IBBUL
Lapai Journal of Applied and Natural Sciences
LAJANS Vol 6(1): 231 - 235

REVIEW PAPER

Mobile Phone Cloning: A Conceptual Review

Siyaka, O.H., Oladipupo, E.T., *Pinmiloye, C.A., Duniya, G. D. and Muhammed, U.
Department of Computer Science, Federal Polytechnic, Bida, Nigeria,

ABSTRACT

Mobile phone cloning is the practice of taking the programmed information stored in a valid mobile phone and criminally programming the same information into another mobile phone. This cell phone piracy has become more prevalent in recent times and of course a matter of serious concern in the computing world since the rate at which it is used to commit crime is increasing at an alarming rate. Although, different detective measures such as duplicate location, velocity trap, radio fingerprint, usage pattern, call logs, smart pin code together with preventive measures such as phone password, creation of awareness on not to trust anybody, changing of password from time to time. Hackers are still having their ways and a lot of people are falling victim of this menace. This vulnerability of the unsuspecting phone users is due to the strong believed that those detective and preventive measures are strong enough to deter the hacker from lunching their attacks. From the review literature, it is obvious that the preventive and detective measures are not effective in stopping the hackers from their malicious activity; suggestion is therefore made on how hacker can be checked.

Keywords: Cloning, Piracy, Mobile Phone, ESN, MIN, GSM, CDMA

INTRODUCTION

Mobile phone cloning is the process of transferring the identity of one phone to the other, the intent most of the times is to commit fraud. Mobile phone cloning also known as cell phone piracy has been taking place throughout the world since decades (Manjula & Rajanna 2015). Mobile phones are essential parts of human life, they are easy to use, efficient and economical. One can hardly do without phones these days. It has also become an area of interest since a lot of revenue can be generated from it as lot of businesses depend on it.

In mobile phone cloning, the subscriber information taken from one phone is copied onto the other with the intention of obtaining free calls. The other mobile phone becomes the exact replica of the original mobile phone like a clone. As a result, when calls are being made from both phones, only the original phone is billed.

Millions of mobile phones users, be it GSM (Global System for Mobile Communications) or CDMA (Code Division Multiple Access) run at threat of having their phones cloned. As a mobile phone user if you have been receiving enormously high bills for calls that you never placed, chances are that your mobile phone has possibly been cloned. Unfortunately, the subscriber may not easily suspect that his/her phone has been cloned. But actions like call failing or anomalies in monthly bills can act as tickers (Akash et al, 2014). The cloner can set the options for his phones to ring when the victim makes a call, the victim in the other will have no idea that the cloner is listening to his conversation from their own mobile device. The cloner can read text message, phone book entries, look at pictures etc. Also, the cloner can dial phone numbers from his phone, and a whole lot more.

According to Eureka (2017), cell phone cloning started with Motorola "bag" phones and reached its peak in the mid 90′s with a commonly available modification for Motorola "brick" phones such as the Classic, the Ultra Classic, and the Model 8000. Cloning involved modifying or replacing the EPROM in the phone with a new chip, which would allow one to configure an ESN (Electronic Serial Number) via software. The MIN (Mobile Identification Number) would also have to be changed. After successfully changing the ESN/MIN pair, the phone would

Received 02 November, 2021
Accepted 13 December, 2021
Address Correspondence to:
christypinmiloye@gmail.com

become an effective clone of the other phone. Cloning only requires access to ESN and MIN pairs. And ESN/MIN pairs can be discovered in several ways: Sniffing the cellular network, trashing cellular companies or cellular resellers and Hacking cellular companies or cellular resellers.

With the high rate of phone cloning, many measures have been introduced over the years and techniques implemented to help solve the problem of phone cloning, but the rate of phone cloning seems to be on the high side. In this research works effort has been made to find information that would be handy for hackers to handle their attacks. Based on these findings, various measures were suggested that the users can put in place in addition to the detective and preventive measures against phone cloning are suggested:

1. introduce the concept of mobile phone cloning,
2. examine the consequence of mobile cloning,
3. discuss various measures that have been introduce and implemented to help solve the problem of phone cloning, and
4. argument the need for introduction of new possible ways of retrieving cloned phone

OVERVIEW OF MOBILE PHONE

How Mobile Phone Works

According to Akash, et al (2014), mobile phones send radio frequency transmissions through the sky on two distinct channels, one for voice communications and the other for control signals. When a mobile phone builds a call, it normally transmits its Electronic Security Number (ESN), Mobile Identification Number (MIN), its Station Class Mark (SCM) and the number called in a tiny burst of data. This burst is the short buzz you hear after you press the SEND button and before the tower catches the data. These four things are the components the cellular supplier uses to ensure that the phone is programmed to be billed and that it also has the identity of both the customer and the phone. MIN and ESN are collectively known as the 'Pair' which is used for the cell phone identification. When the cell site gets the pair signal, it determines if the requester is a valid registered user by comparing the requestor's pair to a cellular subscriber list. Once the cellular telephone's pair has been recognized, the cell site emits a control signal to permit the subscriber to place calls at will. This practice, known as Anonymous Registration, is carried out each time the telephone is turned on or picked up by a new cell site.

Types of mobile phone

1. GSM stands for Global System for Mobile communication
2. CDMA stands for Code Division Multiple Access

Difference Between GSM and CDMA

GSM stands for Global System for Mobile communication, while CDMA stands for Code Division Multiple Access GSM uses FDMA (Frequency division multiple access) and TDMA (Time division multiple access). GSM supports transmitting data and voice both at once, but CDMA have not this feature.

The main distinction between GSM and CDMA is that in GSM, the customer information is put on a SIM card which can be moved to a new mobile phone. Whereas only mobile phones from a set of whitelisted companies can be used with a CDMA network.

GSM Phones

Global System for Mobile Communications (GSM) is a digital cellular phone technology based on time division multiple access (TDMA). GSM phones use a Subscriber Identity Module (SIM) card that contains user account information. Any GSM phone becomes immediately programmed after plugging in the SIM card, thus allowing GSM phones to be easily rented or borrowed. Operators who provide GSM service are Airtel, Hutch etc.

In their work, (Mishra & Nilesh, 2014) said that mobile service providers needed to secure their networks from attack and misappropriation of networking resources. In the attempt to achieve the goals set out in GSM of protecting access to mobile services and to protect any relevant item from being disclosed on the radio path; the GSM security protocols were developed. There are many technical constraints that are needed to be addressed when adding security to mobile communication. When authenticating against a mobile wireless network, the mobile equipment needs to be able to send from one base station to another without a loss of communication or interruption to an active connection. The

requirement to roam without interruption was a major factor in development of mobile networks that would allow a user to be able to authenticate to and use all parts of the network seamlessly. A major difficulty faced by mobile networks is the ability for a user to roam from one network to another network operator which allows mobile network providers to bill foreign users and systems. The authentication protocol deployed to address these problem was the SIM based GSM protocol. In GSM networks, a mobile station is connected to visit network by several radio link to a particular base station.

CDMA Phones

CDMA is a method for transmitting simultaneous signals over a shared portion of the spectrum. There is no Subscriber Identity Module (SIM) card unlike in GSM. The digital cellular standard for CDMA is developed by Qualcomm. CDMA is a 2G mobile telecommunications standard. In CDMA, the same frequencies are allocated to share multiple radios links. It is a type of multiplexing which is used to optimize the bandwidth of single channel. CDMA is a form of multiplexing, which allows several signals to optimize the available bandwidth. (Aaruni et. al, 2012).

Electronic Serial Number (ESN)

The unique identification number according to Eureka (2017), is embedded in a wireless phone by the manufacturer. Each time a call is placed, the ESN is automatically transmitted to the base station so the wireless carrier's mobile switching office can check the call's validity. The ESN cannot easily be altered in the field. The ESN differs from the mobile identification number, which is the wireless carrier's identifier for a phone in the network. MINs and ESNs can be electronically checked to help prevent fraud and features. Each ESN is a 32-bit number consisting of three fields: a manufacturer code (eight bits), a unique serial number (eighteen bits), and an extension (six bits). In practice, the serial number and the extension have actually been combined into one 24-bit serial number to identify each mobile unit. Under this assignment format, 256 manufacturers could be distinguished by ESN. But when this number proved insufficient, the 32-bit ESN assignment was altered to reflect a 14-bit manufacturer code and an 18-bit unit identification number.

Mobile Identification Number (MIN)

The Mobile Identification Number (MIN) (Eureka, 2017) is a number that uniquely identifies a mobile telephone subscriber. MINs are 34-bits in length. The first 10 bits are sometimes known as MIN2, while the last 24 bits are referred to as MIN1. Together they are simply known as the MIN.

PROCESS OF PHONE CLONING

How ESN/MIN Are Detected

Cellular thieves can capture ESN/MINs using devices such as cellphone ESN reader or digital data interpreters (DDI). DDIs are devices specially manufactured to intercept ESN/MINs. By simply sitting near busy roads where the volume of cellular traffic is high, cellular thieves monitoring the radio wave transmissions from the cellphones of legitimate subscribers can capture ESN/MIN pair. Numbers can be recorded by hand, one-by-one, or stored in the box and later, downloaded to a computer. ESN/MIN readers can also be used from inside an offender's home, office, or hotel room, increasing the difficulty of detection (Manjula & Rajanna, 2015).

How ESN/MIN Are Programmed On Another Phone

To reprogram a phone, the ESN/MINs are transferred using a computer loaded with specialized software, or a “copycat” box, a device whose sole purpose is to clone phones. The devices are connected to the cellular handsets and the new identifying information is entered into the phone. There are also more discreet, concealable devices used to clone cellular phones. Plugs and ES-Pros which are about the size of a pager or small calculator do not require computers or copycat boxes for cloning. The entire programming process takes 10-15 minutes per phone (Manjula & Rajanna, 2015).

Cloning A Mobile Phone

Each mobile phone has a specific broadcasting fingerprint in its transmitted information signal. This fingerprint is very unique for a particular number. This print does not get altered even if the user changes MIN or ESN number. The

process of Cloning access ESN and MIN pair in following ways to make a success:

a. Sniffing of radio waves sniffing devices.

b. Usage of garbage of mobile phones or hacking of mobile phone service Provider Company.

c. Breach the security to gain unauthorized access in mobile companies.

Cloning Gsm Phones

Cloning has been shown to be successful on code division multiple access (CDMA) but more difficult on the Global System for Mobile (GSM). GSM is one of the most widely used mobile telephone communication systems. However, cloning GSM phones is achieved by cloning the SIM card contained within, not necessarily any of the phone's internal data. Cloning of GSM mobile is a rare process. It is one of the reasons that make GSM phone more popular as cloning of such mobile is only possible through the cloning of SIM card inserted into it. The main reason for this is that these phones do not have ESN or MIN number. They only have IMEI number. SIM can be copied by removing the SIM card and placing a device between handset and SIM card to extract KI or secret code. This process may take a few days. The process of cloning in GSM mobile phone is a tough process so it is being a research area for researchers.

Cloning For CDMA Mobile Phones

CDMA clone transfers all the user setting and data from original legitimate phone into fraudulent phone that is indistinguishable in make and firmware version. In CDMA mobile, the EPROM (Erasable Programmable Read-Only Memory) is replaced with a new chip with new configured ESN by the use of software. The second step is to change the MIN and to make a successful ESN/MIN pair. This pair sometimes pronounced as Mobile Equipment Identifier (MEID). The ESN/MIN is transmitted to cellular company to authenticate device into mobile network. After making this modification, the mobile phone PRL and number itself or MIN number can pave the way for fraudulent calls, as the target mobile phone is now the clone of the mobile phone from where the original ESN and MIN numbers are obtained. Cloning in CDMA mobile requires ESN and MIN pair. The figure below shows a typical pictorial view of how a phone is cloned.

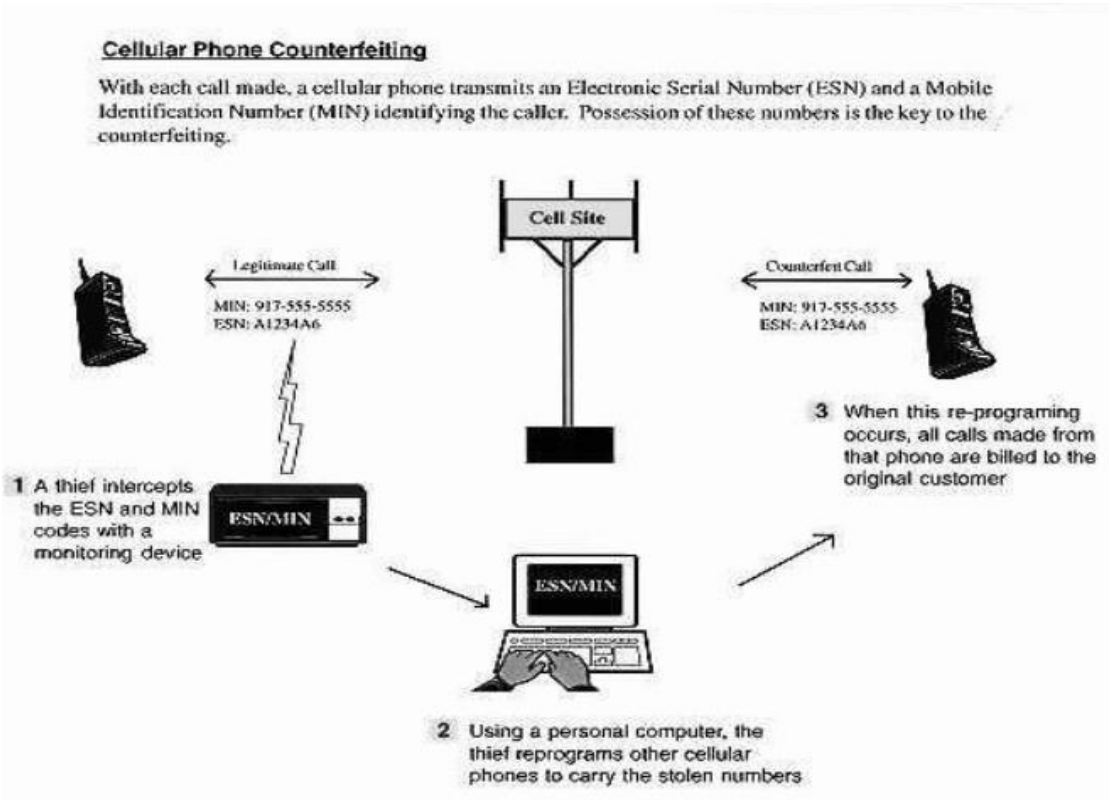

Figure 1: Cellular Counterfeiting/Cloning Fraud. Source: (Manjush *et al.,* 2013)

METHODOLOGY

The following are the method we use in getting these report

i. Online research
ii. Reference to different journals
iii. Personal interview with some colleagues

Detection of Phone Cloning

These are the different ways of detecting a suspected cloned phone given by (Sonal&Upasna, 2015)

i. When there is duplicate Location

This is also called duplicate detection. When a service provider discovers that the same phone is used in several places at the same time. The service provider may shut down the network and wait for the legal user to respond back to the service provider. At this point, the ESN/ MIN can be reprogrammed resulting in detection of the false user. The only loophole in this system is that it is very much difficult for the service provider to trace out the duplicates.

ii. Velocity Trap

This is almost like the first one above, but in this case, if the location of the phone is continuously changing or the location is too far away from last call within the seemingly impossible amount of time, then it falls under velocity trap. For an example, if first call is made from Nigeria and another is made from Canada within sixty minutes, or if the calls are encountered from Lagos and another from Owerri within three minutes, Velocity Trap is suspected.

iii. Radio Fingerprint

This is the process of identifying a cellular phone or any other device by a unique "fingerprint" that characterizes its signal transmission. The identification of a wireless device is done by the electronic fingerprint detected due to its unique radio transmission characteristics. Cellular operators use Radio fingerprinting to prevent cloning of mobile phones. When a phone is cloned, it will have a similar numeric equipment identity but a different radio fingerprint.

iv. Usage Pattern

This can be called usage profiling. When the usage patterns of the users are studied, any obvious differences can be noted, and the original authenticated user is contacted. For instance, if a user is normally known for local calls and suddenly or a call is tracked immediately from foreign country, then it's possible the phone has been cloned.

v. Call Logs

Every phone keeps records or logs of calls it has been used for since purchased. Every service provider also keeps the same logs. If the logs from the service provider and the user's logs are not matched, then chances are that the phone has been cloned.

Note that call logs is also known as call counting.

vi. Smart PIN Code

This is a case where the service provider assigns a smart PIN (Personal Identification Number) code to an authentic user. The authentic user will request for service privilege from service provider and temporary suspension of service before and after each call respectively. This PIN code is normally shared by authenticated user and service Provider. The encryption standards and the security algorithms, can be implemented on this PIN rather than ESN/MIN Pair.

How To Prevent Cloning

These are some preventives measures out listed by (Eureka, 2013).

1. Service providers have adopted certain measures to prevent cellular fraud. These include encryption, blocking, blacklisting, user verification and traffic analysis.
2. The software also determines whether it is physically possible for the subscriber to be making a call from a current location, based on the location and time of the previous call.
3. Traffic analysis detects cellular fraud by using artificial intelligence software to detect suspicious calling patterns, such as a sudden increase in the length of calls or a sudden increase in the number of international calls.
4. Suggestive Factors That Indicate That A Phone Has Been Cloned
   a) The owner of the mobile phone will notice recurrent phone calls from wrong numbers.
   b) Receiving messages from wrong numbers.
   c) Call breaching

d) There will also be difficulty in making calls even when there is sufficient network.
e) Continuous receipt of line busy signals when trying to place calls
f) There will be prevalent difficulty in receiving calls or voice messages.
g) Anomalous transactions not initiated by the rightful phone user.
h) Outrageous call bills from service providers.
i) Inconsistent bills for an unknown transaction.

Cell Phone Cloning- Possible Preventive Measures

Here are possible number of ways in which one can prevent his/her phones from being cloned. They include:

a) Crosscheck your bills either daily weekly or even monthly to ensure there are no much variations in the bills. You may wish to contact your service provider.
b) Saving of highly classified information in mobile phones should be minimized.
c) Ensure that all your mobile phones are under insurance by the company policy.
d) Use of password to secure your phone.
e) You really don't have to trust anybody with your phone
f) Change your phone password from time to time.
g) Use more of GSM phones than CDMA phones if you can't be too careful as CDMA phones are more difficult to clone.

Observations

Despite the different preventive and detective measures that were introduced by different researchers in the reviewed works, the hackers are still having their ways in cloning peoples phone by coming up with new ways and techniques day by day. It was observed that frequent changing of phone password by phone users has help in reducing hackers access incarryingout their criminal act, and also, user's mobile phones been under insurance by the company policy have help in reducing the attack of mobile phone cloning.

Suggestions

The following measures are suggested to help reduce the high rate of phone cloning.

a) Phone users should frequently change their phone password
b) Phone users should put their phone under insurance company
c) There should be need for further research by software engineers on how the problem of phone cloning can be reduced or possibly halt.

Conclusion

This paper has examined the concept of phone cloning, its consequences, and possible ways of detecting a cloned phone and also suggested a number of preventive measures for the aversion of this crime. Hence, it must be considered that the various preventive and detective measures which is currently used is not fruitful enough to secure the system in future. So it is very important to verify the working of security system time-to-time and also must change or update it over every month or year once. The software engineers should come with more Preventive steps, it should be taken by the network provider and the government the enactment of legislation to prosecute crime related to cellular phones is not viewed as a priority.

REFERENCES

Aaruni Goel, M. S. (2012). The Approaches to Prevent Cell Phone Cloning in CDMA. *International Journal of Computer Applications (09 75-8887) volume 45-No. 21*, p.16.

Akash, K., Mahato, K. & Akashdeep, S. (2014). Mobile Phone Cloning. *International Journal for Research in Applied Science and Engineering Technology (ijraset)*, p.224.

Anandkumar, K.M. & Jayakumar, C. (2012). Pro-Active Prevention of Clone Node Attacks in Wireless Sensor Networks. Journal of Computer Science 8 (10): 1691-1699, 2012 ISSN 1549-3636.

Barbera, M.V. & Mei, A. (2012). Personal Marks and Community Certificates: Detecting Clones CDMA Technology. *International Journal of Innovative Research in Computer and Communication Engineering*, p.11.

Cellular Telephone Cloning Final Report (2000). Economic Crimes Policy Team United States

Cloning: History, Present Scenario and Precautionary Techniques. *International Journal of Application or Innovation in Engineering & Management (IJAIEM) ISSN 2319*, p.4.

Culler, D., Estrin, D. & Srivastava, M. (2004). "Overview of Sensor Networks", IEEE Computer, Development Group, 575 Anton Boulevard, Suite 560 Costa Mesa, California 92626. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, p.3846.

Eureka .S. (2017). Mobile Phone Cloning. *International Journal of Scientific & Engineering*

Fernando Augusto da Silva Cruz Bernardo Gonçalves Riso Carlos Becker Westphall Federal University of Santa Catarina (UFSC). *International Journal of Computer Applications (09 75-8887) volume 45-No. 21*, p.16.

K.M, C. Jayakumar Journal of Computer Science 8 (10): 1691-1699, 2012 ISSN 1549-3636.

Karl, H. & Willig, A. (2012). Protocols and Architectures for Wireless Sensor Networks, John Wiley in Wireless Mobile Social Networks, Distributed Computing in sensor Systems (DCOSS), 2012 IEEE 8th International Conference, Page (s):83 –91. *International Journal for Research in Applied Science and Engineering Technology (ijraset)*, p. 224.

Manjula, D. & Rajanna, M. (2015). Implementing Mobile Phone Cloning in GSM

Martinez, K., Hart, J. K. & Ong, R. ( ). "Environmental sensor networks", IEEE

Mishra, S. & Nilesh K. M. (2014). False Base Station Attack in GSM Network

Mislan, R., Casey, E., & Kessler, G. (2010). The Growing Need for on - Scene Triage of

Mobile Devices. *Journal of Digital Investigation*, p.6.

Murphy A. (2012). The Fraternal Clone Method For CDMA Cell Phones International Journal

Networks (WOCN), 2010 Seventh International Conference in Sept, 2010.

Nidhi,T. & Sachin, C. (2015). Mobile Phone Cloning.

Notare, M.S.M.A. ; Boukerche, A. ; Cruz, F.A.S. ;Riso, B.G. ;Westphall, C.B. (1999). "Security management against cloning mobile phones" Global elecommunications Conference, 1999. GLOBECOM '99 Page(s): 1969 - 1973 vol.3.

Notare, M.S.M.A.; Boukerche, A. ;Westphal, C. (2000). "Safety and security for 2000 telecommunications"EUROCOMM 2000. Information Systems.

Notare, M.S.M.A., DaSilva Cruz, F.A, Riso, B.C. & Westphall,C.B, (1999).Wireless Pro-Active Prevention of Clone Node Attacks in Wireless Sensor Networks. *Volume 8, Issue 5*, p.24.

Jyhi-Kong, W.; Han-Tsung, C.; Lir-Fan, S.; Wei-Peng, Y., (1995). "Clone terminator: an authentication service for advanced mobile phone system" Vehicular Technology Conference, 1995 IEEE 45th , vol.1Page(s): 175 - 179

Ren, Y.; Chen, Y. & Chuah, M. C. (2012)."Social closeness based clone attack detection for mobile healthcare system" Mobile Adhoc and Sensor Systems (MASS),2012 IEEE 9th International Conference Page(s): 191 – 199.

Riso, B.C. & Westphall,C.B. (2000). Security Management against Cloned Cellular Phones. Federal University of Santa Catarina (UFSC): Sankaranarayanan ,"Mobile phone cloning", Wireless And Optical Communications

Science and Engineering (ICISE). 2nd International Conference, Page(s):4277–4280,

Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438, p.350. *Security in the GSM network*byMarcin Olawski*CDG Document 138 Version 0.34* CDMA

Security Management against Cloned Cellular Phones: Mirela Sechi Moretti A noni Notre

Sentencing Commission , January 25, 2000 Computer Applications Volume 45 No.2 May 2012 [online] Available at : https://www.movzio.com/howto/cell-phone-cloning-guide/ Sentencing Commission

Small Scale Digital Device (2009) Forensics Journal, Vol. 3, No. 1, June 2009 ISSN 1941-

Son, B., Her, Y. & Kim, J. (2006). A design and implementation of forest –fires surveillance.

Talmale, M., Kinhekar, A., Saraf, A. & Bhajan, M. (2013). Mobile Phone

telecommunications networks Mobile Computing, IEEE Transactions on Volume: 1 , Issue: 2 , Page(s): 123 – 131

Wiley and Sons, Inc., New York, NY, USA, second edition, (1996). wireless sensor networks for South Korea mountains", International journal of Computer Science and Network Security (IJCSNS), 6, 9 124-130, 2006. Wireless Sensor Networks. Journal of Computer Science, 8 (10): 1691-1699, 2012 ISSN 1549-3636.

Wu, S. B. & Li, C. S. (2010). A method of USIM anticloning in LTE/SAE, Information

Yi-Bing, L., Ming-Feng, C. & Rao, .C.H. (2002). Potential fraudulent usage in mobile phone.