www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 4 April 2015, Page No. 11153-11156

Security measures for CDMA Mobile Phone Cloning

S.Kanimozhi, D.Lavanya, S.SivaChandiran, D.Jayakumar
PG Student
Department of Computer Application
IFET College of Engineering

***Abstract**: Mobile phone cloning is a technique wherein security data from one mobile phone is transferred into another phone. The other mobile phone becomes the exact replica of the original cell phone like a clone. As a result, while calls can be made from both phones, only the original is billed. Though communication channels are equipped with security algorithms, yet cloners get away with the help of loop holes in systems. So when one gets huge bills, the chances are that the phone is being cloned.(1) Cloning CDMA cell phones(2)A Pattern Recognition Technique is used to classify the telephone users into classes in order to identify if a call does not correspond to the patterns of a specific user; and (3) Distributed Object Technique is used for the implementation of this distributed system (i.e., manager and agents).*

Keywords: CDMA, Distributed Management, Telecommunication Security, Formal Description Technique, Pattern Recognition, CORBA.

1. INTRODUCTION

The main objective is to augment the security in telecommunication networks, avoiding frauds of cloned mobile phones. In order to program a non genuine mobile cloned phone, for instance to debit calls from a genuine mobile phone, one only needs to buy a piece of portable radio equipment called a scanner, which registers the frequency in which mobile phones operate in its immediate surroundings. The person committing the fraud may, for example, park his car around a shopping center, jot down various frequencies, transfer the data to clones and then pass them on to whom ever may be interested.

According to media reports, recently the Delhi (India) police arrested a person with 20 mobile-phones, a laptop, a SIM scanner, and a writer. The accused was running an exchange illegally wherein he cloned CDMA based cell phones. He used software named Patagonia for the cloning and provided cheap international calls to Indian immigrants in West Asia.

Pattern recognition techniques are used to classify the telephone users into classes according to their usage logs. Such logs contain the relevant characteristics for every call made by the user. From this classification it is easier to identify if a call does not correspond to the patterns of a specific user, and thus, identify whether the call was effected by a non-genuine caller. As a consequence, the immediate identification of a fraud (as opposed to the moment of receiving the monthly bill) will reduce losses for both users and carriers. With this software, neural network algorithms (such as k-means, p-nearest neighbour and gauss) are implemented. Moreover, due to the characteristics of the telecommunication networks – distributed and heterogeneous –the system uses the CORBA architecture. The ODP/OMG CORBA (Open Distributed Processing/Object Management Group Common Object Request Broker Architecture) is a management technology for distributed objects

2. CLONING CDMA CELL PHONES

Mobile telephone thieves monitor the radio frequency spectrum and steal the cell phone pair as it is being anonymously registered with a cell site. The technology uses spread-spectrum techniques to share bands with multiple conversations. Subscriber information is also encrypted and transmitted digitally. CDMA handsets are particularly vulnerable to cloning, according to experts. First generation mobile cellular networks allowed fraudsters to pull subscription data (such as ESN and MIN) from the analog air interface and use this data to clone phones. A device called as DDI, **Digital Data Interface** can be used to get pairs by simply making the device mobile and sitting in a busy traffic area (freeway overpass) and collect all the data you need. The stolen ESN and EMIN were then fed into a new

CDMA handset, whose existing program was erased with the help of downloaded software. The buyer then programs them into new phones which will have the same number as that of the original subscriber.

2.1. CDMA PARAMETERS

ESN (Electronic Serial Number)

Every mobile on the system is uniquely identified by the Electronic Serial Number (ESN) which is a 32 bit number pre-programmed at factory setting by the mobile phone manufacturer. The ESN is used to identify a mobile on the network.

MIN (Mobile Identification Number)

The Mobile Identification Number (MIN) is a 10 digit number that is assigned by the Service Provider to a mobile on the network. This too is unique to each mobile on the network and is used in conjunction with the ESN to identify the mobile on the network.

MDN(Mobile Directory Number)

The Mobile Directory Number(mdn) is another 10 digit number which is assigned by the service provider to a mobile on the network. This is the number which is known to the outside world as the user's mobile number. Cloning is a malicious process whereby a rogue intruder in the system assigns an unauthorized pair of ESN and MIN to a mobile phone thereby pretending to be a genuine user and try and break into the network.

3. MOBILE PHONE SECURITY MEASURES

 Using spread spectrum, the traffic between the signal transmissions over a cell coverage area can be reduced. Such that the tracing of signal could be reduced.

 Using pattern recognition the neural network can be defined as a processor distributed massively in parallel and which has the natural propensity to store experimental knowledge and make it available for use.

 Combination of CDM and FDM would increase security through splitting the frequency channels.

 Utilization of COMP128 authentication algorithms would increase the efficiency of encryption of signals.

 Encryption of ESN/MIN before passes through the mobile station controller (MSC).

 Writing individual code for every spitted frequency of the channel will also reduce the cell phone clone.

 Comparison of station class mark before processing the signal transmission between

 the paired mobile users.

3.1. PATTERN RECOGNITION

Neural network(when seen as an adaptive machine) can be defined as a processor distributed massively in parallel and which has the natural propensity to store experimental knowledge and make it available for use. It is similar to the mind in two aspects: (1) Knowledge is acquired by the network by means of the learning process. (2) The weights of the presently, this specification is being validated and translated to code.

3.2. AUTHENTICATION ALGORITHMS

3.2.1. A3, the MS Authentication Algorithm

The authentication algorithm used in GSM security model is A3. Its function is to generate the SRES response to the MSC's random challenge, RAND, which the MSC has received from the HLR. The A3 algorithm generates a 32 bit output known as the SRES response after it gets the RAND from the MSC and the secret key Ki from the SIM as input. Both the RAND and the Ki secret are 128 bits long.

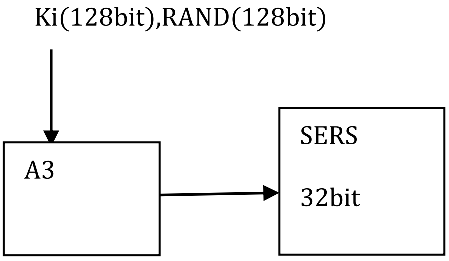


Fig 1.A3 Algorithm

Nearly every GSM operator in the world uses an algorithm called COMP128 for both A3 and A8 algorithms. COMP128 is the reference algorithm for the tasks pointed out by the GSM Consortium. The COMP128 takes the RAND and the Ki as input, but it generates 128 bits of output, instead of the 32-bit SRES. The first 32 bits of the 128 bits form the SRES response.

3.2.2. A8, the Voice-Privacy Key Generation Algorithm

The key generation algorithm used in GSM security model is the A8 algorithm. The A8 generates the session key, Kc, from the random challenge, RAND, received from the MSC and from the secret key Ki. The A8 algorithm generates a 64- bit output from two 128 bits input. This output is the 64-bit session key Kc. This is the same Kc which the BTS receives from the MSC. HLR is able to generate the Kc, because the HLR knows both the RAND (the HLR generated it) and the secret key Ki, which it holds for all the GSM subscribers of this network operator. One session key, Kc, is used until the MSC decides to authenticate the MS again. This might take days.

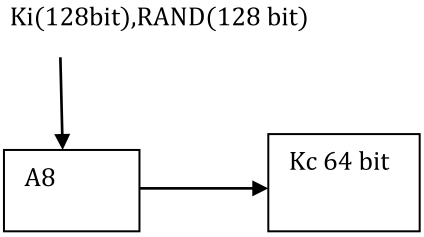


Fig 2. A8 algorithm

Both the A3 and A8 algorithms are stored in the SIM in order to prevent people from tampering with them. This means that the operator can decide, which algorithms to use independently from hardware manufacturers and other network operators.

3.2.2. An Authentication model

An Authentication model is best represented by shown below. As soon as the User desires some service from the Serving System a random number is thrown at it from the Serving System as a Challenge to authenticate itself. The User uses this random number and performs a cryptographic algorithm on it using a Secret Key which is known at both ends. The same process is carried out at the Serving System using the same cryptographic algorithm and Secret key. The resultant output from the User side is given to the Serving System as a Response. The Serving System compares the response with its own computation. If the two match the User is either permitted access to Services or is denied entry.

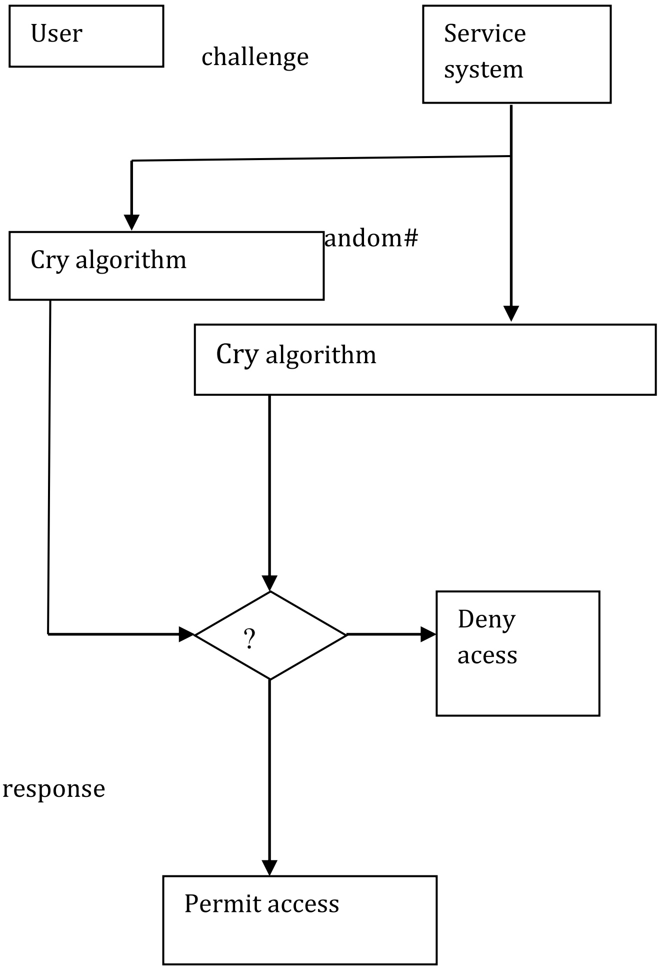


Fig 3.Authentiction model

4. PATTERN MATCHING ALGORITHM

Step 1: at the first level of connections of a radial base network, one must first of all identify the number of neurons of the hidden layer;

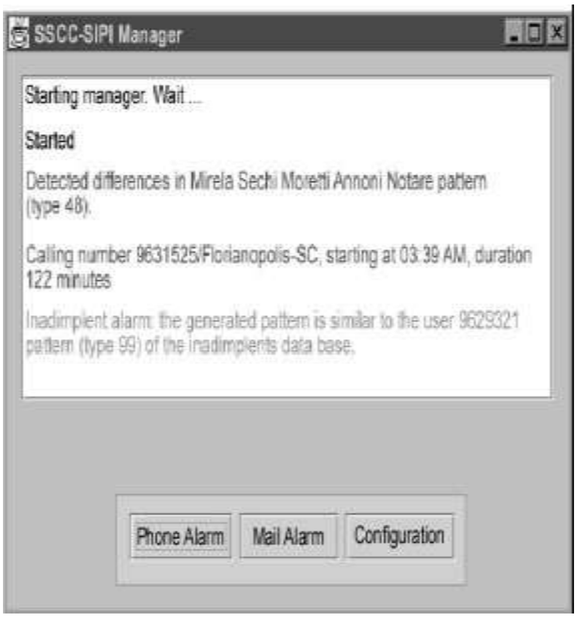
Step 2: next the centers cj are found (j=1,.....,M) which make-up the base of an M-dimensional space.

Step 3: for each presented input pattern for, which describes the level of classification of the input patterns. Step 4: the output is calculated as a sum of the activated neurons (excited neurons) of a hidden layer. The K-means and P-nearest neighbor algorithm were used to obtain the centers and radiuses of each cluster and variance between the centers, respectively.

Step 5:The Gauss function was used for obtaining the output of a hidden layer (centers data, input patterns and radii) and a linear function (denoted *purelin*) contained in the neural Toolbox.

5.IMPLEMENTATION

The implementation used Java Development Kit(JDK), and Visibroker 3.1. JDK includes the necessary tools to compile, refine and execute applets and application written in Java language. Visibroker 3.1 for java is a software that integrated CORBA and Java technologies, allowing the implementation of client-server applications, written in Java . Java was used because it is simple object oriented language, architecture independent, portable, multi-task, dynamic, robust, secure and offers high performance.



```
Starting manager. Wait ...

Started

Detected differences in Mirela Sechi Moretti Annoni Notare pattern
(type 48).

Calling number 9631525/Florianopolis-SC, starting at 03:39 AM, duration
122 minutes

Inadimplent alarm: the generated pattern is similar to the user 9629321
pattern (type 99) of the inadimplents data base.
```

In the Figure shows that the Manager receiving alarms from the Agents about possible frauds. Then the Manager will be able to detect if this altered pattern matches with an existent impostor pattern, and also, to send immediately a warning to the user, by phone and by mail.

6. CONCLUSTION

Existing cellular systems have a number of potential weaknesses that were considered. It is crucial that businesses and staff take mobile phone security seriously. Mobile Commerce, Mobile Banking and other Financial transaction applications over the mobile will require high level of security which can be provided for by the CDMA networks when the CDMA message signaling encryption is enabled. In addition the networks can check on the fraudulent use of their networks by preventing cloning of the mobile phones by enabling Authentication procedures on the network. Awareness and a few sensible precautions as part of the overall enterprise security policy will deter all but the most sophisticated criminal. It is also mandatory to keep in mind that a technique which is described as safe today can be the most unsecured technique in the future.

Therefore it is absolutely important to check the function of a security system once a year and if necessary update or replace it. Finally, cellphones have to go a long way in security before they can be used in critical applications like m-commerce.

7. REFERENCES

[1] D.S. Alexander; W.A. Arbaugh; A,D. Keromytis; J.M.

Smith. “Safety and Security of Programmable Networks Infrastructures”. IEEE Communications Magazine. Vol. 36.
N10, Oct98. Pp. 84-92.

[2] G. McGraw, E. Felten. *Java Security*. Ed. Wiley, 1997.

[3] G. Pavlou. *From Protocol-based to Distributed Objectbased Management Architectures*. DSOM 97. Australia, pp. 25-40, 1997.

[4] W. Stallings. *Network and Internetwork Security – Principles and Practice*. IEEE Press. Prentice-Hall. IEEE, pp. 462, 1995.