A Study on Jamming Vulnerability of Aeronautical Communication System Using Android Phone

Woo Bong Cheon*, Won Hyung Park**, Tai Myoung Chung*
*School of Information and Communication Engineering,
Sungkyunkwan University,
Chunchun-dong 300, Jangan-gu, Suwon, Kyunggi-do, Republic of Korea
cwb3242@naver.com, tmchung@ece.skku.ac.kr

**Industrial & Information Systems Engineering,
Seoul National University of Science and Technology,
172 Gongreung2-dong, Nowon-gu, Seoul, Republic of Korea
infosecure@seoultech.ac.kr

Abstract— **Recently, As a android phone offers more superior functions and interface than an existing traditional phone, the number of user has been increased rapidly. But, the number of vulnerable android phone in security has been rising due to customizing the system of android phone for the convenience of user. there are many cases of customizing the system. Simultaneously a number of android phones which vulnerable to security increase Exponentially. Also, the number of malware which targets android phone increases Annually, namely the threat has intensified. In this thesis, we suggest the techniques and countermeasures against the attacks which target Aeronautical communication system by modulation of Android phone RF module.**

Keywords- Malware; Android phone; Aeronautical Communication System; Frequency Modulation

I. INTRODUCTION

Recently, high performance of a cellphone by developed communication infrastructure and various requirements by users made a android phone appear. The android phone convergence is realized in our life as multiful interfaces and functions are provided from a android phone. The android phone with advanced ability rather than an existing phone is defined as the cellphone with a general operation system which is similar to PC. An existing traditional cellphone only can use fixed functions by manufacturers. On the other hand, a android phone can use customized functions by users such as a personal computing environment. As a matter of fact, user rights are expanded. These advantages of android phone make the number of android phone users in Korea increased rapidly. On 'diagram 1', the number of android phone users in 2010 increased by 5.24 million compared to 460 thousand in 2009. In all mobile communication users, android phone users in 2010 accounted increasingly for 12% compared to 1% in 2009. In other words, it increased by twelve times for a year. If the trend continues, most of mobile communication users will use a android phone.

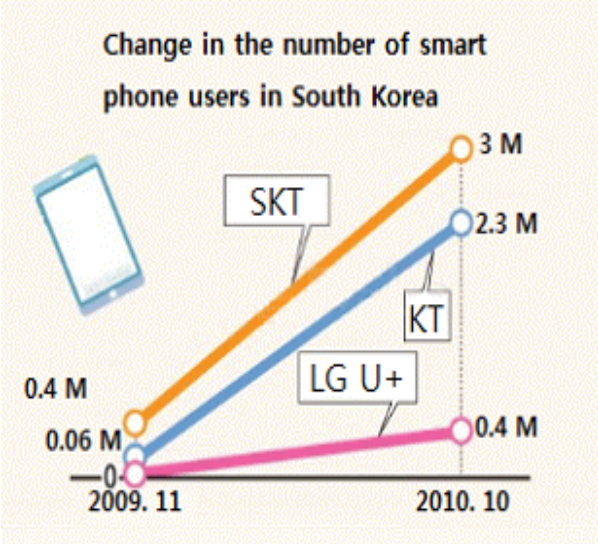

Figure 1. Change in the number of smart phone users[1]

However, a android phone has weakness to be exposed to a malware like a virus, worm which work on PC. Because a android phone has a similar environment with PC. Actually, F-Secure, antivirus firm based in Finland, demonstrated that virus for android phone can be produced as securing a proof of the concept code 'Cabir' from the virus producing group '29A'. After the emergence of 'Cabir', various malware has been being found and it threatens the environment of android phone with new strains of malware[2]. There is the table about android phone malwares which are arranged the appearance of android phone malware in chronological order [TABLE I] below.

978-1-4244-9224-4/11/$26.00 ©2011 IEEE

TABLE I. CASE OF ANDROID PHONE MALWARE[3]

Date	Malware Name	Number	Rate(%)
Jun. 2004	Cabir	14	7.7
Nov. 2004	Cdropper	17	9.4
Mar. 2005	Commwarrior	16	8.8
Sep. 2005	Cardtrap	20	11.1
Nov. 2005	AppDisabler	10	5.5
Mar. 2006	Singlejump	11	6.1
Mar. 2006	FlexiSpy	4	2.2
Mar. 2006	CommDropper	11	6.1
Jun. 2006	Romride	11	6.1
Dec. 2007	HatiHati	1	0.5
	etc	65	36.1
Sum	180		100%

Besides, some users modify settings of android phones to get more functions. that would threaten the security of android phones. 'jailbreaker' of iphone and 'rooting' of android are typical examples for that. Given this situations, the security of current android phones is very vulnerable now. Therefore this thesis suggests an imaginary scenario considering critical attacking techniques which force to modify the system of android phone. Also, it suggests a counterplan as analyzing the scenario. There are many android phone operation systems. But the thesis is focused on Android OS.

II. RELATED STUDY

A. The Structure Of Android

Android is a main application involving OS, middleware and JAVA even user interface for a mobile. The platform of android consists of software layers. The lowest layer is Linux kernel. And there is libraries with green field above linux kernel. The libraries work as native code on linux kernel. And there are the execution environment of an independent virtual machine 'Dalvik VM', application framework on a high layer and applications[4].

a) Linux Kernel

Android uses linux for management of internal memories, process, networking, OS service and so on. It doesn't show linux to android phone users and doesn't access to linux.

b) Library

Library is written in C and C++. It is already compiled for the hardware of the mobile by the supplier and already installed on the mobile. The kinds of libraries are surface manager, media codec, SQL database, browser engine and so on.

c) Android Runtime

Android runtime include 'Dalvik VM', Core java library, etc. the reason why Adroid runtime selects a independent virtual machine is that it is plural hardware architecture for internal use and an inevitable choice at this time which has an improved micro processor.

d) Application Framework

When an application is made in the framework, high level building block is provided. This framework is already installed on Android. If it needs, it can be expanded.

e) Application

This is the layer where user's codes are actually executed on the Android platform. The user of applications has no idea about lower layers.

A typical mobile phone communicates through a radio wave and is connected through a fiber optic cable on base stations, satellite, etc. That is '3G' way. A android phone uses '3G' and 'WiFi' method by mixture. The difference between 3G and WiFi is only access channel. Mostly they have a similar structure. The communication system of mobile phone is made up of the process like "Figure 3.". 3G method is to transmit the certain frequency of each base station to certain extent and a mobile device receive only the same frequency with a fixed frequency for the device. And the mobile device selects the base station with the strongest signal and transmits radio wave. And if the base station receives the radio, it would process registration to a switchboard. then, as transmitting the received radio wave, it would offer the wireless communication service to the users. Wifi method uses AP instead of a base station, it's basically similar to '3G'[5].

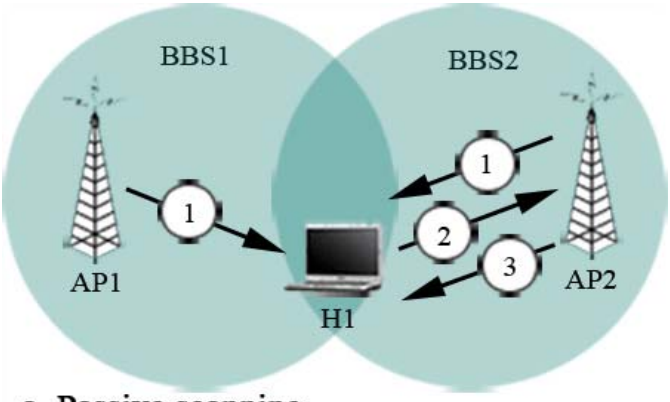

Figure 2. Process of AP Scanning[6]

In this process, the requirements of users are processed partitively at the same time. In the case of Korea, Korea uses CDMA(Code Division Multiple Access) way and other countries use GSM (TDMA, FDMA) way.

B. *Customizing of Android OS*

a) *Rooting*

Rooting is that the user of Android OS is a super user, which means to get the rights of an administrator. Rooting is origin from superuser's ID 'Root'.

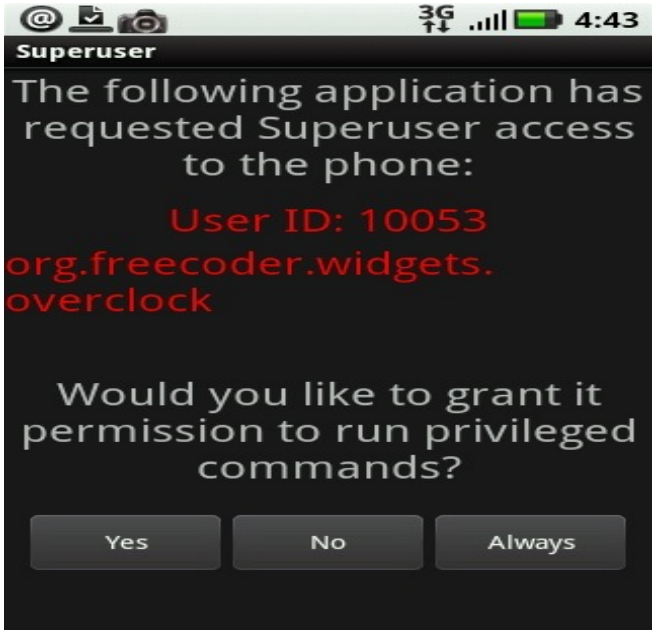

Figure 3. Rooting Application of Android

b) *Two sides of Rooting*

If you get superuser's access through rooting, you can access to a root folder which is below the layer of application. As a result, you can edit settings which was impossible to access and users can realize more functions. On the other hand, it's vulnerable to external attacks as it's possible to access to touchy system settings.

c) *Case of system customizing*

The user of Android OS can customize settings through rooting. Here is a main case of system customizing.

Figure 4. Flow of cpu Overclock

① Increase of processing speed by changing clock frequency of CPU
② Increase of I/O speed by changing format of flash memory embedded
③ Change of fonts randomly
④ Change settings to make volume be mute when taking a picture
⑤ Change positional value of keypad
⑥ Change logo of mobile carrier when booting or shutting down a android phone
⑦ Removal unnecessary applications device maker and mobile carrier provide

C. *Aeronautical Communication System*

a) *Structure of Aeronautical Communication*

The sensors for an automatic flight system consist of AHRS, ADS, GPS, RPM[7].

AHRS measures a pose, roll and acceleration.of an airplane. ADS measures airspeed, pressure altitude and normal speed. GPS measures the location of the airplane. Those sensors are basic information for automatic pilot.

The output signals of every sensor are connected to a sensor-based computer which would calculate the information for automatic pilot and transmit the condition of an airplane.

Among them, GPS prints out altitude, latitude, longitude, speed and heading information while in flight. The Positioning information can be exactly calculated as an exact time and distance from over 3 satellites is measured with a GPS receiver by the triangle method. Now, we usually use the way to get the time and distance information from 3 satellites and correct errors by a satellite.

b) *Structure of Aeronautical Communication*

The control tower in airport guides airplanes with GPS information from each airplain to prepare the accident from planes landing and taking off. And the plane lands by automatic pilot[8].

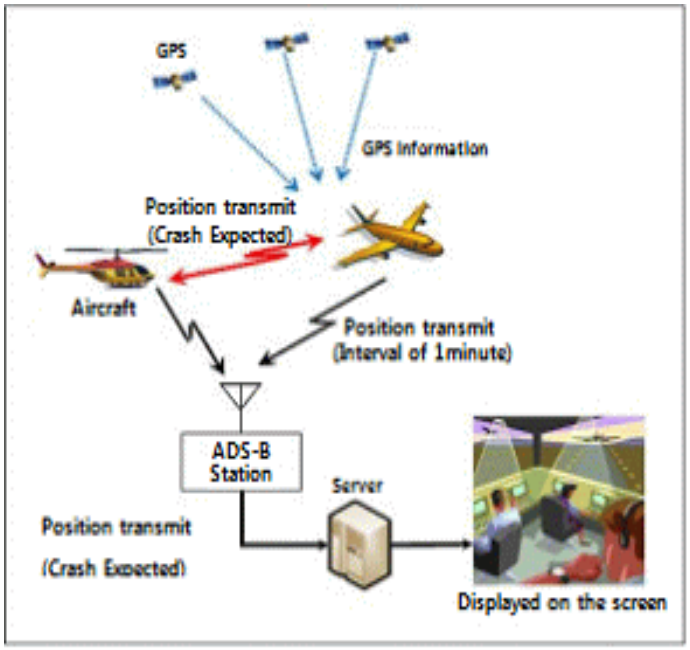

Figure 5. Aircraft ADS-B [9]

But, the frequency for GPS is normally 1.57GHz which is vulnerable to radio disturbance.

If an airplane falls into radio disturbance, the plane can't transmit GPS information. That makes an error in the positioning information and causes dangerous situations even like a collision. [TABLE II] below shows cases of accident by radio disturbance.

TABLE II. CASE OF ACCIDENTS HAPPENED BY JAMMING[9]

Date and Time	Contents
Aug. 1997	Korean Air crashed on landing in Guam and 229 people died
Apr. 2002	A Chinese civil aircraft crashed on landing in Gimhae and 119 people died
Jun. 2008	At O'Hare International Airport in Chicago, a plane failed to land first and landed successfully by making a second approach to airport
Jul. 2008	At International Airport in San Francisco, a plane failed to land first and landed successfully by making a second approach to airport
Mar. 2009	At International Airport in Incheon, a plane failed to land first and landed successfully by making a second approach to airport
Aug. 2010	North Korean attacked a South Korean with radio disturbance in some parts of the West Coast

III. RADIO DISTURBANCE THREAT OF AERONAUTICAL COMMUNICATION SYSTEM

A. *What is Jamming?*

The Jamming means to interfere with the airplane position on the radar, radio communication, wireless and radio navigation. It usually use to reduce the effect of long distance sensors or navigations. It is called 'Jamming' in English or radio disturbance. For this situation about jamming, current frequency bands are divided strictly and should be allowed by law in advance.

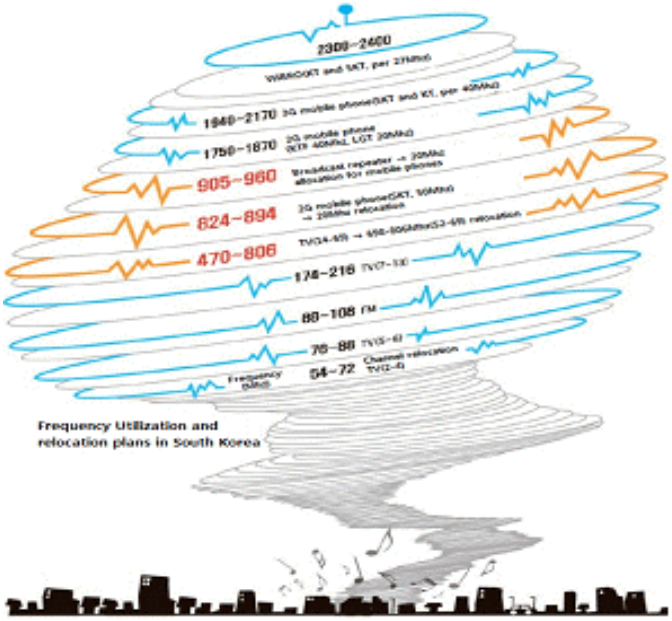

Figure 6. Frequency Utilization and Relocation plans in South Korea[11]

B. *Target of Jamming attack*

Back in October, there were reports from major communications about the deterioration of GPS in Gimpo, Munsan, Ilsan. Korea Communication Commision chased the radio dispatch as amplifying the radio. as result of the chase, the place of dispatch was Gaeseong of North Korea. The happening on October ended as a little inconvenience for the common users. But at that time, Kim Tae young, the minister of national defense, pointed out that North Korea has a Jamming ability and radio disturbance to GPS within the range of between 50 and 100 Km. Given the minister's comment, if the Korean war breaks out, Jamming attacks may cause critical results. Also, the jamming can interfere with communication between a control tower and a pilot in flight frequency bands. When an airplane sets up airway, the airplane needs the GPS information for altitude and coordinate. When jamming interferes with the radio of GPS information, the airplane can be off course or crash during landing and taking off[10].

C. *Jamming Attack Scenario*

Given those situations, jamming can make critical damages and edit system settings of android phones. For these reasons, the report suggests an ttack way. A mobile device generates little radio. but the more infected devices increase, the more the radio congestion increases rapidly like DDoS(Distribute Denial of Service) attack. The rough attack flow is on the "Figure 10." below and the process is as in the following.

- A modulation application installation to android phone with rooting.
- Confirmation whether the infected android phones are changed into flight mode or not and GPS information of the android phone users.
- If GPS information is the same with the fixed coordinate or if the communication is changed into flight mode, RF communication frequency is changed into GPS frequency(1.57Ghz) and Aeronautical frequency(108Mhz ~ 137Mhz).
- Radio modified Android phone emits noise radio continually to the frequency band.
- There is jamming caused by noise radio which is from the airplane and airport.
- Radio communication is cut off and a GPS coordinate is disagreement.
- It makes critical damages such as crash, getting out of the line.

Just modifying output frequency of RF communication module can be used as a tool for attack.

D. *Further Analysis of Attack Scenario*

The Mobile phone communicates with AP as generating radio wave. To make the radio, RF communication module, power amplifier and antenna are needed.

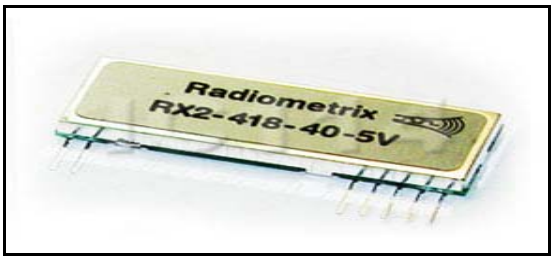

Figure 7. RF Communication Module

In RF communication module "Figure 7." it sets up the frequency band to generate and determine the strength of signal with a power amplifier. And the radio transmits through an antenna. Thus, to make jamming attacks, system setting for RF communication module of android phone should be modified. The communication algorithm of Android OS is conducted like "Figure 8."below.

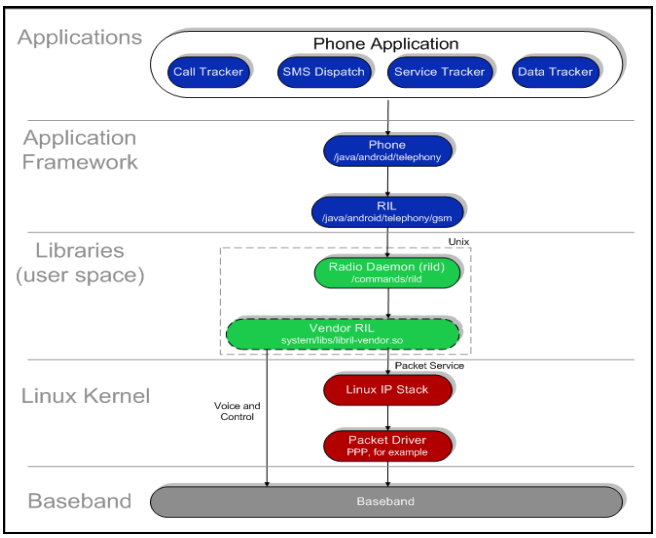

Figure 8. Communication Algorithm of Android OS[12]

The applications that the communication like Call, SMS, wireless internet of Android needs request to phone, RIL in the lower class which is the framework. RIL provides an abstract class for between communication service and hardware and processes wireless communication requests as referring RILd and Vendor RIL library. This library is a set of function. Therefore , it is possible to change into a flight mode as adding a bad function. And if the GPS coordinate is certain, the inserted function that loads the library can be conducted. And the control part of frequency of RF communication module. Is located in ROM that saves firmware. As modifying this part, it's possible to change the frequency.

IV. EFFECT OF ATTACK AND COUNTERMEASURES

A. *Ripple Effect of Attack*

Jamming attack is the way to interfere consistently in the wireless devices around the place of attack. So if we know the frequency band, the assumption that is possible to attack every communication equipment comes into existence. Now, usual wireless devices such as GPS, mobile phone, Navigation, Radio, wireless internet come into wide use. Development of wireless communications makes our life convenience, while the level of dependence on communications is high. Thus, users feel inconvenience when communication problem causes even for a while. Beside that, if a national communication problem takes place, it will causes great confusion.

B. *Technical Countermeasures*

Cause of jamming attacks is that user can modify system settings of android phone using softwares. Thus, which can control every hardware running. To cope with the attack, we have to focus on hardware not software because even if the attack is blocked in software, it can get around. The frequency output in the attack of RF communication module is abnormally modified. Therefore, the range of The frequency output of RF communication module should be limited to change frequency output using only the frequency band for the mobile.

V. CONCLUSION

This thesis analyzed the possible security threats in android phone environment and studied countermeasures based on analyzed results We could find out that android phone providing convenience in life can be an electronic bomb which threatens the equipment for wireless communication through this study. Therefore, users consider android phone as a computer and control the behavior that worsens a security of system and do not run nauthenticated applications. Also the authorities have to be on the alert for threats of android phone and analyze it in depth.

REFERENCES

[1] http://www.dt.co.kr/contents.htm?article_no=2010112302010351742002, Nov. 2010.
[2] http://www.f-secure.com/v-descs/bluetooth-worm_symbos_cabir.shtml
[3] http://www.f-secure.com/v-descs/mobile-description-index.shtml
[4] http://developer.android.com/guide/basics/what-is-android.html
[5] Bernard Sklar, Digital Communications 2th, Feb. 2004.
[6] James F. Kurose, Computer Networking 5th, Mar. 2009.
[7] http://think-tank.tistory.com/36
[8] Michael Schnell, Future Aeronautical Communications Concepts and Their Impact on ATM Procedures, http://www.b-vhf.org/b-vhf/doc/paper/2005/FullPaper_ATCA2005.pdf, 2005
[9] http://media.paran.com/news/view.kth?dirnews=3265736&year=2010&pg=1&date=20101020&dir=9
[10] http://100.naver.com/100.nhn?docid=761462
[11] http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=100&oid=001&aid=0004690243, Oct. 2010.
[12] K. Elissa, "Title of paper if known," unpublished.