Abstract

During last several decades' mobile communication has aimed a dramatically development, and brought remarkable change of people's life. Mobile communication offer wireless connectivity that enables mobility and computing in dynamic communication environments.

The market demands driving the mobile communication technology development fast ever. Numbers of communication systems have been developed and numerous service providers and equipment vendors entered this market. Therefore many new advance techniques have been introduced into it which gives subscriber a larger bandwidth, more powerful processing capability, and advances in computing technology.

The rapid growth of mobile and wireless communication technology not only brought convenience to people's ordinary life, but also brought high risk of security issue. From subscriber to network operator, even mobility feature can have serious security problems.

On the other hand, pattern recognition maintains a good development and has already been applied in our daily life; hand writing is one of the most important applications which already been used in a lot of mobile device such as: mobile phone, PDA, and lap-top.

In this thesis, we address the mobile communication security issue in authentication and access control. We will proposal a possible combination of hand writing and hand drawing pattern recognition with modem mobile communication system such as GSM and Wireless LAN to improve the security capability to protect the system from security attack such as dictionary attack.

Preface

This thesis is submitted in partial fulfillment of the requirements for the Master of Science at Agder University, Faculty of Engineering and Science. This thesis was carried out under the supervision of Professor Vladimir A.Oleshchuk.

First of all I like to thanks my supervisor Vladimir A.Oleshchuk for his first class guidance throughout the project period. His insight and analytical skill has been greatly appreciated in numerous interesting discussions regarding the problem area targeted in this thesis. And his profound knowledge in computer security science inspired me and brought a lot of new ideas in this project.
I also wish to thanks Stern Bergsmark for his advice regarding thesis writing.

Grimstad, May 2008

Yuan Jun

Content

Chapter 1 Introduction

After Guglielmo Marconi successfully sending a wireless signals from his father's country estate at Pontecchio in 1895, wireless technology has made a dramatically development during the last 100 years. And especially after the Second World War, as the wireless techniques been wildly applied, mobile communication drove a remarkable change of people's life.

Nowadays, mobile communication device have been used in every part of our daily life, such as mobile phone, lap-top, PDA and all kind of blue tooth communication. It brought convenience to people's life, underneath hype and publication, the service provider only show advantages to the public. And usually the security problem has been ignored by its subscriber.

Although there already implemented security protection for present mobile communication system, but since the radio wave is the medium that can be accessed by any one, this is obviously a security threaten for the subscriber's communication.

The modem mobile is mainly structured by GSM (Global System for Mobile communication), as known as 2G and UMTS (Universal Mobile Telecommunication System), as know as 3G. These two communication system's security protection was thought to be strong and secure; however, the mobile communication technology has keeping a highly develop speed in last several decades, and the algorithm we were thought secure is not secure any more.

Initially, the GSM system was designed with a moderate level of security. It was designed to authenticate the subscriber using a pre-shared key and challenge-response. Therefore in GSM system, user authenticated to the network. This makes this security model offers confidentiality and authentication, but limited authorization capabilities, and no non-repudiation.

The algorithms that been used in GSM system are algorithm A3 is used for authentication, A5/1 and A5/2 for encryption, A8 for the generation of a cipher key. These two algorithms are stream ciphers which are used to ensuring over-the-air voice privacy. They were thought secure for a while, but the flaw has been discovered soon. Compare with A5/1, A5/2 is weaker, and it is possible to be broken with a cipher-text-only attack. And not long ago, some organization found that A5/1 is also easy to be broken with a rainbow table attack [1].

Besides cellular system, there is also WLAN (Wireless Local Area Network), which has already been widely used but has really serious problem. At the very beginning, when WLAN communication standard been published, WEP was

used as WLAN security core. But soon its insecure properties have been discovered one by one. And recently, you can easily find any free software that can break the WLAN communication in a short time.

For the communication security, there are many methods has been designed and implemented. In this thesis we will consider hand writing pattern recognition technology combine with current mobile communication system which can provide a secure mutual authentication mechanism for mobile communication security, and used to strengthen authentication security in today's mobile communication system.

In contrast with the current mobile communication system, our approach will consider as an effective way for current system's improvement. We will also show the data we collect from the experiment, which can show the efficient improvement for the mobile communication systems we are using.

1.1 Thesis definition

The final thesis definition is formulated as follow:

The students will approach the problem of mobile communication security which is mainly focus on authentication and cipher keys generation. The current hand writing pattern recognition technique will be introduced into the mobile communication system as a main method to solve the mobile communication security problem, especially in Wireless Local Area Network (WLAN). Furthermore, the performance will be evaluated to prove the improvement of

mobile communication security.

1.2 Report outline

This thesis is outlining as follow:

Chapter 1 is introduction of current chapter;

Chapter 2 simply introduces the cellular system's security mechanism and its flaw; besides, the wireless local area network's security mechanism is also introduced and the security flaws will be identified.

Chapter 3 the theory of pattern recognition and hand writing techniques; we will introduce two main way of pattern recognition and classification which are naïve bayes classifier and Hidden markov mode (HMM). The hand writing technique introduction will follow next.

Chapter 4 is introducing approach of using pattern recognition to solve the mobile communication security problem, our approach will work alone the current mobile communication system, and so many basic protocols will follow the current standard of mobile communication system.

Chapter 5 will give the discussion of approach's performance and evaluation;

Chapter 6 in this section, the conclusion of this approach will be given, and it also has the further discussion of the future work.

Chapter 2 Cellular system's security feature

This chapter will generally introduce the current cellular system and specifically its security features which include the authentication mechanism and encryption method, and the inherent flaw which need to be solved.

2.1 GSM system

GSM system is the most successful and popular digital mobile phone system in the world. GSM is used by over 800 million people in more than 212 counties and territories. The second generation fully digital system was founded in 1982, and soon it is named as Global System for Mobile Communication (GSM).

The primary goal of GSM system was to provide a mobile phone system that allows users to roam throughout Europe and provides voice services compatible to ISDN and other PSTN systems. GSM is a typical second generation system which was designed to replace the first generation analog systems. There are three versions GSM system which are GSM 900, GSM 1800, and GSM 1900.

GSM is designed mainly to offer voice services and this is still constitutes the main use of GSM systems. The following figure is showing us the GSM system architecture [2].

GSM: elements and interfaces

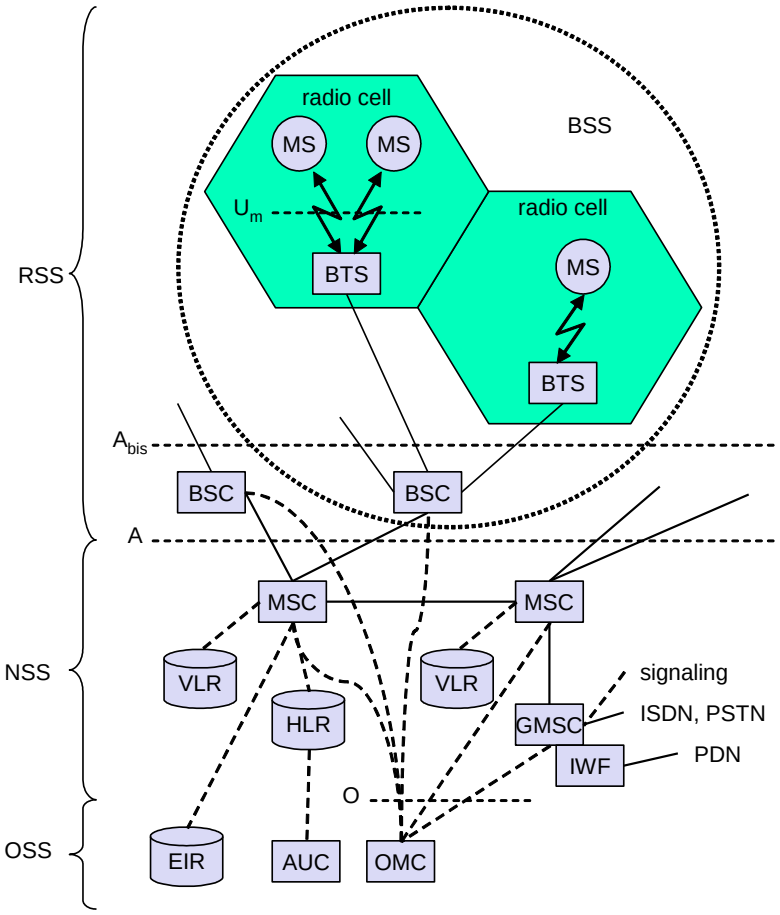

Figure 2.1 Function architecture of a GSM system [2].

Figure 2.1 gives a general overview of the GSM system as specified in ETSI (1991b). We can see the GSM system is mainly contributed by three subsystems, the radio subsystem (RSS), the network and switching subsystem (NSS), and

the operation subsystem (OSS).

Radio subsystem

Radio subsystem is comprised by all the radio specific entities, such as mobile station (MS) and the base station subsystem (BSS). We can see in figure 2.1 the connection between RSS and NSS via the A interface (solid lines) and the connection to the OSS via the O interfaces (dash line). The A interface is typically based on circuit- switched PCM-30 system, and the O interface uses the signaling system NO. 7 [2].

- Base station subsystem (BSS): Each BSS controlled by a base station controller (BSC). The BSS performs all necessary functions which is needed to maintain radio connection to an MS, coding/ decoding of voice, and rate adaptation to/ from the wireless network part [Jochen Schiller, “Mobile communication”, second edition, 2003, pp. 102]. Many BSS is contributed a GSM system.
- Base transceiver station (BTS): Its connection to MS is via Um interface, and to the BSC via the Abis interface. A BTS comprises all radio equipment, and it is able to form a radio cell or, several cells.
- Base station controller (BSC): Used to manage the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within a BSS, also do the paging job to the MS. Besides, the BSC is also multiplexes the radio channels onto the fixed network connections at the A interface.

- Mobile station (MS): For a GSM subscriber, it is usually known as mobile phone. A MS consists of user independent hardware and software. In a MS, the Subscriber Identity Module (SIM) is stores all the specific information that relevant to GSM. And a MS is also can be identified via the international mobile equipment identity (IMEI). The SIM card contains all the needed information of the subscriber, such as card-type, serial number, services of the subscriber, personal identity number (PIN), a national mobile subscriber identity (IMSI). Besides this, the SIM card is also store some dynamic information while its logged on a GSM system, such as cipher key Kc, temporary mobile subscriber identity (TMSI) and the location area identification (LAI).

Network and Switching subsystem

Network and switching subsystem (NSS) formed the "heart" of the GSM system. The NSS performs all necessary functions of the GSM systems, such as handovers between different BSSs, comprises functions for worldwide localization of users and supports charging, accounting, and roaming of users among different service providers. A NSS is consisting of following switches and database:

- Mobile services switching center (MSC): MSC is highly performance ISDN switch. The connections to other MSCs and BSCs are via the A interface, and form the fixed backbone network of a GSM system. A MSC use the

standard signaling system NO.7 (SS7) to handle all signaling needed for connection setup, connection release and handover of connections to other MSCs. SS7 covers all aspects of control signaling establishing for digital network [2].

- Home location register (HLR): The HLR is the most important database in a GSM system, it is stores all user-relevant information. The information includes static information such as the mobile subscriber ISDN number (MSISDN), subscriber services and the international mobile subscriber identity (IMSI); also there is some dynamic information like the current location area (LA) of the MS, the mobile subscriber roaming number (MSRN), the current VLR and MSC. HLRs can manage data for several million customers and contain highly specialized data bases which must fulfill certain real-time requirements to answer requests within certain time-bounds.
- Visitor location register (VLR): The VLR is a dynamic database associated to each MSC, which is stores all important information needed for the MS users currently in the LA. When a new MS comes into an LA the VLR is responsible for, it copies all relevant information for the user from the HLR.

Operation subsystem

The operation subsystem contains the necessary functions for network operation and maintenance. The OSS possesses network entities of its own and able to

access other entities by SS7 signaling [2].

- Operation and maintenance center (OMC): Via the O interface by using SS7 with X.25 the OMC monitors and controls all other network entities. Typical OMC functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing.
- Authentication centre (AuC): The AuC has been defined to protect user identity and data transmission. It contains all needed algorithms for authentication like keys for encryption and generates the values for users register in the HLR.
- Equipment identity register (EIR): The EIR is stores all deice identifications registered in the network. It has a black list which has all the relevant information of the stolen MS, and disables them. The EIR also contains a list of valid IMEIs and list of malfunctioning devices.

2.1.1 GSM authentication mechanism

The security service offered by GSM system includes user authentication and communication data encryption. And the GSM is using confidential information stored in the AuC and in the individual SIM which is plugged into the user's mobile phone. The security services offered by GSM are explained below:

- Access control and authentication: The first step is authenticate the valid user for the SIM, which the user needs a secret PIN to access the SIM. And next step is the subscriber authentication, and this is based on a

challenge-response scheme.

- Confidentiality: After authentication, BTS and MS apply encryption to voice, data, and signaling. The confidentiality only exist between MS and BTS, but it dose not exist end-to-end or within the whole fixed GSM/telephone network.
- Anonymity: In the VLR, all users' data is encrypted before transmission, and user identifier are not used over the air. So in the GSM system, it transmits a temporary identifier (TMSI), and this can be changed by the VLR any time.

There are three algorithms have been use in GSM system to achieve the security goals. Algorithm A3 is used for authentication, A5 for encryption, and A8 for the generation of a cipher key. The following figure is showing the interface of A3, A5, and A8 in the GSM system.

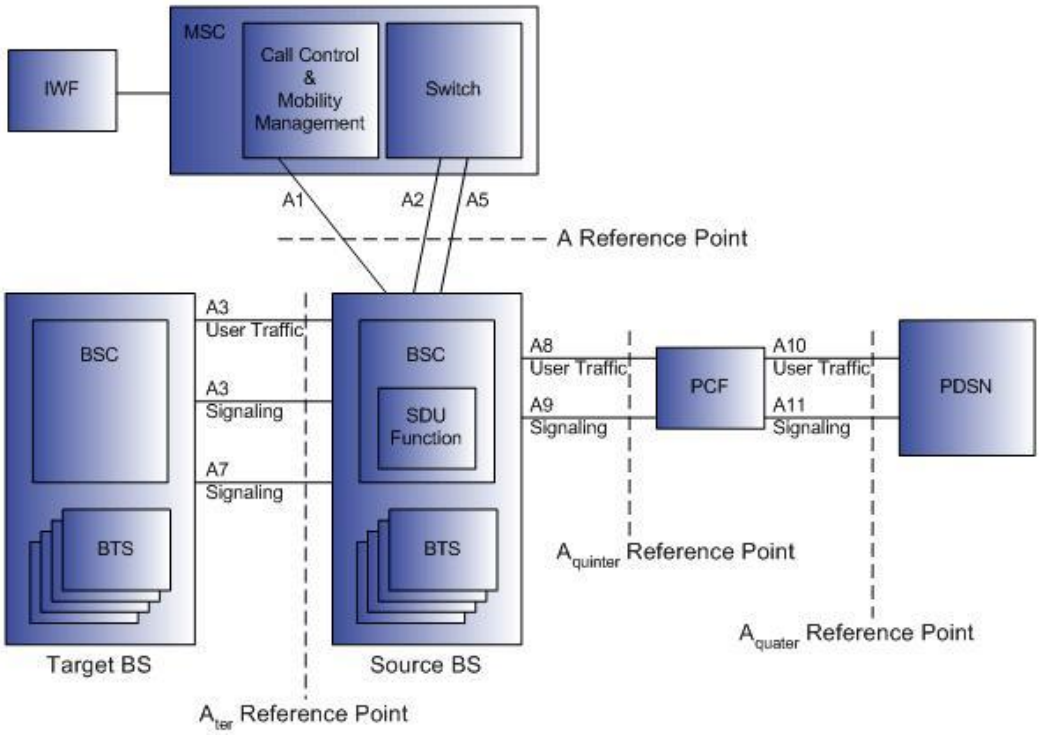

Figure 2.2 the interface of GSM algorithms

GSM authentication process

The GSM authentication is base on the SIM, which stores all the relevant information of the subscriber needed to be authenticated, such as the individual authentication key K_i, the user identification IMSI, and the algorithm used for authentication A3.

The following figure is showing the progress of the GSM systems authentication.

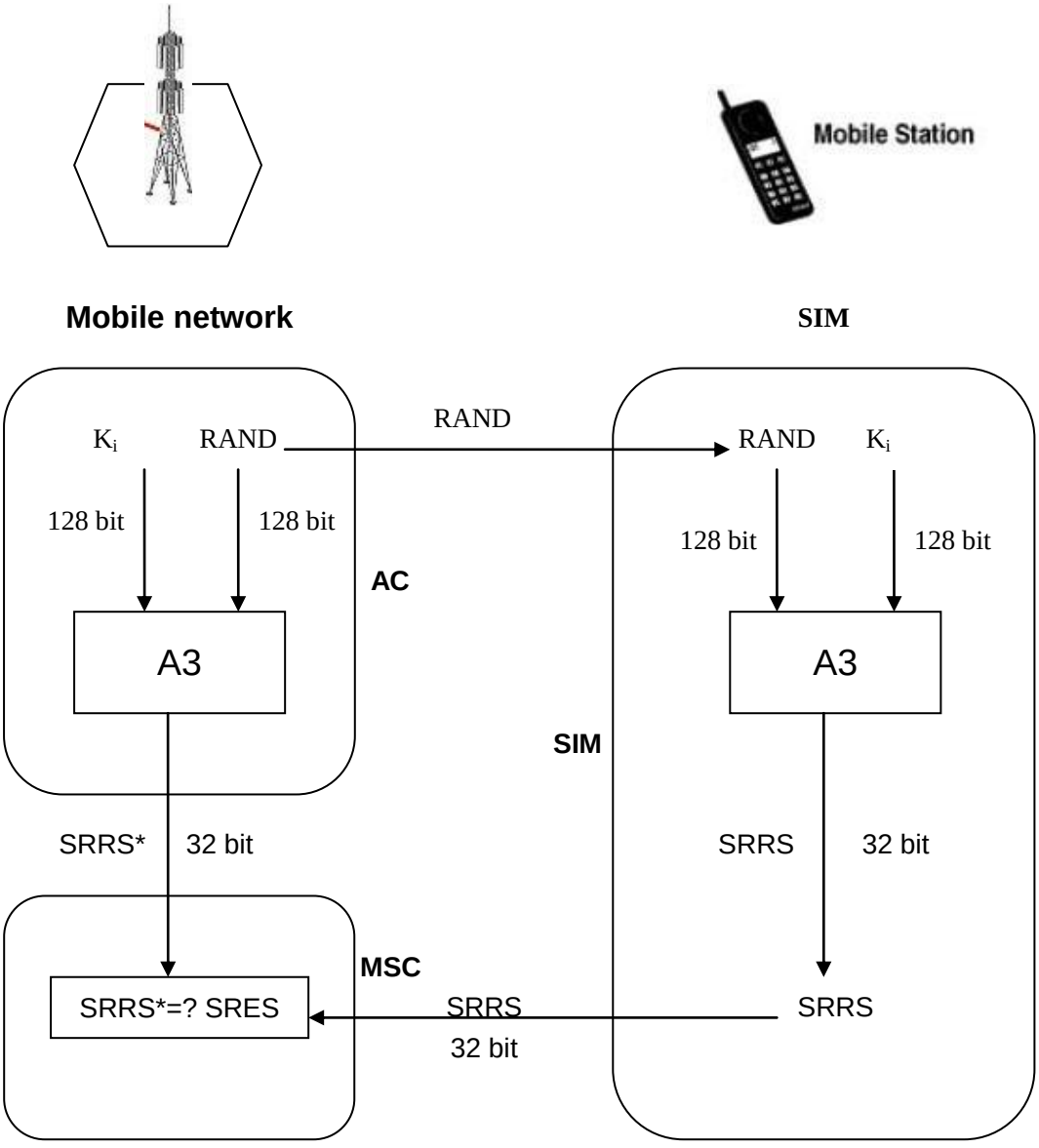

Figure 2.3 The progress of subscriber authentication [2]

The GSM system is uses a challenge-response mechanism to achieve

authentication job, they are progress like this: a random number RAND is generated by the access control AC as challenge, and the SIM in the MS will answer this by a response with SRES (signal response). The AuC performs the basic generation of random values for RAND, SERS, and K_c from the HLR.

When a network authenticates a subscriber, the VLR will generate a random value RAND to the SIM. While the SIM create the SERS by algorithm A3 and send it back, the network also performs the same operation. When network receive the SERS from the SIM, it will compare both values. If they are match, the VLR will accept the subscriber; otherwise the subscriber will be rejected.

2.1.2 GSM encryptions

As we can see in figure 2.4, in the GSM system all the messages containing user-related information are encrypted in GSM over the air interface.

After authentication, MS and BSS will use the cipher key K_c to do the encryption work. K_c is generated by the individual key K_i and a random value by applying the algorithm A8. The key K_c can be calculated base on the random value RAND by SIM and the network. And the key K_c is not transmitted over the air interface.

As the figure 2.4 shows, both MS and BTS can encrypt and decrypt data using algorithm A5 and the cipher key K_c. K_c should be a 63-bit key which is not strong enough. The key K_c is strong to protect the communication from simple eavesdropping.

However, the publication of A3 and A8 on the internet showed that in certain implementation 10 of the 64 bits are always set to 0, so that the real length of the key is thus only 54 consequently, the encryption is much weaker.

The figure below will show us the GSM system encryption progress.

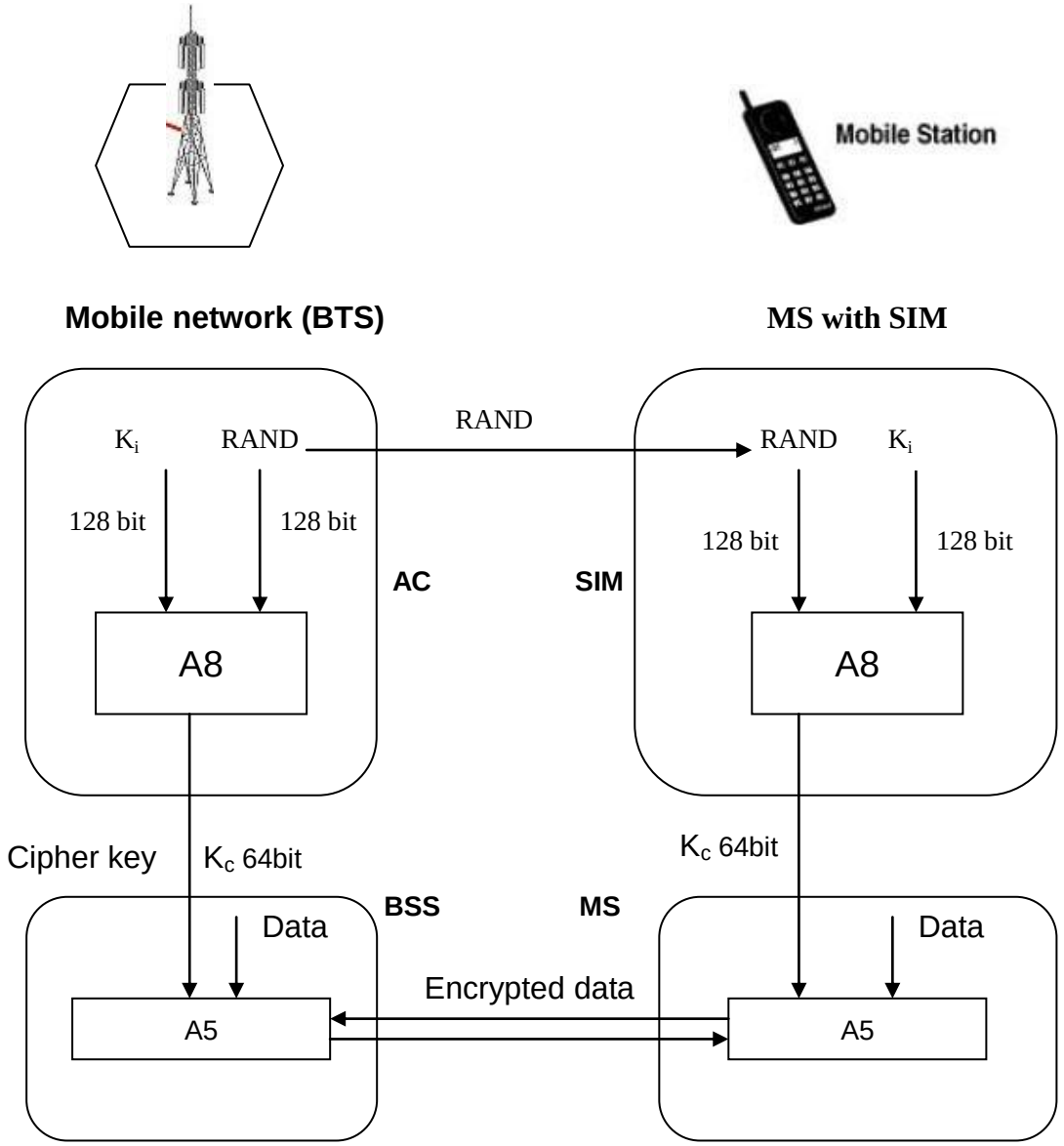

Figure 2.4 Data encryption in GSM system [2]

As we can see in this section, although the GSM system has offered some

security service in its network, but those algorithm it use in the system has some inherent flaws that makes the security system still vulnerable, especially when the some one has malicious intent to eavesdropping others communication.

2.2 WLAN system and its security core

After Wireless Local Area Network (WLAN) has been introduce into the market at earlier 1990's, it is aimed a very high development speed and achieve a remarkable progress in last 2 decades.

The term WLAN we use nowadays usually refers the IEEE 802.11 standard, which was first publish at the end of last century; we can also use the term Wi-Fi to refer the WLAN.

802.11 is a member of the IEEE 802 family, which is a series of specifications for local area network (LAN) technologies. The figure below shows the 802 family and the position of 802.11 protocol's position.

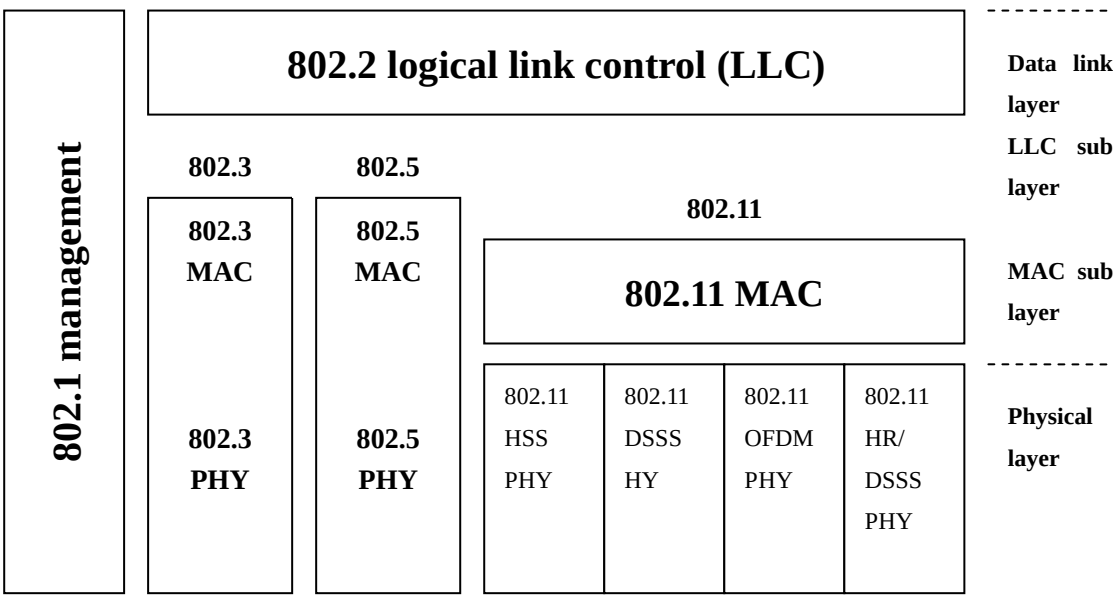

Figure 2.8 802 family and related OSI model layers [5]

We can see in figure 2.8, the IEEE 802.11 protocol belongs to 802.2x LAN standards. The standard indicated the physical and medium access layers to adapt to the wireless LAN requirement. So in this paper, the term WLAN is mainly refers the IEEE 802.11 wireless distribution network.

2.2.1 Advantages of WLAN

Wireless local area network (WLAN) offers wireless connectivity in a small area, when wireless LAN been introduced into market at the earlier of 1990's, its properties shows its potential in wireless communication market. Since it is utilize radio waves as its communication medium, the WLAN offers a lot of

benefits which tradition cable internet connection can not be offered.

The cost efficiency, ease of integration with other network makes wireless LAN became a hot spot in wireless communication market. The benefits of wireless LANs include[5] :

- Mobility: With the public networks, users can access the internet even out of their office. Most of coffee chain store like Starbukes is usually offers their customers free wireless connection.
- Convenience: The wireless nature of the network allows users are able to access the network at any convenient place for them within the network signals coverage. Especially nowadays when the laptop-style computers users is increasing really fast.
- Deployment: The initiation of setup an infrastructure-based wireless network only requires a cable connection and a single access point. But on the other hand, wired networks have the additional cost and much more complex because of the complex physical location.
- Expandability: A network access point is capable to allow several different uses to access the network. Compare with the wired network, this is a tremendous improvement and don't need to deploy any new cable as the wired network when a new user is join the network.
- Cost: The cost of deploy a wireless network is mainly focus on the access point and sometimes may need a little bit more. Especially, after the initial setup, we don't need to deploy any physical equipment any more.

2.2.2 The WLAN types

There are two main WLAN prototypes, infrastructure-based and the Ad-hoc network.

The Ad-hoc network is a self-construction network, and the most important property is this network is a dynamic topology. This type of network is usually constructed in a small area by different mobile device, such as lap-top and PDA or smart phone which is able to access the WLAN network.

Compared the ad-hoc network, the infrastructure-based network's topology is a static network construction, and this type of network is also the most commonly used in our daily life. Infrastructure-based network's users access the network is mainly through the access point.

The figures below show the two types of network.

Figure 2.9 The infrastructure network topology

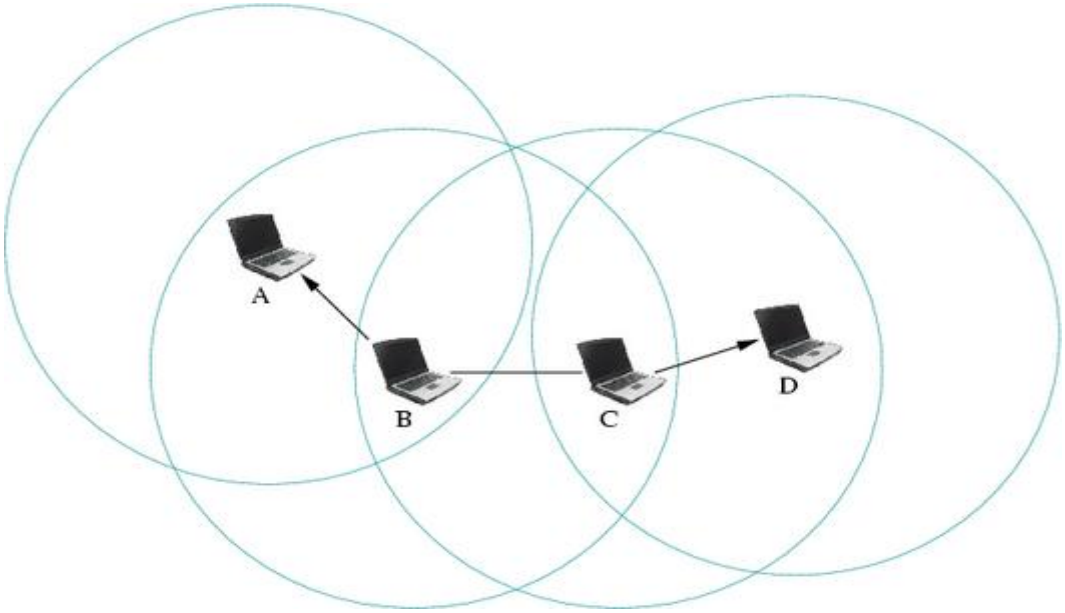

Figure 2.10 The Ad-hoc network

We can see in last two figures, the design of infrastructure-based wireless network is simpler than the Ad-hoc network. But infrastructure-based also lose flexibility, and in this network, the collision some times happens when the medium access of the wireless nodes is not coordinate with the access point.

2.2.3 WLAN protocol and bridging

We can see in figure 2.8, like other 802.x LANs protocol, IEEE 802.11 standard's coverage is the physical layer PHY and medium access layer MAC. Also as indicated from the standard number, IEEE 802.11 fits into other 802.x standard seamlessly. The figure below is showing us a most common scenario

which a IEEE 802.11 WLAN connected to a switched Ethernet via a bridge.

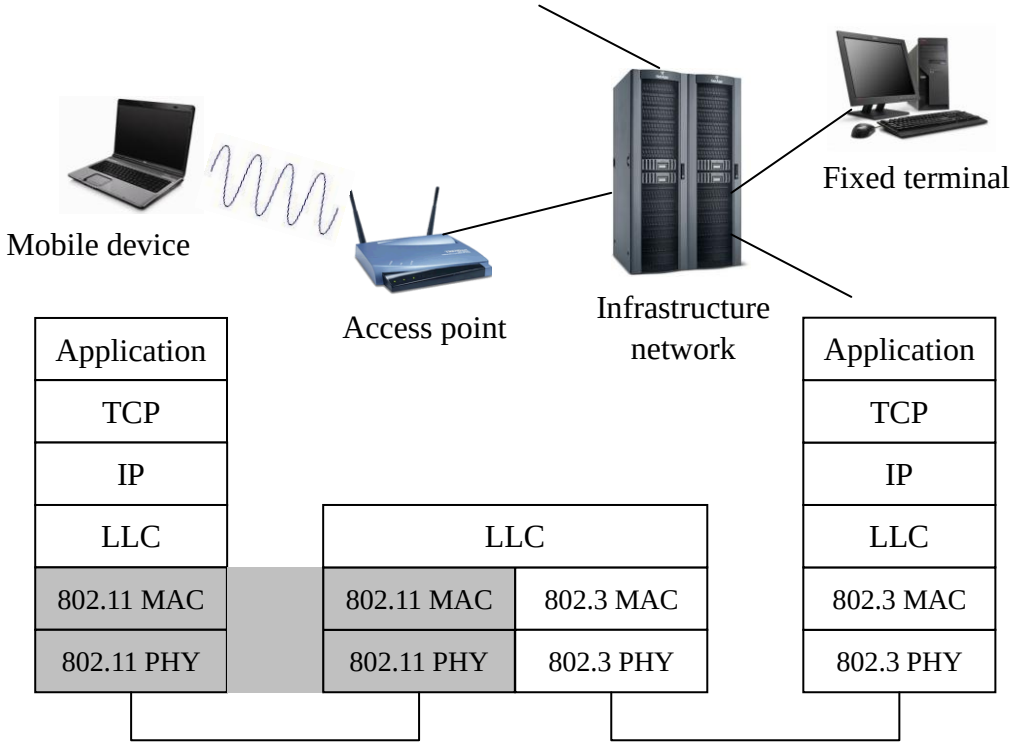

Figure 2.11 IEEE 802.11 protocol architecture and bridging [2]

Usually in the IEEE 802.11 application, the lower bandwidth and the high access time from the wireless LAN shouldn't be noticed. As a result, for the higher layer, such as application, TCP, IP, treat the wireless node as same as the wired nodes. Actually, in most WLAN application scenario today, the logical link control (LLC) is usually invisible.

In the IEEE 802.11 standard, the physical layer is subdivided into another two

layers, the physical layer convergence protocol (PLCP) and the physical medium dependent sub-layer (PMD). The PLCP sub-layer's mainly task is providing a carrier sense signal and a common PHY service access point (SAP). On the other hand, the PMD sub-layer handles modulation and encoding/ decoding of signals.

Different from PHY layer, the basic task of MAC layer is mainly focus on medium access, fragmentation of user data, and the encryption.

Besides those sub-layer protocols, IEEE 802.11 standard also specifies management layer and the station management, which means the MAC layer is also achieve the association and re-association between mobile station and access point. The security services such as authentication, encryption provided in this layer. Meanwhile, the PHY layers job is not that much less than MAC layer, it mainly works on the signal such as channel tuning and PHY management information base (MIB). The figure below shows the detail of IEEE 802.11 protocol.

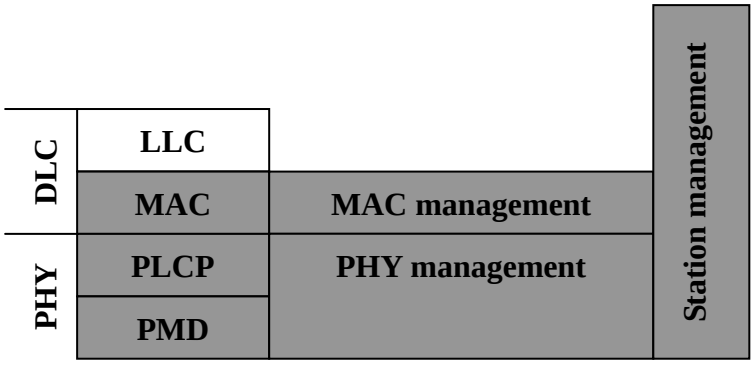

Figure 2.12 Detailed IEEE 802.11 protocol architecture [5]

2.2.4 WLAN security core and its flaw

As we mentioned at the end of last section, the main security service such as authentication, data encryption and decryption are provided in the MAC layer. There are two security service scenarios, one is provided through the Wired Equivalent Privacy (WEP) and another is using the 802.1x protocol. We will discuss them separately next.

The security service in IEEE 802.11 was originally secure, but as those flaws get more and more clear, the WLAN security service is not secure enough. And today we can easily download all kinds of free charge software on the internet which is able to break the WLAN security service easily within a short time. In 2005, the FBI shows a free software which download from the internet, it can crack the WEP within 3 minutes.

Web Equivalent Privacy (WEP)

When WEP was introduced in 1999 as the data string protection, it was intended to provide confidentiality as tradition wired network. So in WEP it uses the string cipher RC4 to provide confidentiality, and the CRC-32 checksum is provided for the data integrity. The figure below is showing us the standard WEP secure progress.

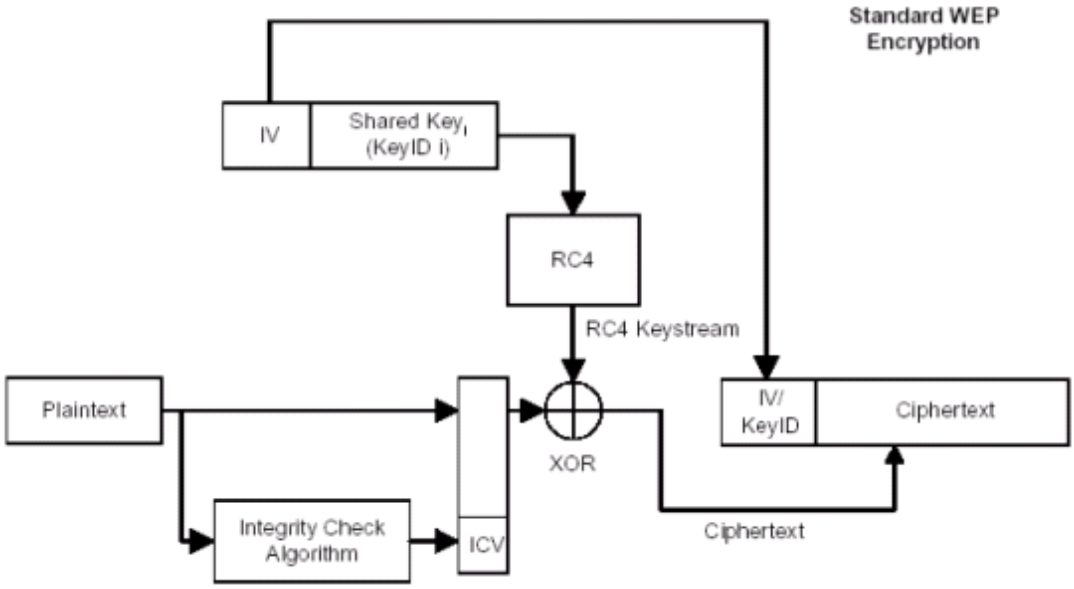

Figure 2.13 WEP encryption processes [3]

We can see in this figure the WEP encryption process is

1) Create the 104-bit key and the Initiate Vector (IV), and use Key-scheduling algorithm (KSA) to generate the key string;
2) Use pseudo-random generation algorithm (PRGA) to create the data string, this could give every packet a encryption key, and XOR with the plaintext to get the cipher text;
3) When the encryption finish, the IV will be added and send;
4) The decryption is a reverse progress.

In this course, there are two very serious problems, which is also the reason of the WLAN security threatens.

First, if a hacker knows the data before the encryption, then he just needs to capture the cipher text and XOR with the plaintext and get the key string. To get the cipher text, you just need a wireless sniffer. How to get a plaintext? There are many ways to achieve that, the most effective way is use the WLAN packet, which we can know a lot of variable, such as IP header, IPX header, SNAP header, etc… and the SNAP header always send as the first byte of the packets, so if we know cipher text n and n+1, we can XOR them and get the n+1 plaintext. Second, the attacker can get the whole key string, but key string is the key and IV creates by using KSA and PRGA. This is means that we have to get the IV to know the key and decrypt the cipher text. The problem is the IV is send to the encrypted data in plaintext!!

We can see in WLAN security, there are many security problems, and for the first step- the authentication and the key generation is most critical part. In next

section we will introduce the technique which we will used to improve the security in mobile communication system.

Chapter 3 hand writing and drawing pattern recognition

3.1 Pattern recognition model

Pattern recognition's research goal is to achieve the automatic classification of data or other special objects such as picture or signature's classification by computer or any other similar digital devices.

The classification is based on the priori knowledge or some static information which extracted from the pattern. In a complete pattern recognition system, sensor is an important part to gather the classified data from observation; feature extraction will be done after the data collects from the object which called training; classification scheme will dose the actual job for classifying the objects based on the data which collected by the feature extraction mechanism. The following figure is showing the basic progress of the pattern recognition.

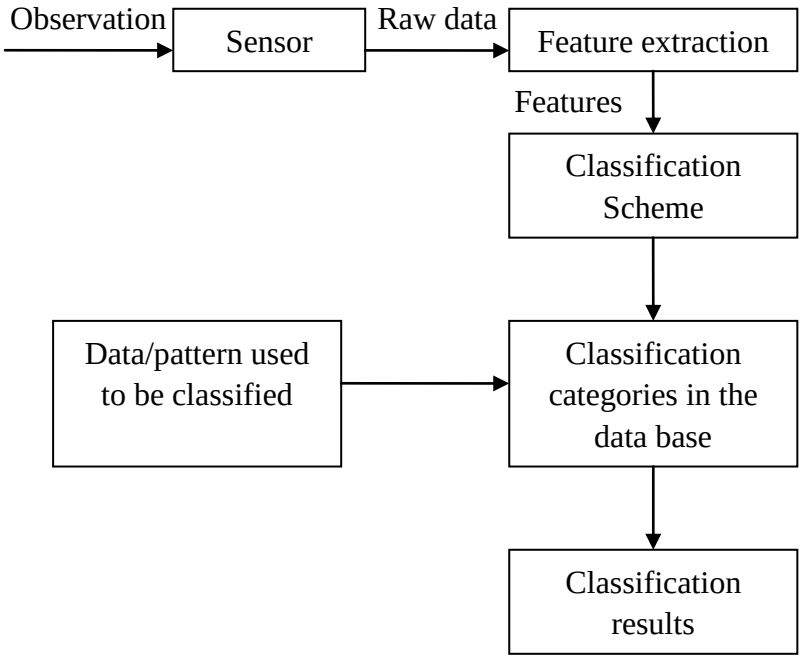

Figure 3.1 the basic process of patter recognition

The following parts will introduce different basic methods used in pattern recognition such as text classification, hand writing recognition, and image recognition.

3.1.1 Naïve bayes classifier

The naïve bayes classifier's design is based on the bayes theorem, which is a probability model for classification. The Bayesian classification assumes that for a given class C, there is several different attributes effect on it, F_1 to F_n, and all these attribution is independent from each other. We note it as:

$$p(C| F_1, F_2, \ldots\ldots F_n) \ (n \geqslant 1)$$

We call this assumption *class conditional independence,* and p (C| F_1, F_2…… F_n) is called **posterior probability.** Using bayes' theorem we also write

$$p(C|F_1,\ldots,F_n) = \frac{p(C)\ p(F_1,\ldots,F_n|C)}{p(F_1,\ldots,F_n)}$$

We use this formula to calculate the probability of p(C) which is effective by several different factors. The probability p(C) we used to call it *priori probability.*

Now we will simply introduce the progress of Naïve Bayesian classification.

We assume that we have a group of data X_i, and each of them been effected by several independent factors, note it as n-dimension vectors (x_1, x_2, …….x_n). So it is written as: X_i=(x_1, x_2, …….x_n). All these data can be classified into m classes. Therefore when an unknown data X is given, based on the highest probability which is calculated through the bayes theorem, we can classifies the X into class C_j. This can be expressed by the equation below:

$$p(C_j|X) > p(C_i|X) \text{ for } m \geqslant i \geqslant 1$$

According to the equation we wrote before we can calculate the probability as follow:

$$p(C_j|X) = p(X|C_j)\ p(C_i)/p(X)$$

In this equation, the p(X) is constant for all classes, and if the class prior probabilities are not known, we usually assume that the classed are equally likely, p (C_1) = p (C_2) = ……= p (C_m). As we were assumed that all the effective factors on the data X_i is independent. So

$$P(X|C_i) = \prod_{k=1}^{n} P(x_k|C_i)$$

For an unknown sample X, we classifier it into each class C_i is if an only if

$$P(X|C_i)\,P(C_i) > P(X|C_j)\,P(Cj) \text{ for } 1 \leqslant j \leqslant m, j \neq i.$$

3.1.2 Hidden markov model (HMM)

The hidden markov mode is a statistical mode which is used to describe a markov process contains unknown parameters. And in this model, the most challenge job is to find the hidden parameters from the observation parameter. And the key point is the model's observation parameter's extraction. How to choose an observation parameter and how many of them we should extracted from the observation model will be critical for the further analysis. So hidden markov model is very useful to applied in the pattern recognition, and for its properties and special model structure, it is been widely used in the character and voice pattern recognition [6].

Before we introduce the detail of hidden markov model (HMM), a short description will be given to show a simple hidden markov model (HMM) application in our life.

The following example will give you a general ideal about this model.

Assume you have a friend who lives far from you, and everyday he call you and tell you what he did that day. The mainly things he did are: walking in the park, shopping and clean his room. What he does will depends on the local weather.

Since you living far from him, so you don't know the weather in his place, but you know general trends. Base on the information he told you what he did that day, you can guess the weather situation in his place.

On the other hand the weather situation is working like a markov chain, the two conditions are "raining" and "sunshine", you are unable to know it directly, this is means, and the weather is hiding for you. For your friend, to choose what he do that day will be ruled by some probability of walking in the park, shopping and clean his room. And when he told you what he did that day would be the observation data for you. So this whole system makes up a hidden markov model.

As the definition given by Rabiner, a hidden Markov model *"is a doubly embedded stochastic process with an underlying process that is not observable (it is hidden), but can only be observed through another set of stochastic processes that produce the sequence of observations."* In the example we mentioned above, the unknown weather for us is an *underlying process* which is also called hidden markov chain. And the *sequence of observations* is what the friend told in telephone.

In the following part will introduce hidden markov model in mathematic details and its classification application. First, we will give the definition of the model notation [6]:

T Length of observation sequence (total number of time step).

N Number of states in the model.

M Number of observation symbols.

S $\{S_1, S_2, \cdots, S_N\}$, states.

Q $\{q_1 q_2 \cdots q_T\}$, state sequence.

V $\{v_1, v_2, v_3, \cdots, v_M\}$ discrete set of possible observations.

q_t State visited at time t

A $\{a_{ij}\}$, $a_{ij} = P(q_{t+1} = S_j | q_t = S_i)$, state transition probability distribution.

B $\{b_j(k)\}$, $b_j(k) = P(v_k \text{ at } t | q_t = S_j)$, observation symbol probability distribution in state j.

π $\{\pi_i\}, \pi_i = P(q_1 = S_i)$, initial state distribution.

The hidden markov model we use here is give parameters of the model, and computer the probability of a particular output sequence. Usually we use forward-backward algorithm to solve this problem.

For an observation sequence $O = \{O_1, O_2, \cdots O_T\}$, it can give a model λ, so we can use $P(O|\lambda)$ to perform classification. The simplest way is computing $P(O|\lambda)$ by enumerating every possible state sequence. So the calculation will be:

$$P(O|\lambda) = \sum_{\text{all } Q} P(O, Q|\lambda)$$

$$= \sum_{\text{all } Q} \pi_{q_1} b_{q_1}(O_1) \prod_{t=2}^{T} a_{q_{t-1} q_t} b_{q_t}(O_t).$$

Since we use forward-backward algorithm to solve this problem, to compute the $P(O|\lambda)$ will need $O(TN^2)$ as computations. So the forward variable $\alpha_t(i)$ is

$$\alpha_t(i) = P(O_1, O_2, \cdots O_T, q_t = S_i | \lambda)$$

The induction of $\alpha_t(i)$ work as follow:

For all $1 \leqslant i \leqslant N$, $\alpha_1(i) = \pi_i b_i(O_1)$

When $1 \leqslant t \leqslant T-1$ and $1 \leqslant j \leqslant N$,

$$\alpha_{t+1}(j) = \left[\sum_{i=1}^{N} \alpha_t(i) a_{ij}\right] b_j(O_{t+1})$$

So final result would be $P(O|\lambda) = \alpha_T(i)$.

The equation is tenable only under the assumption of statistical independence.

On the other hand, for the backward part, we define the backward variable $\beta_t(i)$ is

$$\beta_t(i) = P(O_{t+1}, O_{t+2}, \cdots O_T, q_t = S_i|\lambda)$$

As the similar computation process as forward algorithm, the backward algorithm will get

$$\beta_t(i) = \sum_{j=1}^{N} a_{ij} b_j(O_{t+1}) \beta_{t+1}(j)$$

so for any $1 \leqslant t \leqslant T-1$

$$P(O|\lambda) = \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_t(i) a_{ij} b_j(O_{t+1}) \beta_{t+1}(j).$$

The bellowing figure shows the operations required the forward-backward algorithm computation.

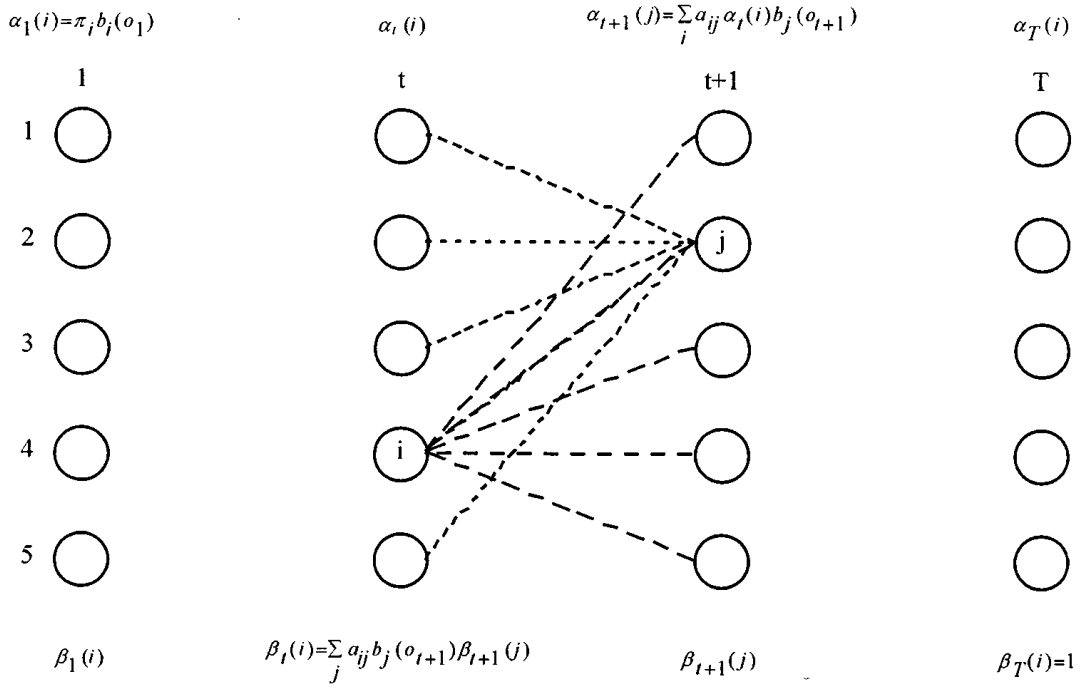

Figure 3.2

3.2 Handwriting pattern recognition

Handwritten word recognition was originally an implementation of automaton reading machine. And this task is characterized by high data rates, large amounts of data, possibly error-filled input, and the need for real-time response. The challenge for this task is due to the incomplete, imprecise, and ambiguous content of handwritten word image. The bellowing figure is showing a handwritten note [6]:

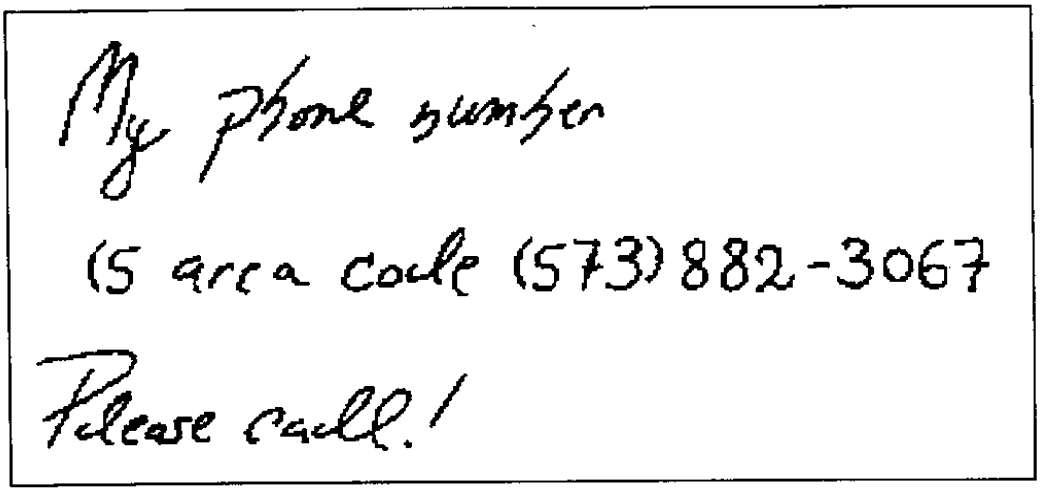

Figure 3.3

This kind of note is very normal in our life, and it is not hard to recognize its content which is “My phone number is area code (573) 882-3067. Please call!” for us. But for the computer or reading machine, it is a big difficult problem. We can see in the note, the challenge is not only comes from the great variety of the character’s shape, but also the overlapping and the interconnection of the neighboring characters. Let’s take look at the note, the word “is” and the code number “(5” is very similar. And the “h” in the word “phone” is also looks the same as the “b” in the word “number”. Also the “d” in the word “code” and the “l” in the word “please” are also written identically.

Now we can have a general idea about what kind of difficult we are dealing with, this note is written by a single writer, and there are many variations we need to consider, such as character’s size, shape, etc. there are many design offered different approach for handwriting character’s recognition, based on its type of classification methods we have neural networks, fraction eigen-features

based recognition, fisher's discriminate.

During past decades, Hidden Markov Models have been applied in handwritten recognition; some development of hidden markov models has aimed good performance in handwritten recognition area. The following introduction will follow the section 3.1.2, and some denotation will be the same as in the section. The Hidden Markov model we used here is continuous density HMM, since it can provide more flexibility for different levels of complexity and feature attributes of the individual character classes.

The following figure shows an overview of a word recognition system.

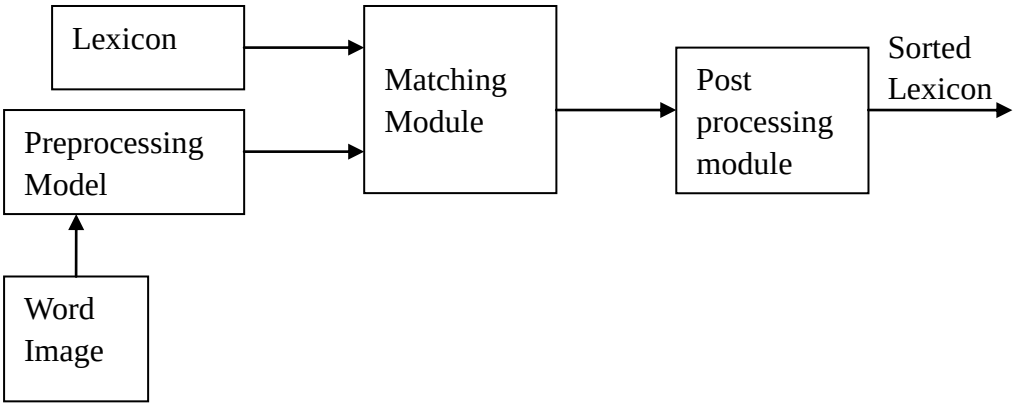

Figure 3.4 overviews of a word recognition system

We can see in a recognition system, it usually has 2 input: a word digital image, and the lexicon. The lexicon here representing the possible identities for a word image. The preprocessing model here is usually applied to reduce the recognition mistake, such as noise filter and boundary check, etc. For the word recognition, it will look for the maximum match in the lexicon. The match score

of a string in the lexicon means the degree of the image “looks like” the lexicon string.

In the recognition processing, the feature extraction is the most important task. Appropriately extract features from the image will directly influence the recognition result. From the binary word image, we can have an observed vector group { O_1,O_2,⋯, O_T}. These vectors also referred as the transition features. Figure 3.5 shows a general progress of handwritten word recognition progress.

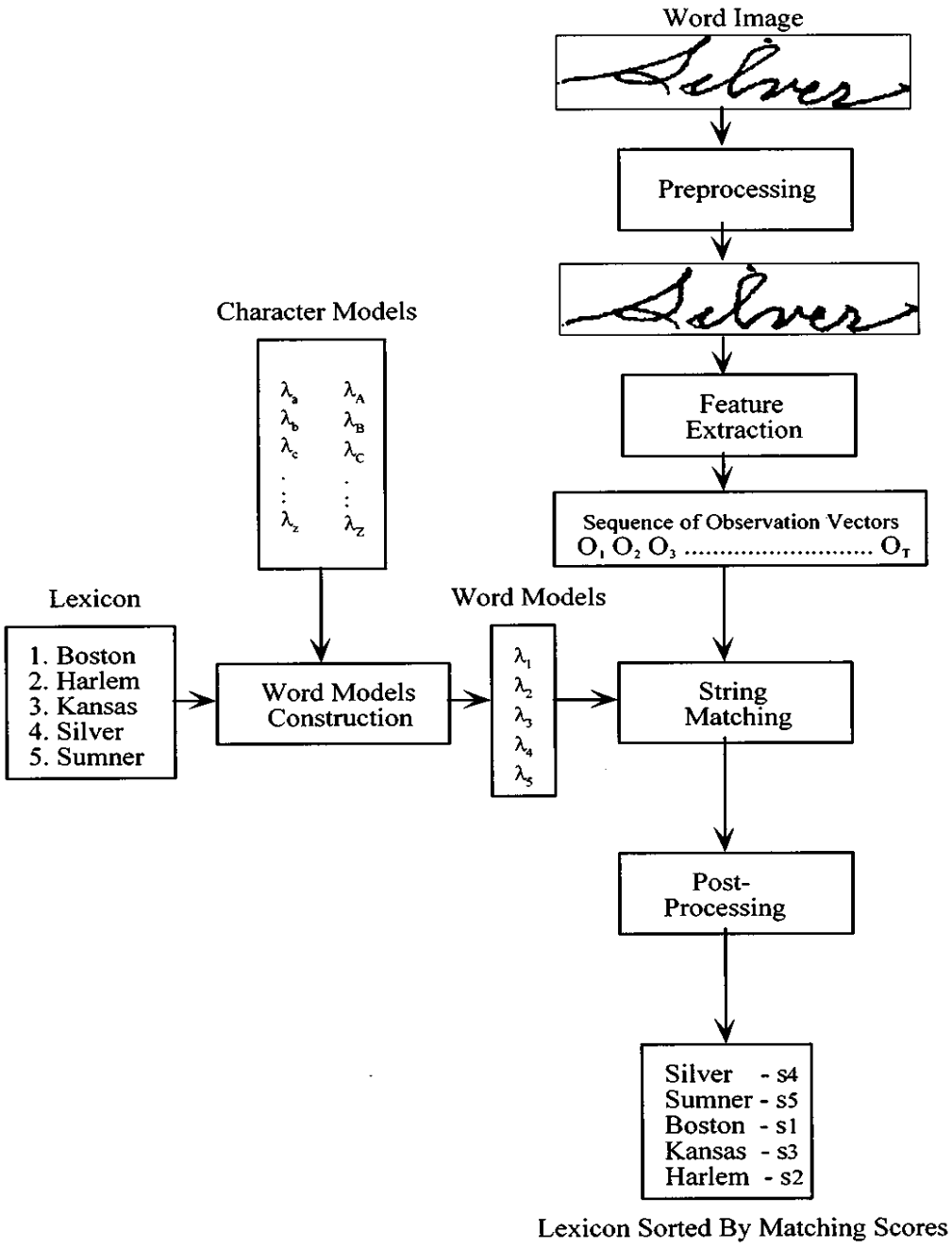

Figure 3.5 the process of word recognition

The transition feature is computed from the location and number of transition from background to foreground pixel along vertical lines. And for the character modules training, the observation sequences has fixed length T = 24. In the figure 3.5, the character models λ is the follow the alphabet with lower case and upper case. So for Latin characters, it is usually having 52 classes in English.

In the handwriting recognition, there is another problem need to solved, which is how to isolate the hand writing word from its neighbor letters. In this part, the left-to-right model can be the solution. The following figure is showing the structure of a character assuming five states.

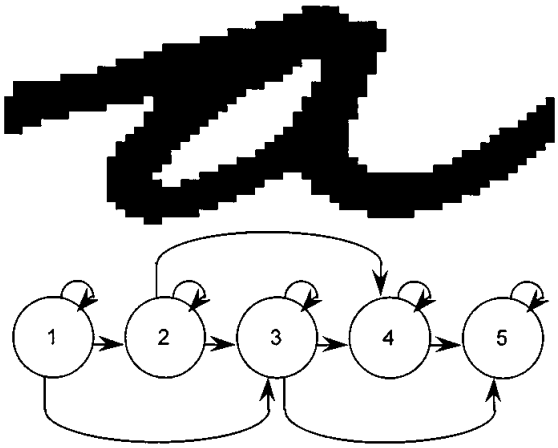

Figure 3.6 a character model and five assuming state

In this model, the state i to state j is only allowed j⩾I, this model is very useful to build a word model from character models [6].

Chapter 4 Approach for mobile communication security

According to we described in chapter two, we can see the most important issue in wireless communication is the user's identity authentication and the security of the session data cipher, which involve the cipher keys generation.

In tradition way, the user's password can be used for authentication. But, the password use sometimes put us into a dilemma; if we want our account secure, we should make our password as long as its possible, however, when the password is too long, we may unable to memorize it.

We all had experience, which is even we can not remember long password, but we can remember some simple picture or figure easily and some words or sentence we write a lot in our daily life. So if we can use figure or simple hand draw picture or our handwriting to achieve the authentication and complex key generation task. It should be a good way to improve our communication system's security.

Today, most mobile devices such as cell phone, PDA, lap-top are allowed the users use iron pen write on the screen as a way to input or mouse draw in certain panel. Most of these functions are only used to input character into the communication. So if we can use handwriting pattern recognition for

authentication and the data which generated in the progress of authentication to generate the cipher key, this could be a solution of the mobile communication system's security problem.

In this chapter we will introduce our approach of the improvement of the mobile security. And it will consist by two part, handwriting recognition and hand drawing recognition.

4.1 The user authentication by hand writing

The term *hand writing* here is indicates the letter or characters we write down, used for the system authentication.

As we can see the figure 3.1, the authentication process is also very similar. When the client log into the network for the first time, the registration of "password" will be require. And this data will be collected by the authentication server as the authentication information in the future.

Here we are using the hidden markov model (HMM) to deal with the hand writing on the mobile device. This is the first step when we are log in a network, and this step's task including authenticate the user's identity and the authentication information's generation which will be used to exchange with the authentication servers.

We already know how a handwriting recognition system works, so when a client log into the network. Its input-their handwriting pattern-will be first processed on the own mobile device. Only when the input regards validation, then it will

send the identity data to the authentication server.

The HMM used in handwriting pattern recognition usually extracted features from the digital figures. Usually pixels along vertical lines from the background to foreground will used to computer the location and number of transition. And this would be the generation of transition features.

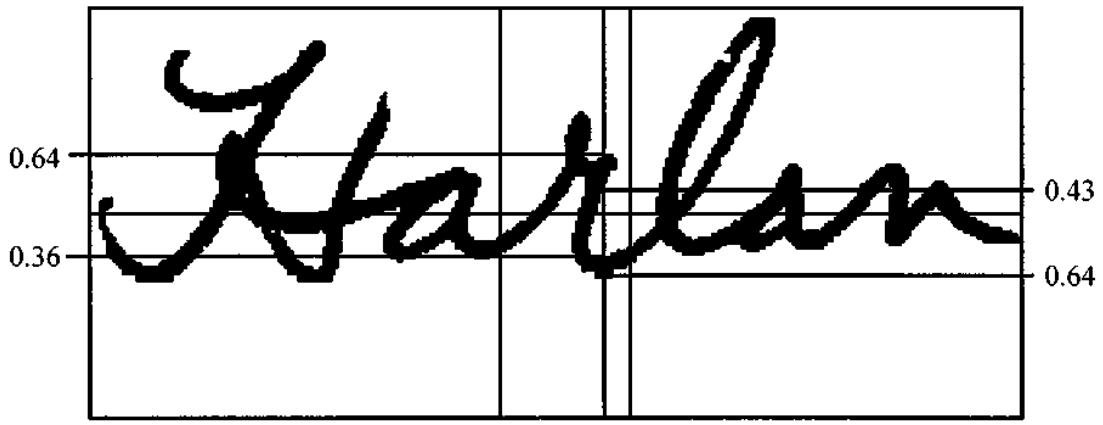

Figure 4.1

We can see in figure 4.1; when we extract the feature, the first step we do is to estimate a horizontal center line of the word. And this line will be used to account for differences in the positions of characters in a word, this would be depending on whether a descender or ascender at that point. We can see in the lower case “a” is at the bottom of a word image. And on both side the descender and ascender can be used to isolate it from other word [6].

According to we discussed about HMM used in handwriting pattern recognition. We can see that use the parameter A, B, or π to generate a matrix to be an access control method. For a HMM model, if we take 3 states and 3 distinct

observation symbols in a word digital pictures we can generate a matrix like below:

90.0 45.0 30.0 135.0 90.0 45.0 179.8 135.0 89.8

90.5 45.2 29.8 135.2 90.3 44.9 180.3 135.2 89.7

90.3 44.9 29.6 134.8 90.1 45.2 180.4 135.1 90.0

89.9 45.0 30.3 135.0 89.9 45.1 180.0 135.0 90.0

90.0 45.0 30.0 135.0 90.0 45.0 180.3 135.2 89.7

90.0 45.0 30.0 135.0 90.0 45.0 180.0 135.0 90.0

90.5 45.2 29.8 135.0 90.0 45.0 180.0 135.0 90.0

90.0 45.0 30.0 135.0 90.0 45.0 180.0 135.0 90.0

90.0 45.0 30.0 135.0 90.0 45.0 180.0 135.0 90.0

90.5 45.2 29.8 135.0 90.0 45.0 180.4 135.1 90.0

90.0 45.0 30.0 135.0 90.0 45.0 180.0 135.0 90.0

90.0 45.0 30.0 135.0 90.0 45.0 180.0 135.0 90.0

90.5 45.2 29.8 135.0 90.0 45.0 179.8 135.0 89.8

90.5 45.2 29.8 135.0 90.0 45.0 179.8 135.0 89.8

90.0 45.0 30.0 135.0 90.0 45.0 180.0 135.0 90.0

90.0 45.0 30.0 135.0 90.0 45.0 180.0 135.0 90.0

90.0 45.0 30.0 135.0 90.0 45.0 180.0 135.0 90.0

90.0 45.0 30.0 135.0 90.0 45.0 180.0 135.0 90.0

90.3 44.9 29.6 134.8 90.1 45.2 180.4 135.1 90.0

89.9 45.0 30.3 134.8 90.1 45.2 180.3 135.2 89.7

90.3 44.9 29.6 134.8 90.1 45.2 180.4 135.1 90.0

89.9 45.0 30.3 134.8 90.1 45.2 180.3 135.2 89.7

This matrix can be used as an access control matrix in the mobile system. And for the word recognition, the number of states N can be ranged from 5 to 12 for each model. So it can generate a much more complex and string enough access control matrix for the communication system's authentication task.

4.2 Hand drawing for user authentication

Although the handwriting may good enough to protect some wireless communication attack. But for some other attack such as dictionary attack, there may still has some flaws exist. So we thought maybe there is some improvement we can do for it.

Since Hidden Markov Model can be used for handwriting pattern recognition, so we thought could it used for the figures recognition? If we can use it in the figure pattern recognition, it will give more option to the user and also can protect our communication channels from tradition attack.

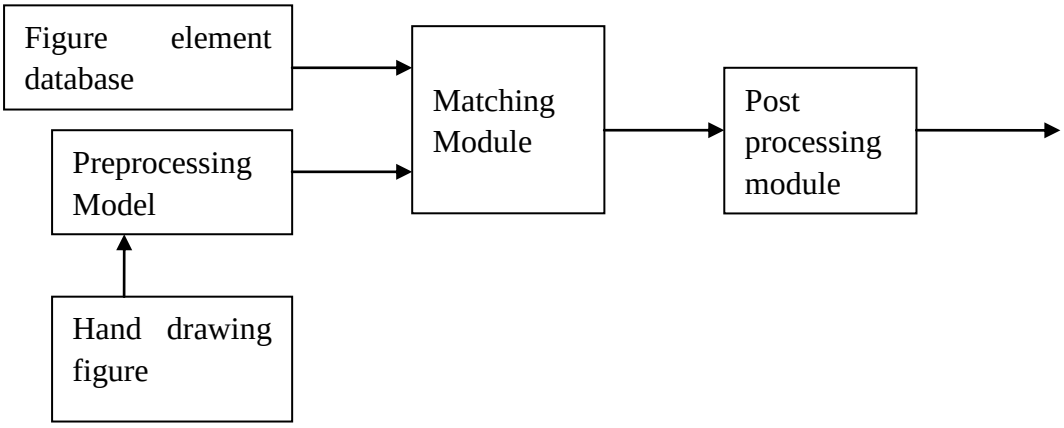

Figure 4.2 the process of hand drawing figure

We can see this process is very similar as the word recognition system. In the figure element database, it contains all kinds of regular elements that people used to draw a figure, such as circle, triangle, square or an arc and etc. and the matching module will identify the elements in a drawing figure and the logical position relationship between each element will also clarified, such as *object a is staying at the left of object B, object A and B is within the object C, and etc*. After that these information will send to the post processing module, and here will generate a zero-one matrix. This matrix will use for access control just like the word recognition task.

For the hand drawing figures on the pad we also need to isolate its element from each other and achieve a matching recognition. When we draw a simple figure like below:

We can see this is a very simple figure and we draw it very easily on our mobile device. So this hand drawing here contains four elements three circle and an arc. In this case we call the biggest circle circle 1 and eyes would be circle 2 for the left and circle 3 for the right. Arc will be numbered 4. For this figure here we can contribute a matrix[4] like this:

	circle	triangle	ellipse	square	arc	line
Circle 1	1	0	0	0	0	0
Circle 2	1	0	0	0	0	0
Circle 3	1	0	0	0	0	0
Arc 4	0	0	0	0	1	0

Table 4.1

So we can format a zero-one matrix for this hand drawing face. Besides this matrix, there is also a relationship list generated such as:

Object 2, 3, and 4 within object 1;

Object 2 is on the left of object 3;

Object 4 is under the object 2 and 3;

The distance of center point of object 4 to object 2 and 3 is almost equal.

For the objects position relation in the figure we can also use relation zero-one matrix to show this.

For the objects in-relationship, if one object is in another one we note it as 1 in the matrix. Otherwise it will be noted as 0.

	Circle 1	Circle 2	Circle 3	Arc 4
Circle 1	0	1	1	1
Circle 2	0	0	0	0
Circle 3	0	0	0	0
Arc 4	0	0	0	0

Table 4.2

Besides the in-out relationship matrix, we can also create relationship matrix for other position such as left-right, up-down.

Therefore, when in hand drawing pattern, its elements increase, the matrix will gets complex. We assume that we have a pattern contains 8 elements, so when we wants create matrix like Table 4.1, the total elements in that matrix should be more than 64, and for the relationship matrix, the elements in the matrix could also more enough. We can give a certain number here is because some times we may use dot in the figure, and also some other elements that can not contains elements in it.

We can see when we create these matrixes that contain more enough elements in it, and then these elements could be used for our password creation.

We use the zero-one matrix and these objects relationship to restrict a legal user’s password which is also a simple figure. And this is an efficient way to protect the malicious attack such as dictionary attack.

We here is only show a simple drawing figure with very simple matrix and its

relationship. Usually we can draw much more complex figure, and this could be an effective way to improve the protection of our communication. Because when the elements increase, the elements in the matrixes are also increase. This increment is directly influence the generation of the user's password. This means when the matrixes get complex the length of the password will also get longer.

So we can see when we use a hand drawing pattern as our authentication feature, we do not have to remember very long and password with irregular orders. What we do is just to draw a figure that we are good at, such as a simple smile face, or any other things. And the password generation will be the job of computer.

We have reasons to believe, that this way can be a totally new approach for today's mobile communication security. The figure can be a good replacement of tradition password. And it will be more randomly and dynamic, also hard to predict the password for the hacker.

Chapter 5 discussion

This master thesis is mainly work on the improvement of the mobile communication security especially authentication. And during the first period of the discussion we try to use the tradition way to solve this problem such as looking for a new authentication mechanism and key exchange protocols. But according to the experiment, many of them are not secure enough.

During the mid of this project, we come out the idea of using hand writing and drawing pattern recognition to solve this problem. Since nowadays, a lot of mobile device is capable to allow the user to input words by hand, so we think the data generated during the recognition process maybe used for our security improvement.

5.1 Pattern recognition for security improvement

For the tradition way of typing password to achieve system authentication, use pattern recognition will be an easy and secure option for the user.

Usually, to secure you account, we usually prefer to use long and complex password. But they are usually hard to memorize. Even we can remember it, sometimes malicious attacker still can figure out the password we use, such as dictionary attack.

But use pattern recognition; we can have aim a flexible dynamic password. And all we need to do is just input our signature or draw a simple figure as our password. And authentication information and channel encryption key generation will be the job of computers. Since every time, the signature we wrote down or the figures we draw is generally the same, so the different details can be used for the original source of dynamic keys generation. And also for the matrix's generation in handwriting characters recognition, when the matrixes are generally the same, the user's identity can be recognizing as the same user.

To sum it up, we use hand writing and drawing pattern recognition in mobile communication system can offered a more secure and individual information for one user. And also the different of the signature will also offer the system dynamic information for user's authentication and channel encryption. Therefore, we believe this can be a good solution to current mobile communication system's security issue.

5.2 Access control matrix

We can see in chapter 4, the matrix generated during the word recognition course can be very complex. So when more features extracted from the object, the matrix can be more complex. This offered us a very strong password which we don't have to take times to remember it.

For the figure pattern recognition, the security improvement would be directly connected with the figure we draw. When the figure gets complex, the matrix

and the relationship list would offered a strong protection for the communication systems. Also this can be a very good way to protect the users from the dictionary attack, because for a legal user, the element in his “password” can have much more choice compared with the characters.

So according to what we describe up, use patter recognition to generate access control matrix can be much more efficient way to improve the mobile communication system’s security.

Chapter 6 conclusion

We can see in this project, the combination of pattern recognition and modem mobile communication system can be a good application to improve the security of mobile communication. It can provide very flexible options for the user and complex and dynamic system security assurance.

For the future work, there still have some work to do.

First, for the hand drawing pattern recognition, collect the element, and training them is a big challenge. Different from the word we write, the figure we draw can contribute a very big database.

Second, for the element in the figure, there are also a lot of challenges, how to identify an element precisely is a very critical problem. When some elements overlaps or some relation is similar but nor clear enough, could computer recognize it and don’t make any mistake can directly influence the effect of system’s security [7].

Finally, the precise of recognition would be very important. Pattern recognition for hand writing and drawing is not only one mathematic model can solve this problem. So if we want to build up a really good system for security, some other tools need to be used to improve the accuracy of recognition.

Reference

[1] http://en.wikipedia.org/wiki/GSM#GSM_security

[2] Jochen Schiller, “Mobile communication”, second edition, 2003

[3] http://www.wirelessdevnet.com/articles/80211security/img2.gif

[4] Ralph P. Grimaldi, “Discrete and Combinatorial Mathematics”, third edition

[5] Mathew S. Gast, 802.11 Wireless Networks: The Definitive Guide, 2002

[6] Magdi A. Mohamed and Pail Gader, Generalized Hidden Markov Models

[7] Liu Gang, Zhang Hong-gang, Guo Jun, The handwriting number’s feature extraction base on HMM

[8] Liu Qiong, Zhou Hui-Can, Wang Yao-Nam, Optimum design for Gabor Parameters in handwritten numeral recognition

[9] Li San-ping, Yue Zhen-jun, realization of Handwrittern Numeral Recognition System Based on PNN with MATLAB

[10] Kannan Srinivasan, Stephen Michell, Performance of State Based Key Hop Protocol for security on Wireless networks

[11] Chen Zhuo, Hong Fan, Hong Liang, A New Authentication and Key Exchange protocol in WLAN

[12] Phongsak Prasithsangaree and Prashant Krishnamurthy, Analysis of Tradeoffs between Security Strength and Energy Savings in Security

Protocols for WLANs

[13] Mohit Virendra, Shambhu Upadhyaya, SWAN: A Secure Wireless LAN Architecture

[14] Lawrence O'Gorman, Irina Rabinovich, Photo-Image Authentication by Pattern Recognition and Cryptography

[15] Sabine Kröner, Andreas Latter, Authentication of Free Hand Drawing by Pattern Recognition Methods[16] Ozlem Guven, Selim Akyokus, Mitat Uysal, Aykut Guven, Enhanced Password Authentication Through Keystroke typing Characteristics

[17] Joon S. Park, Derrick Dicoi, WLAN Serucity: Current and Furure

[18] Franjo Majstor, WLAN Security Threats & Solutions