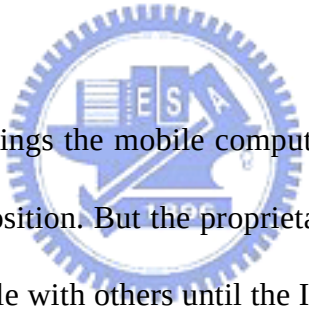
Chapter 1

Introduction



The wireless LAN brings the mobile computing come true. People do not need to be restricted in fixed position. But the proprietary wireless infrastructure could be expensive and incompatible with others until the IEEE 802.11 [1] standard published in 1997. Since the IEEE 802.11 standardized, the technology of wireless LAN is processing rapidly, such as the hardware cost down and bandwidth quickly increased from 2 Mbps to 11 Mbps and recent 54 Mbps [2]. In just a few years, there have been millions wireless devices running around the worldwide.

The wireless network has several advantages over wired network as follows.

1. Device mobility: Under the radio coverage, users can access data or network while they are moving. Even they come to the room from another, they don't

need to reconnect and setup again for joining the wireless LAN.

2. Low cost and time saving: Wireless LAN gets rid of the traditional wire layout, it saves a lot time and cost to design the path and pull cables. In other hand, this speeds the network deployment.
3. Flexibility: No wired line means you can easily add stations to the network without any cable pulling. In case of following the business growth, the company can expand the internal network LAN more quickly and easily.

The wireless takes advantage of its superior and nature medium that already exists everywhere. But it is possible that wireless security could suffer from this unbounded medium. In traditional wired-network, each node is connected physically with the wire, thus it makes the attacker more difficult to intercept the messages unless they tap the wire. But in wireless LANs, user can access the network under the radio coverage everywhere, that means the unauthorized party, person or organization, can also access the network.

The IEEE 802.11 standard for wireless LANs uses "wired equivalent privacy (WEP) protocol" and "group-shared static key" for network security. Unfortunately, the WEP key had been completely broken in late 2001 [3]. Furthermore, anyone now can freely download the WEP cracking program with source code [4] from the Internet. That program just takes between 1,000,000 ~

5,000,000 packets to succeed the WEP cracking. The "group-shared static key" shows that the standard is lacking of the key management mechanism. The current manual key management makes the secret key not really secret enough. As a result of security holes, it leaves people a lot of security concerns and prevents most companies from using the wireless LAN widely.

To address the security problem, the IEEE 802.11 TGi [5] prepares a new specification 802.11i [6] to overcome all of the possible weakness, but this specification is still in a draft state.

In order to support widely existing equipments, the IEEE 802.1x [7] standard has quickly become the important demand before the 802.11i standardized. The IEEE 802.1x provides better access control in the authentication and optional key management mechanisms. In the other hand, it offers the fundamental aspects of the business model, access control and billing. But the IEEE 802.1x requires additional authentication server, it is inconvenient for the small or medium network deployment.

In the meantime, many other suggestions for wireless security have been proposed. In [8], Wool proposes a lightweight key management to solve station revocation and WEP weakness with key refresh mechanism. In his approach, the access point (AP) and stations exchange the WEP group keys at the authentication state. Then, the station has to re-authenticate whenever it needs a fresh key. Narendar

et al. [9] use the DHCP protocol with additional option to provide a transport mechanism for wireless key management. When a station joins the network, it receives an IP address and the current and the next WEP key. The station renews its IP address and WEP key depending on the DHCP lease time. A simple key distribution method proposed by Gunter et al. [10], they apply key management server (KMS) and SNMP protocol for key management. The station receives key distribution frame from KMS and decrypts the frame with its individual key. In the AP side, it sets the WEP default key via SNMP protocol.

Note that the above approaches do not replace the native WEP and RC4 [11]. This is because they believe the fact that the attacker needs to collect several million packets to decrypt the WEP key. Thus, they change the WEP key frequently to defend the collecting. But their methods depend on the additional hardware or software and increase the installation cost. In addition, all these methods distribute the key- distribution frames frequently. This is not efficient and increases the risk.

In this thesis, we consider the wireless security problem and propose a simple key management, called Round-Robin key management (RRKM), for the WEP key distribution. The method updates the WEP key within a specific period, but it does not need any periodic key-distribution frame to distribute the new key. In our method, the AP and stations can generate a fresh WEP group key periodically and synchronously. Thus the RRKM gives a better security and efficiency. Moreover, the

RRKM only requires very small extra-resource, because it inherits the conventional WEP and RC4 of IEEE 802.11 and uses a simple hash function as the key generator. These characteristics are important to the compatibility with current IEEE 802.11 infrastructure and devices.

In the next chapter, we will introduce the IEEE 802.1x and its subtype EAP-TLS. Then we describe our designed issues and the RRKM method in Chapter 3. In Chapter 4, we compare the performance of RRKM to that of IEEE 802.11 and 802.1x in Chapter 4. Finally, a summary is given in Chapter 5.