Автоматизированные системы. Термины и определения" (утв. постановлением Госстандарта СССР от 27 декабря 1990 г. N 3399).

3. Аванесов В.С. «Форма тестовых заданий». Учебное пособие для учителей школ, лицеев, преподавателей вузов и колледжей. 2изд., переработанное и расширенное. М.: «Центр тестирования», 2005.-156с.

4. Доррер, А.Г. Моделирование и разработка интерактивных обучающих систем с адаптацией: диссертация ... кандидата технических наук: 05.13.01, 61 06-5/972.

Резюме

В статье рассматривается информационная модель адаптивной системы для интерактивного обучения программирования, ее структура.

Resume

The article describes the information model of an adaptive system for interactive learning software.

UDK 004.7

WIRELESS TECHNOLOGY AND SECURITY

М. Балык
Университет им. Сулеймана Демиреля, г. Алматы

Overview

This chapter provides an overview of current wireless technologies and security schemes that are part of the IEEE 802.11 standard.

Because this research focuses on the potential effects of enhanced wireless security on network performance readers should be familiar with various topics including the physical layer of IEEE 802.11, how authentication and encryption work on a secured wireless network, and how to observe these processes on the network.

This chapter begins with an in-depth look at the IEEE 802.11 protocol in order to note differences between an unsecured wireless network versus one that is protected by various layers of encryption and authentication. The chapter then provides a brief overview of the IEEE 802.1 1b and 802.1 1g standards. Finally, the chapter finishes with a complete overview of various encryption and authentication methods that are present on secured wireless networks and how they play into the IEEE 802.1 1i standard.

The vast majority of the IEEE 802.11 background was drawn from [1] and the majority of all security background information was drawn from, and [2].

Together these texts provided virtually every piece of information presented in this chapter.

IEEE 802.11 Standard

IEEE 802.11 was the first widely-used wireless local area networking standard and was selected for use in 1997. The standard consists of a medium access control (MAC) sublayer, MAC management protocols and services, and three physical layers (PHYs). The three PHYs were an infrared PHY, a frequency hopping spread spectrum (FHSS) radio PHY, and a direct sequence spread spectrum (DSSS) radio PHY. These original PHYs provided data transfer rates of 1 Mbps and 2 Mbps [1].

The 1999 revision included two more PHYs, IEEE 802.1 1a and 802.1 1b, which would become standards in the industry with data transfer rates of 54 Mbps and 11 Mbps, respectively. The difference between the two new PHYs was that IEEE 802.1 1a operated with an orthogonal frequency division multiplexing (OFDM) signal at Unlicensed National Information Infrastructure (U-NII) bands verses the DSSS signal used at 2.4 GHz for IEEE 802.1 1b. In 2002 the widely used IEEE 802.1 1g standard was developed as an extension of IEEE 802.1 1b, providing backwards compatibility [1].

MAC Layer

The MAC sublayer provides reliable data transmission for the IEEE 802.11 standard similar to a wired network. To this extent, the MAC sublayer provides three functions: a reliable method to transmit data for users, shared access to the medium among users, and the protection of transmitted data accomplished through encryption.

Because the transmission of IEEE 802.11 signals occurs wirelessly these functions must be conducted differently in the MAC sublayer because signals that are transmitted cannot simply be assumed to have been received on a wireless system.

Reliable Data Delivery

The first function, reliable delivery, is completed with a series of two frames, as shown in Figure 2.1. One is sent by the wireless client to the access point and the second is an acknowledgement frame sent from the access point to the client indicating that the frame was received. If there was no acknowledgement frame received at the client then that station can assume the access point did not receive the first frame and the client can retransmit it after a certain wait time.

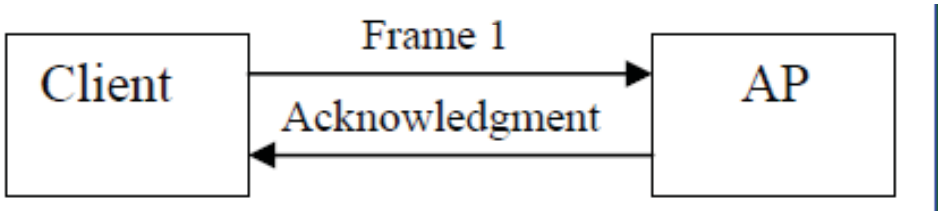

Figure 2-1. 802.11 Delivery

There is a conflict with this process that is often referred to as the “hidden node problem” [2]. The problem occurs when one client is not in a position where it can communicate direct with another client but both clients are in a position to communicate

with a common station. One station may not know that another station is transmitting and, therefore, causes a collision by transmitting a frame of its own.

To address this problem the protocol provides an optional solution with two additional frames called the request-to-send (RTS) and the clear-to-send (CTS) frames. Before a client transmits it first sends a RTS indicating its intention to send a frame; however, it will not transmit information until it receives a CTS from the destination. Because the use of these two additional frames can reduce the data throughput rate of the network it is not enabled in all situations [2].

Shared Access

The second task of ensuring shared access to all clients is accomplished through two access mechanisms: the basic access mechanism which utilizes the distributed coordination function (DCF) and the centrally controlled access mechanism which utilizes the point coordination function (PCF).

The basic access mechanism of IEEE 802.11 utilizes carrier sense multiple access with collision avoidance (CSMA/CA) and binary exponential backoff. This access mechanism uses a “listen before you talk” approach and ensures that if the destination is already handling traffic another client will not attempt to transmit as well, avoiding a collision. If a client detects another transmission in progress it will wait a set amount of time, called the contention window (CW), before it attempts its own transmission. This value increases each time that a client detects a transmission in progress to increase the chance that the medium is available for the next transmission. This value is standard for each PHY [1].

The DCF, which is the functional unit of the basic access mechanism, operates by checking both the physical and virtual carrier sensing mechanisms. In the event both of these mechanisms indicate that there is no transmission for a set period, based on timing intervals, then the MAC may begin a transmission. These timing intervals provide a station with a set time to wait before beginning transmission in order to help prevent collisions [1].

The PHY determines two intervals: the short interframe space (SIFS) and the slot time. From these, three additional intervals are derived: the priority interframe space (PIFS), the distributed interframe space (DIFS), and the extended interframe space (EIFS). Each of these timing intervals changes depending on the number of times that a transmission is detected while a station is attempting to transmit [1]. Timing intervals are illustrated in Figure 2-2.

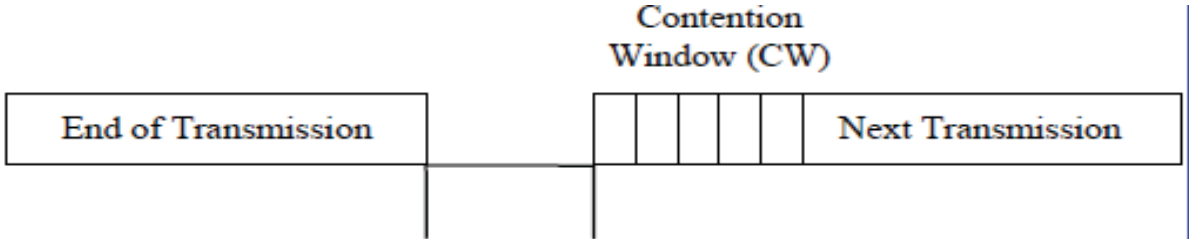

Figure 2-2. 802.11 Timing Intervals

The centrally controlled access mechanism, which utilizes the PCF, uses a poll and response protocol for the medium. This is an optional protocol that is housed within the access point and operates over the DCF, providing another method of preventing collisions . It operates by requiring stations to be added to a polling list within the access point providing traffic information to the stations [1].

REFERENCES (INTERNET)

1. O'Hara, Bob & Petrick, Al. *IEEE 802.11 Handbook: A Designer's Companion (2nd ed.).* IEEE Press, New York, NY, 2005.

2. *CWNA – Certified Wireless Network Administrator (3rd ed.).* McGraw-Hill/Osbourne, Emeryville, CA, 2005.

Түйіндеме

Қазіргі таңда WLAN корпоративтік жүйінде маңызды рөл атқарады. Ол үйдегі жүйеде қолданылатын белгілі бір топтама болды. WiFi-дың қолданылуының көбенгені сонша, хакер, ұрылар қауіпсіздк жүйесіне оңай зиян келтіре алады. Сондықтан қазіргі уақытта программистер қауіпсіздін жүйесін дамытуда.

Резюме

В настоящее время WLAN играет очень важную роль в корпоративных сетевых средах. Она стала очень известной для приложений домашней сети. Беспроводной доступ настолько возрос, что хакеры и воры могут легко злоупотреблять системой безопасности, поэтому методы более высоких уровеней безопасности, таких как продвинутые алгоритмы шифрования и аутентификации эффективных процессов решаются все больше и больше.