INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT
Int. J. Network Mgmt 2004; **14**: 305–313 (DOI: 10.1002/nem.526)

AAA architecture for Mobile IPv6 based on WLAN

By R. C. Wang, R. Y. Chen, and Han-Chieh Chao[*][†]

Mobility support for Internet devices is quite important for consumer electronics. The number of the hand-held devices is growing quickly. However, there are not enough IP addresses for the number of the rapidly growing devices in the All-IP generation. Internet Protocol version 6 (IPv6) was therefore adopted to solve these problems. Our purposed structure is based on IEEE 802.11. However, IEEE 802.11 has a serious security drawback. Further, from the Internet Service Providers' point of view, accounting is a potential problem. A mechanism combining Mobile IPv6 and AAA based on IEEE 802.11 to overcome these problems is essential.

Both Internet Protocol version 4 (IPv4) and IPv6 support IP security (IPsec) when data packets are exchanged across the IP network. IPsec operates at the IP layer. It can support system authentication and authorization, However, it lacks a system accounting function. Therefore ISPs cannot establish correct billing for their services. This is the reason why we chose to combine the wireless network and AAA functions.

In this paper, the AAA mechanism is used to protect security, with the architecture having authentication, authorization, and accounting functions. We will discuss the benefits of AAA and state the reason why we choose to combine AAA with the mobility architecture. Copyright © 2004 John Wiley & Sons, Ltd.

Reen-Cheng Wang received his BS degree in Computer Science from the National Tsing-Hwa University, Taiwan, in 1996, MS degree in Computer Science and Information Engineering from the National Dong-Hwa University, Taiwan, in 1998. At present, he is a PhD student in the department of Computer Science and Information Engineering, National Dong-Hwa University. Also, he is the manager of R&D division in the Computer and IT Center of National Dong-Hwa University. His major research interests include network protocols, network management, and mobility network.

Rui-Yi Chen, got his Master degree from the department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan, July 2003. Now he is serving as an Engineer of the notebook hardware R&D department at Wistron corporation.

Han-Chieh Chao is a Full Professor and Chair of the Department of Electrical Engineering. He is also serving as the director of the University Computer & IT Center at National Dong Hwa University, Hualien, Taiwan, R.O.C. His research interests include High Speed Networks, Wireless Networks and IPv6 based Networks and Applications. He received his MS and Ph.D. degrees in Electrical Engineering from Purdue University in 1989 and 1993 respectively. He has authored or co-authored 3 books and has published about 110 refereed professional research papers. He has completed 23 MSEE theses students. Dr. Chao has received many research awards, including Purdue University SRC awards, and NSC research awards (National Science Council of Taiwan). He also received many funded research grants from NSC, Ministry of Education (MOE), Industrial Technology of Research Institute, Institute of Information Industry, Chunghwa Telecommunications Lab and FarEasTone Telecommunications Lab. Dr. Chao has been invited frequently to give talks at national and international conferences and research organizations. Dr. Chao is also serving as an IPv6 Steering Committee member and Deputy Director of R&D division of the NICI (National Information and Communication Initiative, a ministry level government agency which aims to integrate domestic IT and Telecom projects of Taiwan), Co-chair of the Technical Area for IPv6 Forum Taiwan, and the executive editor of the Journal of Internet Technology.

[*]Correspondence to: Han-Chieh Chao, Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan, Republic of China
[†]E-mail: hcc@mail.ndhu.edu.tw

Published online 9 July 2004

Introduction

LAN products in the market pose several problems that need to be solved. The popularity of IEEE 802.11 WLAN has prompted the development of innumerable wireless devices. A lack of security and inflexible authentication for large-scale deployment is the first problem. Second, an explosion in the amount of roaming has fuelled an increase in demand for IP mobility. Mobility support for Internet devices is quite important for consumer electronics and Internet appliances (IA). The number of the handheld devices is increasing. Hence, Mobile IP should be rapidly deployed in the WLAN environment.

This is based on IEEE 802.11. However, IEEE 802.11 has a drawback in its security. The AAA architecture is required for Internet Service Providers, because mobile users should be identified when entering the network or during roaming, especially, when mobile users roam across different administrative domains. From the Internet Service Providers' point of view, accounting is an even more important problem. Therefore, we combined Mobile IPv6 and AAA (Authentication, Authorization, and Accounting) based on IEEE 802.11 to overcome these problems.

Both Internet Protocol versions 4 (IPv4) and 6 (IPv6) are supported by IP security (IPsec) when data packets are exchanged across the IP network. IPsec operates at the IP layer. In a masterclient system, the master system can authenticate the client's identity. If clients pass the authentication the master node will then authorize access to services. IPsec can therefore support system authentication and authorization. However, the system lacks an accounting function.

The Wireless Local Area Network (WLAN) will become more important, useful, and generally adopted in the near future.

Wireless Local Area Network

The Wireless Local Area Network (WLAN) will become more important, useful, and generally adopted in the near future. In a wireless network, portable computers can connect to each other over infrared or wireless within a small area environment. The medium in a wireless network is a shared resource and the frequency is an unlicensed frequency band. For example, IEEE 802.11b is carried over the 2.4 GHz band.

—IEEE 802.11 Overview—

IEEE 802.11 is defined by the Institute of Electrical and Electronics Engineers, Inc. It defines the Physical (PHY) and Medium Access layers (MAC) for wireless Local Area Networks (LANs).

The main characteristics of IEEE 802.11 Wireless LAN are as follows:[1]

- Multi-transport rate: The stations work at different transport rates in the communications network. For example: 0.5 Mbps; 1 Mbps; or 2 Mbps. IEEE 802.11a can promote up to 54 Mbps. IEEE 802.11b can promote up to 11 Mbps. And IEEE 802.11g can promote up to 54Mbps.
- The basic communications protocol is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). IEEE 802.11 uses this protocol, CSMA/CA, to avoid collisions, however, this protocol cannot avoid all frames without collisions. Therefore, it is not suitable for use in transporting real-time information.
- Support two transport services: the Distributed Coordination Function (DCF) uses CSMA/CA to transport non-real-time information and support asynchronous data transfer on a best effort basis. The Point Coordination Function (PCF) is a polling-based protocol. It is designed to support collision free and real-time services.
- In DCF, the stations use CSMA/CA to avoid collisions. The polling protocol is not used, so each station cannot be guaranteed a fair bandwidth share.
- Support the authentication and data—privacy functionality. Radio frequency transport is carried over an open medium and any data sent could be intercepted and/or interfered with by anyone. Privacy must be ensured using encryption and decryption

technology to protect the transmitted information.

- Radio frequency transport is not suitable for multimedia services. Although the network can use a polling-based protocol, the bandwidth will be greatly decreased by the increasing number of users. More stations accessing the Internet at the same time will reduce the bandwidth allotted to each station.

—IEEE 802.11 Architecture—

The IEEE 802.11 architecture is composed of cells. The basic service set (BSS) represents the coverage area of an individual cell. There are two different types of BSS providing two different wireless architectures: the infrastructure BSS and the individual BSS (IBSS) or ad-hoc network.

The BSS infrastructure is composed of a central station called an Access Point (AP) and a variable number of mobile stations. The AP acts like a base station in other cellular networks. It acts as a bridge between the wireless and wired network segments. This architecture allows the interconnection of several infrastructure BSS to form what is known as an extended service set (ESS), see Figure 1. The ESS is built by connecting several APs through a backbone network called a Distribution System (DS). The area covered is defined by the AP in the network infrastructure. In an ad-hoc network, the coverage area is composed of the overlapping coverage areas of each station.

An individual BSS or ad-hoc network (Figure 2) is composed of a single cell without an AP. In such a network, there is no central point to manage network communications and connect with the other networks. Stations can communicate with each other inside the BSS.

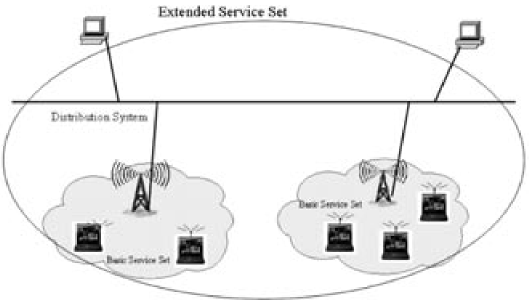

Figure 1. Extended Service Set (ESS)

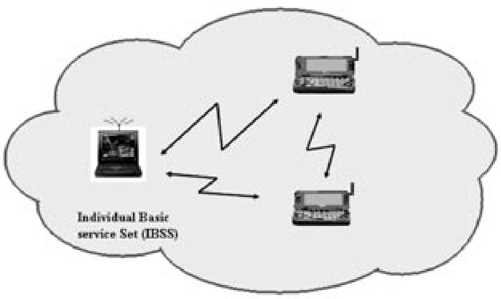

Figure 2. Ad-hoc network

—IEEE 802.11 Security—

There are two authentication services: open system and shared key. The open system is the simplest way for authentication. Open system authentication includes two steps. In the first step, the authentication requester sends the authentication frame that includes the identity assertion. In the second step the receiver replies to the authentication frame. In the shared key authentication system it is assumed that all of the members of a station group have the same shared key. When a member is challenged, a true member will reply with the correct shared key. The shared key is protected by the Wired Equivalent Privacy (WEP) encryption mechanism. There are four steps in shared key authentication.

Mobile IP

There are three elements in Mobile IPv6, the Mobile Node (MN), Home Agent (HA) and Correspondent Node (CN). There is no Foreign Agent (FA) in this architecture. In Mobile IPv6, the FA rule is replaced by a router. When the MN is in a foreign site, the MN will get a care-of-address (COA) derived from the router advertisements, stateless address auto-configuration, or assigned by the DHCP server, stateful address auto-configuration.[2–5]