Journal of Southeast University (English Edition) Vol. 20 No. 2 June 2004 ISSN 1003—7985

MAC isolation to realize effective management in public wireless LAN

Chen Liquan[1] Hu Aiqun[1] Ji Wenke[2]

([1] Research Center of Information Security, Southeast University, Nanjing 210096, China)

([2] Motorola Global Software Group, Nanjing 210029, China)

Abstract: This paper describes how to use medium access control (MAC) isolation to enhance management performance in public wireless LAN (PWLAN). To comply with the IEEE 802.11 standards, a scheme to implement MAC isolation in WLAN access points by re-designing the Distribution_Service component of the MAC state machine is proposed. A variable named dot11Isolation is defined to determine whether the MAC level communication between wireless stations in the same BSS is permitted or not. Finally, a design solution based on MPC860 hardware and embedded Linux software for PWLAN access point is specified. The simulation results of MAC isolation for PWLAN show that the proposed scheme is feasible and effective.

Key words: wireless LAN; medium access control (MAC) isolation; access point; embedded Linux

The wireless LAN (WLAN) technology is now widely used and high-speed wireless access is becoming more and more popular in our lives. Through WLANs, we can enjoy flexible high-speed data access with 1 Mbit/s to 11 Mbit/s and even 54 Mbit/s data rates at home, in campuses, enterprises and hot spot areas. However, current WLAN standards do not adequately solve such problems as large-scale area roaming, authentication, privacy and accounting. Thus, public wireless LAN (PWLAN) has been proposed to solve the problems that have emerged in large-scale areas application environment[1]. In PWLAN networks, operation management including roaming administration, authentication and accounting must be improved.

Network operators need to protect the use of their equipments and help to guarantee data communication security for PWLAN end users. Therefore, direct communication between different end users in PWLANs without operators' permission should be forbidden. The medium access control (MAC) isolation function can effectively solve this problem at the layer-2 level. However, up till now there has not been a good way to realize MAC isolation, also called layer-2 isolation function in WLANs. In this paper, we propose a novel scheme in which the Distribution_Service component of the state machine in a WLAN access point is re-designed, and the layer-2 isolation peripheral access devices are adopted to achieve effective management for network operators.

Received 2003-09-13.

Foundation item: The National High Technology Research and Development Program of China (863 Program) (No. 2002AA143010).

Biographies: Chen Liquan (1976—), male, graduate; Hu Aiqun (corresponding author), male, doctor, professor, aqhu@seu.edu.cn.

1 Model and Analysis

PWLAN systems provide high-speed data access services to wireless end users in hot spot areas. Network operators combine WLAN equipments with their existing network facilities to realize PWLAN systems and offer mobile access capability to end users. The architecture of a PWLAN system is shown in Fig. 1. It consists of five parts: the end users' wireless stations (STAs), wireless access points (APs), access controllers (ACs), remote radius authentication servers (ASs), and the peripheral access devices. APs are deployed by network operators, providing air interface to STAs and necessary management for different STAs. ACs manage and control data transmission among different APs, and collect information for accounting. ASs provide authentication, accounting and authorization (AAA) services for all PWLAN end users.

Providing a practical solution to solve AAA problems for PWLAN end users is a major task of PWLAN network system[2,3]. To protect the use of network operators' equipment, end users' transmission information is gathered and the communications are controlled by network operators. It is not allowed to communicate directly between WLAN STAs in one basical service set (BSS) because the use of network operators' AP equipment is not authorized by network operators. Moreover, the operators also cannot gather the transmission information. Thus, they cannot bill these end users. In other words, STAs are only permitted to communicate through ACs to outside network stations by way of PWLAN access parts and

this transmission is controlled by ACs. We construct the following MAC isolation model.

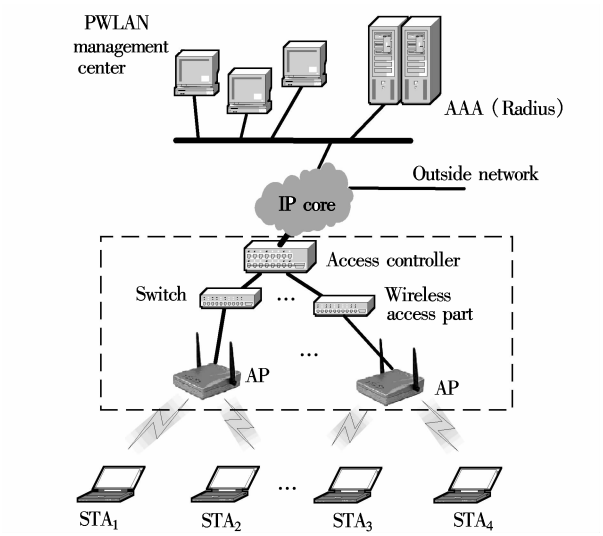

Fig.1 Public wireless LAN architecture

Assume that the capability probability of STA_i (station i) communicating with STA_j is P_{ij}, the capability probability of STA_i communicating with outside network station is P_{iS}, $CON_{isolate}$ is the isolation control switch and $AUTH_i$ is the authorization of STA_i determined by its accounting. For STA_i, Eq.(1) shows that no matter what the value of $AUTH_i$ is, the capability probability for STA_i and STA_j is controlled by $CON_{isolate}$. However, Eq.(2) shows that the capability probability between STA_i and the outside network station is controlled by $AUTH_i$, no matter what $CON_{isolate}$ is. It follows that

$$P_{ij} = \begin{cases} 0 & CON_{isolate} = 1 \\ 1 & CON_{isolate} = 0 \end{cases} \quad (1)$$

$$P_{iS} = \begin{cases} 0 & AUTH_i = 0 \\ 1 & AUTH_i = 1 \end{cases} \quad (2)$$

In the PWLAN model, network operators gather end users' information by ACs. It requires that the MAC isolation function be implemented in APs, peripheral access devices and ACs. With the MAC isolation solution given in this paper, one can isolate end users at the MAC layer level and partly guarantee key applications such as mobile payment and mobile transactions in security. In the wireless access part, different access units adopt different mechanisms to ensure that the whole wireless access system's isolation function is realized as follows.

1) Access controllers (ACs)

ACs are the control ports between the internal part of the PWLAN access network and the outside network. They gather and send users' information to the PWLAN management center. Usually, by setting up an access control lists (ACL), which contains information about each end-user's ID, IP address and the embedded MAC information, ACs can manage end users' communication actions.

2) Peripheral access devices

Peripheral access devices include switches and other relay network devices in the PWLAN access network part. Layer-2 isolation switches and other relay network devices can effect user communication isolation successfully. For example, if one switch has the virtual LAN (VLAN) function, the users' communication would be isolated from different ports in the same switch by activating the related VLAN control feature in this device.

3) Access points (APs)

The IEEE 802.11 standards describe communication actions among wireless end users supported by APs. But the MAC isolation mechanism is not mentioned by these IEEE 802.11 standards. Before describing the MAC isolation solution realized in WLAN APs, we first give a brief description of the **IEEE 802.11 MAC protocol as follows.**

2 MAC Protocol in WLAN

The IEEE 802.11 standards published in 1999 describe the specifications of the MAC layer and the physical layer for WLANs[4,5]. Actually, there are two different mechanisms to control wireless media access: distributed coordination function (DCF) and point coordination function (PCF). The coordination function specifies the mechanism for determining when and which station has the opportunity to transmit or receive data. The IEEE 802.11 standards adopt DCF to be the main coordination function. It uses carrier-sense multiple access/collision avoidance (CSMA/CA) mechanism to control asynchronous data transfer for wireless STAs.

There are eight components in the MAC state machine of the IEEE 802.11 standards to support WLAN MAC layer protocol's implementation. The MAC_Data_Service component processes the MAC service data unit (MSDU) and communicates with link layer; the MAC_Management_Service component manages the working of the MAC protocol in AP and communicates to other components based on a signaling queue mechanism; the Distribution_Service component is the interface between the distribution system (DS) and local MAC; and the MPDU_Generation_AP component processes the segmentation of MSDU and manages relevant data frame processing; the Protocol_Control_AP component is the major part of DCF and PCF procedure processing; the MLME_AP component

generates and processes the management data frame; the transmission module transmits data from MAC layer to physical layer; and the reception module receives data from physical layer. Moreover, the whole WLAN AP system includes not only the above eight components but also their interfaces with link layer named MAC_SAP, with station management entity named SM_MLME_SAP, with DS named DSM_SAP and with physical layer transmission and receive module named PHY_SAP_Tx and PHY_SAP_**Rx.**

3 MAC Isolation in AP

In WLANs, the MAC protocol communicates with the wired network through the Distribution_Service component. The Distribution_Service component has interfaces with DSM_SAP, MAC_Data_Service and MPDU_Generation_AP components to communicate with the DS interface, the local link layer interface and the physical layer interface. The state diagram of the Distribution_Service component is specified in Fig.2.

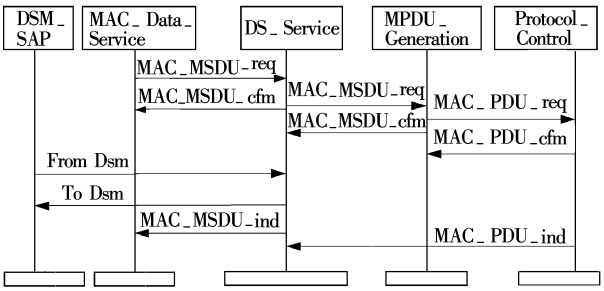

Fig.2 State diagram of Distribution_Service component

There are four bi-directional data paths available in the Distribution_Service component:

1) DS interface to and from physical layer interface;

2) DS interface to and from link layer interface;

3) Link layer to and from physical layer interface;

4) Wireless physical layer to and from wireless physical layer within the same BSS.

To realize the MAC isolation function, we first define a Boolean variable in management information base (MIB) database of AP named dot11Isolation. Whether the end user is isolated or not is controlled by the value of this variable. When dot11Isolation is set to true, the wireless STAs' communication within the same BSS from one to the other wireless STAs through APs is isolated in the MAC level. When the variable is set to false, it complies with the IEEE 802.11 standards and permits direct communication among different wireless STAs within the same BSS. The design flowchart of MAC isolation in APs is shown in Fig.3.

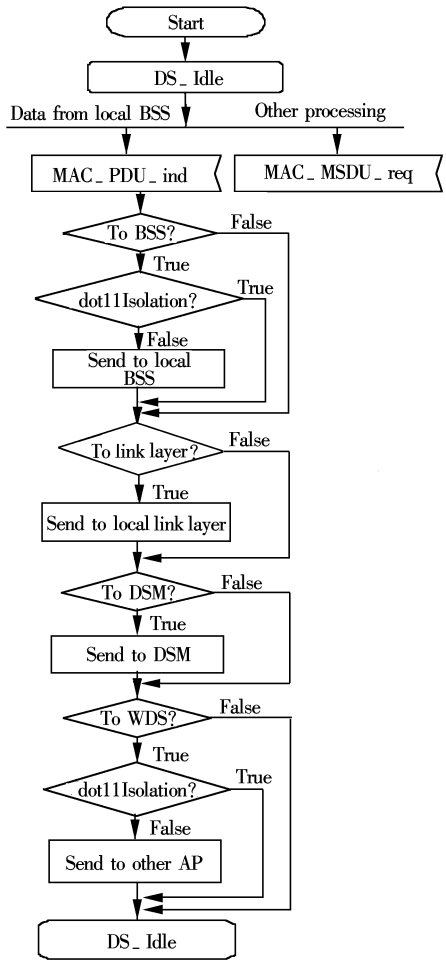

Fig.3 Re-designed flowchart of Distribution_Service

At first, the Distribution_Service is in "DS_Idle" state. It transfers to different states and performs different actions based on different received signals. When the Distribution_Service component receives "MAC_PDU_ind" primitive signal, it first checks the data path. When data is sent to the local link layer and the DSM entity, it will conduct relevant processing complied with the IEEE 802.11 standards. If the destination of data is within the same BSS, it will check the dot11Isolation's value firstly. The data might be forwarded to the destination when dot11Isolation is set to false in order to comply with the IEEE 802.11 standards. Otherwise, the data will be isolated within the same BSS for preventing direct communication between two wireless users. At the same time, when there is a data packet from "MAC_PDU_ind" asking to reach another AP through the wireless distribution system (WDS) mechanism, the value of dot11Isolation will also be checked before the data is transmitted.

Based on this solution, compliance with the IEEE 802.11 standards is guaranteed and realization of MAC isolation function is solved. When the value of

dot11Isolation is set through a simple network management protocol (SNMP) remotely, the isolation management in PWLANs can be effectively done at operators' network management center.

4 AP Implementation and Simulation

In the implementation, we select MPC860 from Motorola Inc and physical layer chipsets from Intersil Inc to be the WLAN AP hardware solution[6] as illustrated in Fig.4. From antenna to RF & IF and then to the baseband processor, the wireless-channel signal is demodulated to base band data and then is sent to the MAC processing chipset. The MAC chipset's major function is to transmit or receive data to or from baseband processor and to control the running at the physical layer such as power control and frequency selection through the auto gain control (AGC) mechanism. The memory management unit (MMU) in MPC860 chipset supports external chip memory equipments, including 4M × 8 bits FLASH and 4M × 16 bits SDRAM. MPC860 also provides integrated interface for Ethernet to construct wired network port and for serial communication controller (SCC) units to control the WLAN physical layer chipset HFA3863.

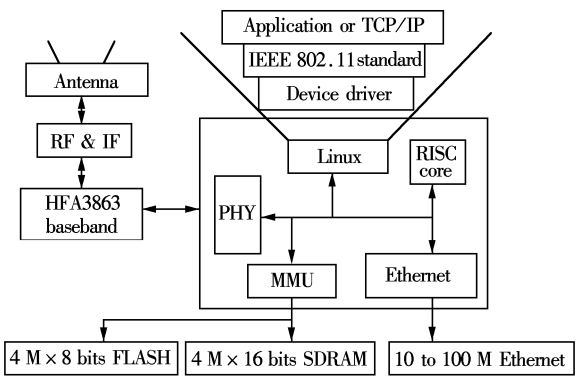

Fig.4 Architecture and software design of wireless AP

In software, we use an embedded Linux operating system as the software platform for the IEEE 802.11 MAC implementation[7]. The refined embedded Linux kernel is firstly ported to MPC860[8], and then, the software drivers for wireless PHY I/O, Ethernet and the serial communication unit are embedded in the Linux kernel, too. These drivers are the base components for implementing the IEEE 802.11 MAC protocol, TCP/IP stack and the application software. Based on these hardware and software platforms, we can construct the WLAN AP MAC protocol which realizes the MAC isolation function.

Finally, we construct the simulation scenario as shown in Fig.5. In this scenario, two WLAN stations communicate with the far-side wired server through

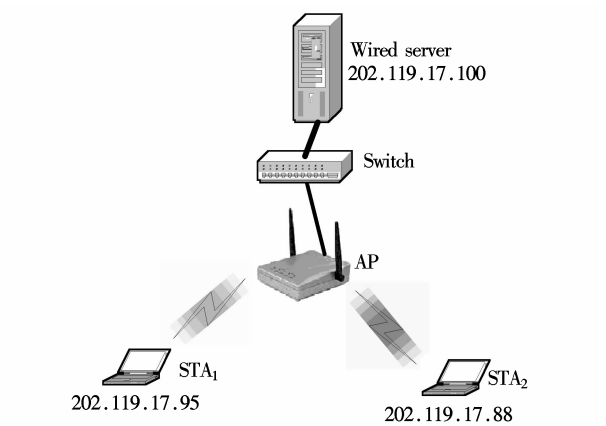

Fig.5 Simulation scenario

one AP and one switch. Assume that STA_1 has IP address 202.119.17.95 and the IP address of STA_2 is 202.119.17.88. The IP address of the wired server is 202. 119. 17. 100. The AP used in this place is constructed based on MPC860 hardware and embedded Linux software and involves MAC isolation capability, the switch used in this simulation study also has the MAC isolation capability. Data communication among STA_1, STA_2 and the wired server is simulated. The simple Ping action and ftp applications were also simulated. Simulation results are shown in Tab.1 and Fig.6.

Tab.1 Ping simulation results

Item	STA_1	STA_2	Wired server
STA_1		No reply	Reply
STA_2	No reply		Reply
Wired server	Reply	Reply	

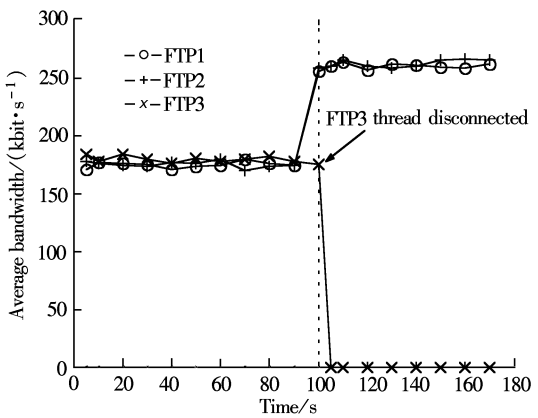

Fig.6 Ftp simulation results for MAC isolation

In Tab.1, assume that STA_1 triggers Ping action with STA_2, we can find out that the data do not reach STA_2 as this AP involved MAC isolation function has isolated the communication between these two stations. On the other side, the Ping action between STA_1 and the wired server and the Ping action between STA_2 and the wired server are not affected by the MAC isolation function implemented at this AP.

In Fig.5, we construct one ftp agent in the wired server and one in STA_2, then download data from these two agents at STA_1 and STA_2. We get three ftp threads: FTP1 is the ftp thread between STA_1 and wired server; FTP2 is the ftp thread between STA_2 and wired server; and FTP3 is the ftp thread between STA_1 and STA_2. Before 100 s, the MAC isolation function is not set on, we can see that these three ftp threads run successfully as shown in Fig. 6, and the average bandwidth of each ftp is about the same (175 kbit/s). On the 100th second, the MAC isolation function in that AP is switched on. We can find out that the average bandwidth of the FTP3 ftp thread is fast reduced to 0 kbit/s, while the average bandwidths of FTP1 and FTP2 ftp threads are increased to about 260 kbit/s. This means that the isolation function between STA_1 and STA_2 is realized.

5 Conclusion

The WLAN technology provides a more convenient way for end users to access wireless networks. At the same time, network operators need to solve the MAC isolation problem in order to provide high quality services to end users and to achieve effective management. The solution proposed in this paper presents an effective method to realize MAC isolation in PWLAN and is compliant with the IEEE 802.11 standards. Adopted with this isolation solution, network operators can construct an operator wireless access network and control end-user communication action effectively.

References

[1] Ala-Laurila J, Mikkonen J, Rinnemaa J. Wireless LAN access network architecture for mobile operators [J]. *IEEE Communications Magazine*, **2001, 39**(11): 82－89.

[2] Prasad A R, Moelard H, Kruys J. Security architecture for wireless LANs: corporate and public environment [A]. In: *Proc Vehicular Technology Conf* [C]. Tokyo, 2000(1): 15－18.

[3] Shen P, Cao X Y. The solution of AAA function in open RAN [J]. *Journal of China Institute of Communication*, **2003, 24**(3): 91－97. (in Chinese)

[4] IEEE. Std802.11 Part11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications [S]. America: the IEEE Inc, 1999.

[5] IEEE. Std802.11b Part11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications: higher-speed physical layer extension in the 2.4 GHz Band [S]. America: the IEEE Inc, 1999.

[6] Motorola. MPC860 PowerQUICC user's manual [EB/OL]. http://e-www.motorola.com/files/netcomm/doc/ref_manual/MPC860UM.pdf. 2003-03-31/2003-07-21.

[7] Wang W, Pang Z H, Liu N A. The realization of access point based on embedded Linux system [J]. *Aviation Computer Technology*, **2001, 31**(4): 24－27. (in Chinese)

[8] Cha Hyun-Joon. Design and implementation of embedded Linux system for networking devices [EB/OL].http://dpnm.postech.ac.kr/thesis/00/tachyon/. 2001/2003-08-06.

PWLAN 中实现有效管理的 MAC 层隔离方法

陈立全[1]　胡爱群[1]　计文柯[2]

([1] 东南大学信息安全研究中心, 南京 210096)
([2] Motorola 全球软件集团, 南京 210029)

摘要: 分析了在公共无线局域网(PWLAN)系统中为实现对用户统一有效管理而要求应用的二层隔离技术, 同时提出通过在无线接入点(AP)的媒体接入控制(MAC)层中定义一个隔离参量 dot11Isolation, 并修改 MAC 层协议中 Distribution_Service 模块的运行状态图以实现二层隔离的一种方法. 同时, 介绍了一个基于 MPC860 处理器并以嵌入式 Linux 操作系统为平台来实现二层隔离功能的 WLAN AP 设备实现方案. 仿真结果表明, 本文提出的二层隔离实现方法是有效可行的.

关键词: 无线局域网; MAC 层隔离; 接入点; 嵌入式 Linux

中图分类号: TN915