ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 10, Issue, 04(C), pp. 31834-31839, April, 2019

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

MOBILE COMMUNICATION PRANK CALLS AVOIDANCE BY PREFIXES AND NUMBER FORMATS

Yashavant S. Ingle and Jayshree Pansare

Department of Computer Engineering, MESCOE, SPPU, Pune

DOI: http://dx.doi.org/10.24327/ijrsr.2019.1004.3347

ARTICLE INFO

Article History:
Received 6th January, 2019
Received in revised form 15th February, 2019
Accepted 12th March, 2019
Published online 28th April, 2019

Key Words:

Prank Calls, HLR, MSC, AUC, Mobile Number Formats

ABSTRACT

There are many ways available to give a mobile user prank calls and cause distress by it. The user can be student or anyone certainly the Prank Calls are not welcome by anyone except the persons making them or promoting them. I want to put a restrictive measure for making mobile user able to decide over his calls and avoid prank calls. Otherwise, people who are receiving prank calls have to call up Customer Care Services and it's having limitations these days to call them 3 times a day. If the prank call receiver calls in distress more than 3 times probably he looses his Service to call to Call to Customer Care from his SIM. The email reply by Customer Care comes within 48 Hrs or even a delayed responses are received sometimes. Prank calls may come from different numbers at different times so person can't predict no to block always and use call manager facility provided to him becomes inefficient. So, the available ways don't solve the problem of person meeting harassment by prank calls. This is more serious offense in some cases leads to serious losses. So, we propose the simple solutions to save the innocent persons being targeted by the prank calls by using prefixes and number formats. The formats needs to meet some change and the verification process is added to ensure type of call and signal it to the user on screen.

INTRODUCTION

THIS paper presents a use of prefixes and number formats to save mobile users targeted by prank calls. The person who is receiving prank calls often receives from familiar looking numbers and may be made to fall prey to receive it. The consequences of prank calls may not be funny but serious. The present policies of companies don't support the ban on any calls. So, the calls from internet will come to your mobile and you will find that you are not able to distinguish it's a correct call or prank call. The investigations for the prank calls often are time consuming for the police. To know about anonymous call the mobile user need to call customer care of his service provider and he can't call more than 3 times a day. If he/she does call more than 3 times a day he/she may lose the facility of calling to customer care for making more calls. Thus making it bad choice for user to call to busy customer care for help on prank calls. Upon grievances person don't get the customer care facility back immediately if thus withdrawn. Let's try Call Manager facility provided to users. User adds numbers to call manager be blocked for calls from which user got prank calls. This will not solve the problem as the calls user will get as prank calls may be from a different unknown number each time. So you will block it and will get a prank call from another number next time as the caller knows limitations of Call Manager. Also, Prank call may be done to you from numbers you are familiar with and saved in your phone memory or SIM Memory. So, knowing this you can't block the number of your father which was used by prank caller to show it on your screen because next time your father may call you from same number, you know. The call manager is having its limitations. So, Call Manager don't provide solutions to Prank Calls. If you would prefer to use your instincts to judge prank call or genuine calls. You will be causing problem to your psychological health as result of failure to judge it correctly or curiosity to know you judged it correctly or not. Why? If you avoid taking calls from all unknown numbers you may lose some most important calls. In today's society one needs to be globally connected sometimes for them the call avoidance is not at all a great solution. And more the trouble increases when your customer care facility is withdrawn for calling to customer care because of 3 calls per day limit as a reason. This leads to a decision by you to take the call or not as there is no hints now to you. The intentions of prank calls are to make fun of someone, disturb, distract, threatening, fooling, impersonating for commercial benefits or enjoyments are successfully manifested because of supported by present facilities available to the mobile users getting prank calls.

Corresponding author:* **Yashavant S. Ingle
Department of Computer Engineering, MESCOE, SPPU, Pune

When customer is equipped for the ability to distinguish between the prank calls and genuine calls the very moment he/she gets a call, this solves the problem leaving a decision on user to receive it or not. With this solution the companies policies remain undisturbed as prank call will be indicated to user but not disconnected and user is made more intelligent by simple implementation of this proposed usages of prefixes and number formats for Prank Call Indication.

Related work

Systems and Methods of Detecting and Preventing Fraudulent Telephone calls

Present we have systems implemented and researched for avoidance of prank calls by terminating them. **Ghisler** invented a method supervising subscribers in a mobile telephone system to detect fraudulent usage of telephone U.S. Pat. No. 4,955,049.[1]Ghisler assigns predetermined sequence of number to each mobile telephone in system. Each time call is made by a subscriber, the next number in the mobile telephone's assigned sequence is transmitted by the mobile station to the serving MSC. The MSC records the numbers utilized, and detects a fraudulent call if there is a break in sequence. Ghisler , however requires modification of each mobile station to store it's assigned number sequence and transmit the next number in the sequence each time a call is made.[2]

U.S. Pat. No. 5,309,501 to **Kozik** *et al*. Kozik discloses a modular switching system for detecting fraudulently identified mobile stations in cellular mobile telecommunications network.[3] Kozik is a switch based fraud detection system which examines class of state transitions to see if a particular mobile station state transition is likely, in view of a recorded prior state of the mobile station. Unlikely state transitions are indications of possible fraud. Kozic, however , only works if the legitimate mobile station and the fraudulent mobile stations in the same location, and finds an indication of fraud if both of the mobile stations are in same state transition in same location.[2]

George Foti inventor of U.S. Pat. 5,970,404 discuss the analysis about call origin by location.[2] George Foti over comes the disadvantages of solutions by Ghisler and Kozic.
A system described by Mr. George Foti is useful method for detecting fraudulent telephone calls in a radio telecommunications network that does not require modification of the mobile station, and that detects fraudulent mobile stations operating in locations different from the legitimate mobile station, and in the coverage area of different switches.[2]

These systems don't address the issue of Caller ID Spoofing but the SIM Cloning. The Caller ID Spoofing is a method of giving prank calls to receiver using variety of means as software and showing any Caller ID of choice on mobile screen of receiver. The present invention provides such methods to prevent the Fraudulent or Spoofed Calls. The method has left it up on choice of Service providers and policies whether to terminate the calls or inform the user about type of call using number formats or any suitable means of indication for prank calls.

Summary of the Invention

The method described by the George Foti is having approach of analysis for the mobile locations stored in HLR. This a approach suggests the addition of fields in HLR and VLR that will help in fraud detection and using George Foti's approach differently for Tie in calls. The permission for strictly one call at a time from the registered subscriber will make fraud detection easy. AUC authenticates subscriber first time and then process is with HLR to manage subscriber.AUC generally don't authenticate subscriber at each call. So, people can use internet or software to generate prank calls using subscriber's MSISDN number. Because of this as there is no check there are multiple call requests at different MSCs for registered MSISDN numbers they get served. The HLR can help a great deal and so VLR and AUC to detect fraudulent calls.

The HLR (Home Location Register)is a database of subscriber information which stores account information, account status, user preferences, features subscribed by user, user's current location and so on. The data stored in HLRs for is similar but do differ in few details as per policies of Service Providers. The HRL are used by MSCs to originate and deliver arriving mobile calls to users.

The VLR is another database similar to HLR, which is useful to temporarily hold information of roaming users who are outside their home area. The VLR database is based on information collected from a HLR. MSCs use VLR to manage roaming users. Each mobile network has its own HLRs and VLRs.

When MSC checks mobile user's presence if user is in home area HLR is used, and if user is roaming VLR contacts the user's HRL to get the necessary information and sets up a temporary user profile. The user location is recorded in HLR and in case of roaming it's also recorded in VLR.

When user wants to make a call : if user is in home area MSC contacts the HLR prior to setting up the call and if user is roaming then MSC contacts VLR prior to setting up the call. When there is incoming call for user the call goes to home MSC ,if user is in home area home MSC delivers the call immediately and if user is roaming home MSC contacts VLR to determine the appropriate switch in roaming area to handle the arriving call and then transfer the call to roaming area MSC.

We know that the AUC authentication center is using HLR for security purposes of SIM. Each SIM card is assigned an individual key (ki), a matching ki contained in AUC. The SIM card and AUC store the key ki in an unreadable format. ki even remains hidden from SIM card owner to prevent network operators from fraud, such as SIM cloning, through enabling user identity verification and ensuring call confidentiality. Key ki is used with IMSI number. IMSI converted to GMT when subscriber is doing international roaming and message is routed across Global Title through SCCP network.

Network and service subscriber validity is determined by successful authentication. The authentication is done when a subscriber request a signal from network. The randomly selected key is generated that encrypts all wireless communication between mobile device and core network. The encryption algorithm is known as A3.The encrypted randomly chosen number (RAND) using the ki must match the stored

number in the AUC and the SIM card. The entire process is completed during wireless connection. If the number do not match, the authentication is invalidated as failed function request. The first time a subscriber attempts to make a call, the full authentication process takes place. However ,for subsequent calls attempted within a given system control time period, or within a single system provider's network, authentication may not be necessary, as the data generated during the first authentication will still be available.

AUC performs authentication function. It will be normally co-located with HLR as it will be required to continuously access and update, as necessary, the system subscriber records. The AUC/HLR center can be co-located with the MSC or located remote from the MSC. The authentication process will usually take place each time the subscriber "initializes" on the system. In this context, Authentication Center AUC is depicted in **Fig.1**.

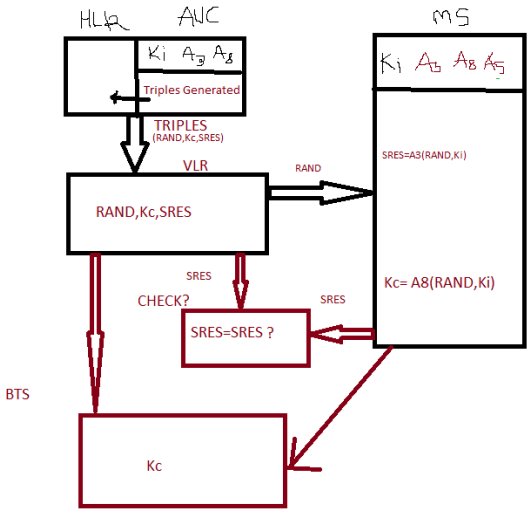


Fig 1 Authentication Center AUC

AUC Authentication Process

To discuss the authentication process we will assume that the VLR has all the information required to perform that authentication process(Kc, SRES and RAND). If this information is unavailable then VLR would request it from the HLR/AUC.

1. 1.Triples(Kc, SRES and RAND) are stored at the VLR.
2. TheVLR sends RAND via the MSC and BSS, to the MS(unencrypted).
3. The MS using the A3 andA8 algorithms and parameter Ki stored on MS SIM cars, together with the received RAND from the VLR, calculates the values of SRES and Kc.
4. The MS sends SRES unencrypted to VLR
5. 5.Within the VLR the values of SRES is Compared with the SRES received from the mobile. If the two values match, then the authentication is successful.
6. If ciphering is to be used , Kc from the assigned triple is passed to the BTS.
7. The mobile calculates Kc from the RAND and A8 and Ki on the SIM.
8. Using Kc,A5 and GSM hyper frame number, encryption between the MS and BSS can now occur over ther air interface.

RAND- Randomly generated number
SRES = Derived from A3(RAND , Ki)
Kc=Derived from A8(RAND , Ki)
A3=From 1 of 16 possible algorithms defined on allocation of IMSI and creation of SIM card.
A8= From 1 of 16 possible algorithms defined on allocation of IMSI and creation of SIM card.
Ki=Authentication key, assigned at random together with the versions of A3 and A8.

Thus AUC Authenticates user *only first time* generally and we need to check user at each call origin call is fraudulent or not.

Expected Fields in Hlr for Fraud Detection

1. AUC Authentication Result(available)
2. SOURCE NO (MSISDN)
3. DESTINATION NO(MSISDN)
4. CALL TYPE(LOCAL,INTERNATIONAL)
5. FRAUDULENT CALL
6. STATE INFO

a. a.BUSY
b. b.INCOMMING CALL
c. c.OUTGOING CALL
d. d.INCOMMING MSG
e. e.OUTGOING MSG

(others like VIDEO,IMAGES,BLUE TOOTH are helpful when doing fraud detection about CALLS knowing what activity is making phone busy.If we are enquiring for fraudulent calls then only a,b,c are required to be checked.)

Setting UP a Call

The Communication type must be indicated by SIM to Network For this Some flags can be helpful to be created in HLR/VLR. Those will help to be set up procedures for fraud detection and also monitor present state of mobile. The flags can be made hidden to Customer Care Representatives to protect privacy of usage of mobile user.

Mobile State Flag Can be maintained as--

SWITCHON/OFF 0 – OFF 1- ON
Just Switch ON 0- IDLE (needs updating of VLR for address if mobile is switch on in new VLR area)
BUSY-

1. BUSY for outgoing CALL Connected
2. BUSY for incoming CALL Connected
3. BUSY for Requesting for Call for connection
4. BUSY receiving a call
5. Busy in sms, chat
6. Busy connected to internet

(busy status can be added for other activities)

The Call will get Authenticated and status will be updated in HLR. Quickly by looking at these flag bits.

Create Record of New Request

(Source NUMBER) (Destination Number) (STATE)
Network first receives SIM State flags quickly along with request ,also network may monitor sim state anytime if it

wishes to do so and fills this record. Let's have a temporary database at HLR /VLR for CURRENT CALLS. When call gets connected Entry will be removed after copying it to another Database of Connected USERs for Call, it will be cleared when call gets over.

Then Enters Call Authentication Process

We Restrict a SIM to make only one CALL at a TIME.
Call Verification
1.Call comes at MSC

2.MSC goes to respective HLR
UPDATES record for CALLING number in
CURRENT CALLS
{
Checks Connected user database for calling i.e. source MSISDN?

YES: CALL is Fraudulent
NO: Do the Mobile _STATE_Checkup
If flags not verified :Call is fraudulent
If flags verified
(still someone may know mobile state rare)
If(CURRENT CALLS shows many entries for one MSISDN)
YES
Do the registered location check in VLR with entries in CURRENT CALLS connect only call of user that matches true location as normal call. This will be best to have ability to get location information immediately if call is from Internet.

OR

If the internet Calls can't be immediately traced for locations then we can depend on type of CALL Check procedure
If (Type of Call=Expected type of Call)
YES: Is Call not from Intern*et al*low Normal Call//
Else
Fraudulent Call

NO: Fraudulent Call

NO

Connect the normal Call with destination user
Update flags
-outgoing Call Connected flag of source&
-incomming Cal Connected flag of destination
}
MOBILE_STATE_CHECKUP
{
Network communicates with HLR state Flags, mobile SIM gets THE STATE OF MOBILE flags also network sets the state Flags by using database knowing present use of mobile.
(Verify flags by Network for CALL authentication.)
{
IF mobile is SWICH OFF Call is fraudulent
Else
If mobile is idle Call is Fraudulent +UPDATE VLR and do AUC Authentication for SIM.
Else
If (mobile is BUSY connected to any services like internet,so that new call can't be made from it)
Call is fraudulent
else
If (mobile is requesting for call connection)
RETURN O K.
Else
Call is fraudulent

//IF It will be difficult to have this FLAG
//verify other flags for BUSY we will
// know if they are false the request is
// made for call from mobile as done above
}
}

CHECK ALLOWED_MNCCALL_DATABASE
{ //Check allowed user database for calling NO
found Connect normal CALL Update destination user records Write MNC name who called.
Not found CALL is Fraudulent update user records in source and destination of this call ,but for anonymous CALLs
}

FRAUDULENT CALL INDICATION Procedure
{
If call is International

Mark # MSISDN this helps user to know fraudulent call has came
}
Fast SIM VERIFICATION By FastEncryptionAlgo
{
Ask SIM to Send Encrypted IMSI by any Fast Encryption algorithm chosen by it's Service provider to authenticate it at run time. Algorithm can be different for different SIM this makes it more Secure

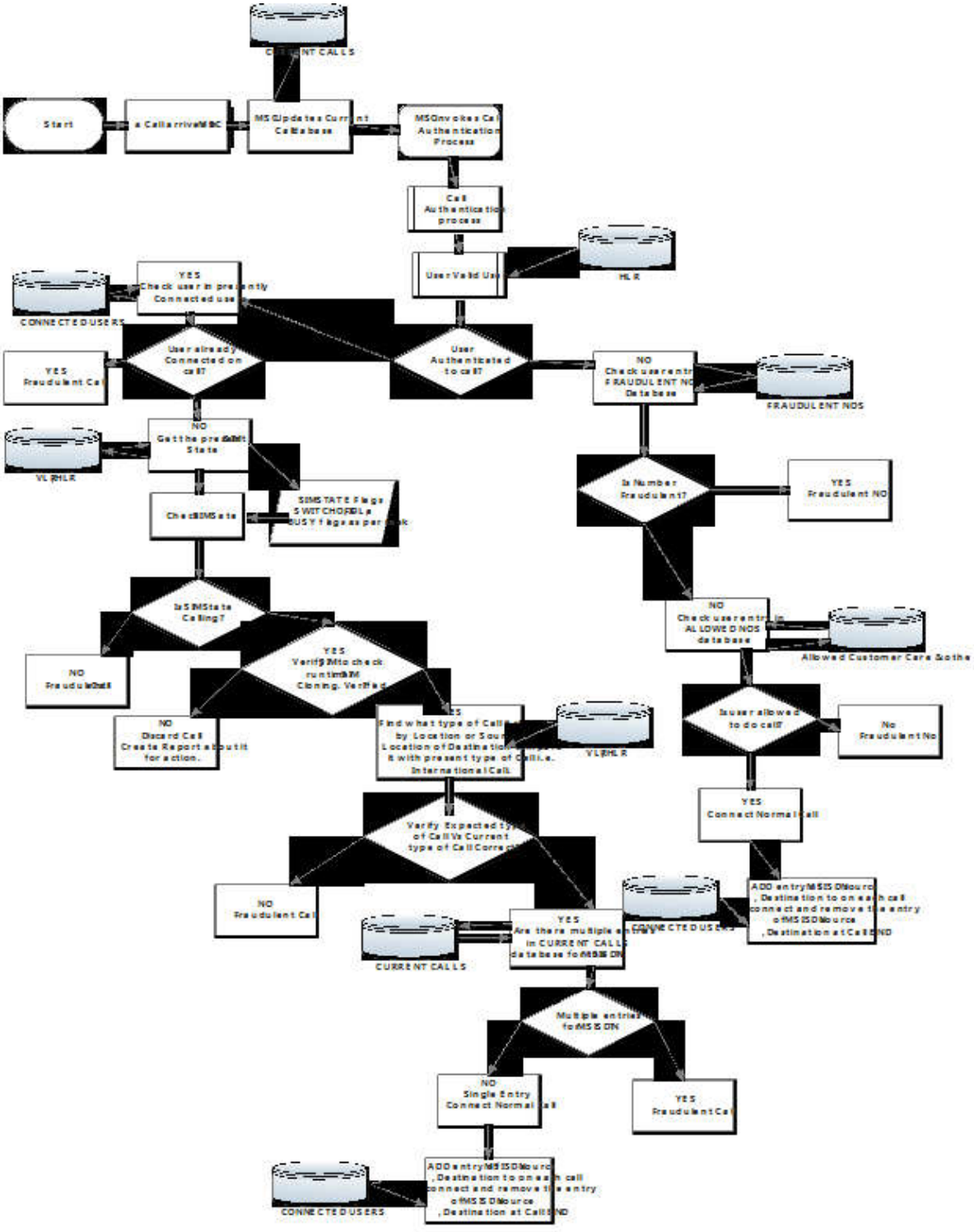
The VLR/HLR asks SIM to send encrypted IMSI using Kc that it got when authenticated for Air Communication by AUC Kc is with VLR and also IMSI of SIM.

If (eIMSI and VLReIMSI matches)
SIM is authenticated not cloned.
Else
Fraudulent Attempt Cloned SIM
}

If call authentication verifies call is from genuine user it connects call as normal else call is detected as fraudulent call and AUC takes suitable action depending upon companies policies for fraudulent calls for CALL Termination or CALL TYPE INDICATION to USER..

Hlr Modifications

Modifying HLR for having information about, the First Authentication by AUC i.e. say AUC STAT1,Present Call Verification Result, Present Source number(CALLER ID), Present Called destination, Type of Call. This really makes HRL powerful to detect present call is spoofed or original.
AUCSTAT1-It's updated when AUC performs A3 checkup on SIM verification. It's useful to decide to Call is fraudulent if we don't find this entry set to "verified" and finds entry in HLR by mistake.



Sequentially, aforementioned discussion is presented in Flowchart as shown in **Fig 2**

Present Call Verification Result– It's set after check if present call is fraudulent or not. After taking suitable action for call verification for termination or Indication. We can update the destination No HLR record for getting call from unverified user in same field.

Present Source number (CALLER ID):- This will help to maintain record of Caller ID shown and inform later on to the Caller ID user about a fraudulent call is made using his/her CALLER ID and if they want to take any action they can proceed. We can also help them by adding in HLR about true caller later on for this call.

Type of Call- Normal ,International, Fraudulent helps for indications to user if CALL TERMINATION is not supported by Companies Policies in some countries this will still save users from getting information about fraudulent CALL is coming and they can terminate it at their own.

Using Mobile Number Formats as Means of Indication of Fraudulant Calls

We have to think as per country the mobile No formats change. Indian Mobile numbers have 10 digits with AB-XYZ-OOOOO format AB-Access Code, XYZ-MSC Code and OOOOO-subscriber number. First five digits are allotted time to time by DoT to all mobile operators. We need to have some change in format to indicate Call is fraudulent if call termination is not allowed as per the companies policies but it should be mandatory for MSCs to inform the user about type of call.So, to do this we can play with number formats.

Say Fraudulant Number is Indian No and detected and on user screen it will appear as per Indian format

Eg. +912261138857
+919096767787
Say Fraudulent Number is UK number and appears on user screen as
Eg.+447xxxyyyyyy
+44<area code><local number>
Sometimes say subscriber's number is 07728248985 and if subscriber is calling international call 0 gets changed to +44.
Eg. +447728248985

In South Arica
072 244 3259 in South Africa will be formatted like +72 244 3259

We need to understand the fact that most of the fraudulent calls are done in each country by making use of call or sms spoofing software and internet or installing call or sms spoofing software in mobile phone. People can show any number while spoofing so if the call is spoofed we can just indicate type of call by Adding extra explanatory symbols in our mobile number formats about type of call. I feel explanation about prank call is mandatory, so when call is generated in India and user chose to show Indian number on screen there is misconception by receiver unable to detect it's normal call or International Call. Now make it a point that call call spoofing was in practice by mobile Customer care personals in history and today also they have their own set of numbers that they declare for giving calls to customers and it's legal. So, while building our databases for indication about fraudulent calls to customers a Database of Objectionable numbers, Restricted numbers, Call Center numbers, authorized numbers should be handy at AUC which performs call authentication. After verification about call if action is Indication about call to user this database will help a great deal.

The AUC checks the type of call if it is International

1.Checks database by matching the caller Id with allowed users database the HLR entry for the calling agency can be checked and verified whether any of it's allotted numbers has chosen from this number to call destination no?

If yes. No need of any indication call is normal. Show the call as per normal known formats now.

But if no, then it's fraudulent call. So, inform user who will receive call as using some symbol prefixed to the number as

#+912261138857 OR
#912261138857 by replacing +sign OR

Using some extra feature in mobile screen to see the type of Call. This is should be done by mobile manufacturing companies being directed by mobile service providers. This will be very good feature helping user know about type of call and decide to take it or not.

CONCLUSION

Fraudulent call detection system is invented by using the method of encryption we can detect the fraudulent call from AUC/HLR. The system is suggesting change in the HLR and AUC Keys and SIM Keys storage. The spoofed Call detection is done using fastest encryption algorithm. Future work the call detection by using HLR Location information is also useful and we also added present source number in HLR to check the state transition. The State transition can be helpful to locate the fraudulent calls. Finally, the Mobile Format Change is suggested or developing a feature in mobiles for call indicator as present policies of service providers do not terminate anonymous calls. But they can contribute

Acknowledgment

I am thankful to the inventors of fraudulent call detection systems for helping me to understand the approaches for discovering them that excited me think up on my own approaches in relation to present policies of companies and I hope I got them right.I would like to thank my Professor Dr. U. A. Deshpande Sir and Project Guide Professor Anil Mokhade Sir for consistent encouragement for doing something innovative and guidance.

References

1. Walter Ghisler,"Method of supervising mobile telephone subscriptions in a mobile telephone system" u.s.Patent 4 955 049, Sep. 4,1990
2. Jack kozik,"Arrangement for detecting fraudulently identifies mobile stations in a cellular mobile telecommunications network" U.S. Patent 5 309 501
3. George Foti, "System and method of detecting and preventing fraudulent telephone calls in a radio telecommunications network" U.S. Patent 5 970 404, Oct. 19, 1999.
4. http://www.teletopix.org/gsm/how-authentication-center-auc-works-in-gsm
5. The difference between HLR and VLR written by AdministratorThursday, 20 August 2009 01:24 - Last Updated Thursday, 20 August 2009 01:27 and Brief HLR-VLR ,Silicon press

****