query VLAN ID
Send VID to IP scope
Policy Setting Module
Authentication DB
VLAN ID + ARP Packet Generation
VLAN Info Registration
IP/MAC PVID/ Plicy DB
Policy Mangement
Set Policy (Block, Release) Host in different VLAN
Sending Authorized Member
Send ARP Message per VLAN
Packet Monitoring
Packet Filter
Packet Analysis
VLAN Packet Creation
VLAN Packet sending
Set Filtering Message
Filtering Member Message
Network Information Collection Module
Send policy message to illegal host
802.1q supported Ethernet Driver

Figure 8. VACS Components

4. Conclusion

MANET and WLAN are based on IEEE 802.11 for MAC layer protocol while they adopt different mode, such as infrastructure and ad-hoc. Flexibility and mobility make wireless LANs both effective extensions and attractive alternatives to wired networks. Wireless LANs provide all the functionality of wired LANs, without the physical constraints of the wire itself. Wireless LAN configurations range from simple peer-to-peer topologies to complex networks offering distributed data connectivity and roaming. Besides offering end-user mobility within a networked environment, wireless LANs enable portable networks, allowing LANs to move with the knowledge workers that use them. It is important to impose strategies to optimize MANET and WLAN.

References

[1] Proxim, Inc - White Paper "What is a Wireless LAN?" http://sss-mag.com/pdf/proximwhatwlan.pdf

[2] T. Sridhar, Flextronics "Wireless LAN Switches — Functions and Deployment" http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-3/wireless_lan_switches.html

[3] Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless Mesh Networking". O'Reilly Wireless Dev Center. http://www.oreillynet.com/pub/a/wireless/2004/01/22/wirelessmesh.html

[4] Wikepedia – MANET http://en.wikipedia.org/wiki/Mobile_ad_hoc_network

[5] What is Vehicular Network? http://blogs.iium.edu.my/jaiz/2008/12/22/what-is-vehicular-network

[6] Wikepedia – Vehicular ad-hoc network http://en.wikipedia.org/wiki/VANET

[7] Wikepedia – Intelligent Vehicular ad-hoc Network

[8] M. Gast, “802.11 Wireless Networks: The Definitive Guide,” O’Reilly, April 2002

[9] T. Clausen, P. Jacquet, “Optimized Link State Routing Protocol (OLSR),” RFC 3626, October 2003

[10] Y. Ge, “Quality-of-Service Routing in Ad-Hoc Networks Using OLSR,” master thesis, December 2002

[11] Wikepedia – Mobile IP http://en.wikipedia.org/wiki/Mobile_IP

[12] Hyewon K. Lee and Youngsong Mun "An Optimized Internetworking Strategy of MANET and WLAN", O. Gervasi et al. (Eds.): ICCSA 2005

[13] Kiwon Hong, Kugsang Jeong, Deokjai Choi, and Choongseon Hong, "A Performance Improvement Scheme of Stream Control Transmission Protocol over Wireless Networks", O. Gervasi et al. (Eds.): ICCSA 2005

[14] Wonwoo Choi, Hyuncheol Kim, Seongjin Ahn, and Jinwook Chung, "Dynamic Access Control Scheme for Service-Based Multi-netted Asymmetric Virtual LAN", O. Gervasi et al. (Eds.): ICCSA 2005