ISSN No. 0976-5697

Volume 5, No. 4, April 2014 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Detection and Prevention of Premium Number Fraud in Mobile Computing

Jadala Vijaya Chandra
Warangal Institute of Technology and Science
Warangal, Andhra Pradesh, India.
vijayachandra.wits@gmail.com

Marri Rami Reddy*
Gemini Consulting and Services
Hyderabad, Andhra Pradesh, India.
ramimarrireddy@gmail.com

Gyaderla Ranjith
Warangal Institute of Technology and Science
Warangal, Andhra Pradesh, India.
gyaderlaranjith@gmail.com

Abstract: The Fraud Detection is identifying unauthorized use of Telecommunication. There are different types of call frauds and the SMS Frauds from premium numbers, which include Wangari Calls and Wangari Call Backs. A Research Conducted taking a Scenarios of Ireland and India. The work carried out in detecting calling card fraud -- the fraudulent use of a calling card account in order to avoid paying for calls, concentrated on Fraud Detection, Prevention and Deterrence. The Different Possible Procedures to Block the entire Problem Premium numbers in the Network is projected. In paper we also discussed Mobile Computing Architecture and different data mining techniques that are used to collect data, demonstrating how the frauds will be predicated and various fraud detection techniques are discussed. The Design and implementation of a software tool is described along with the tool architecture and how the inner workings are interrelated. The conclusion is given for the Prevention and Protection with Experimental Results and Graphical Analysis of Tool Performance. The Final Objective of this Paper is restricting or blocking access to a series of premium numbers that have been used for a recent scam where customers see a 'missed call' and on dialing the number are charged at international premium rates.

Keywords: Wangari Calls, Mobile Computing, SMS Frauds, Call Frauds, Premium Numbers.

I. INTRODUCTION

Solving a real time problem is very important for a researcher, where theoretical and practical implementation is done for detecting problem and prevention in possible strong manner. The Fraud Detection is identifying unauthorized use of Telecommunication, where efficient fraud detection and analysis system can save telecommunication operators and companies a lot of money and help to restore subscribers confidence in the security of their transaction, where the subscriber can reliable on the telecommunication system. The Scammers first hire a Series of Premium Rate Numbers from a telecom provider and then give a Ghost Calls or Wangari Calls or Miss Call Fraud Calls to unsuspecting people. As they latter call back, they pay a higher charge and a part of the amount of Customers pay goes to the account of the scammer who hires the premium number.

A Research Conducted taking the Scenarios at Ireland and India. In Ireland Wangari Calls where throughout Saturday night and Sunday morning thousands of People received missed calls from a number with the prefix 386. Many called the number back under the assumption that it came from an Irish 086 number-which would appear on a mobile phone as 35386, However they connected with the premium number connected to a premium rate service based in Slovenia. In India on the Eve of New Year at Calcutta many people received a missed calls from international numbers 22455xxxxx when the user calls back they are charged 61 rupees for 1 minute. The number looks like an STD number of Mumbai as it starts with 22, A college student at Calcutta received a wangari call and thought of that the call from his friends at Mumbai as the call came at New Year Eve Without any suspicion, He called back and the woman who answered said in Hindi that the number belonged to a Mumbai-based cell phone company. She started telling him that the cell phone number was among the lucky winners of a draw and student would be awarded a cell phone by the company. She also asked for address". He spoke around eight minutes and when the call ended, he realized that he had been charged 488 rupees for it.

This Paper defines Problem scenario and different Problems Solving Techniques, Data Mining Algorithms and Block Diagram where the Architecture and work flow logic is described. A Practical Approach is given for the design and implementation of software tool and its Performance and Experimental Result, Graphical Analysis is provided. Where the conclusion is given and Future Scope is mentioned.

II. RELATED WORK

Mobile Prepaid is a telecommunication service that requires a customer to pay before making calls. Postpaid service is opposite of prepaid where the customer pay to telecommunication after a period of time. In prepaid service are implemented by using any of the following approaches such as wireless intelligent network approach, the service node approach, the hot billing approach and the handset-based approach. In Hot Billing Approach, it uses call details records (CDRs) to process prepaid usage. The prepaid CDR is created in the MSC. The information in a CDR includes type of service, date/time usage, user identification, destination of the call and locator information. These records are generated when the calls are completed and are transported from the Mobile Switching Center (MSC) to the prepaid service center. The balance of the customer's account is decremented according to the CDRs. When a customer uses up the prepaid credit, the Home Location

CONFERENCE PAPER

Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

Register (HLR) and Authentication Center (AuC) are notified to prevent further service access.

In hot billing architecture, a call record is send from MSC to prepaid service center using protocols such as Common Management Information Service Element (CMISE). The same protocol can be used for communication between the prepaid service center and the HLR. The HLR communicates with the MSC by invoking GSM MAP service primitives. The IVR generates automatic messages that allow the customer accounts to be queried and reloaded.

Hot billing prepaid service includes following steps:

a. The customer subscribes to the prepaid service center at the POS or by calling the customer care center.
b. The prepaid service center creates a subscriber data record including IMSI, MSISDN, account of credit, period of validity, tariff model and other authentication-related information.
c. The prepaid service center activates the prepaid service by sending the customer data to the HLR, which then creates a record for the customer.

To remove a customer from prepaid service, the prepaid service center simply sends a request to the HLR to delete the customer's record.

The hot billing prepaid call origination procedure has the following steps:

a. When a customer originates a prepaid call, the IMSI is sent to the MSC.
b. Based on the IMSI the MSC instructs the HLR to determine whether or not it is a valid service request.
c. If the verification is successful, the HLR downloads the customer data and a prepaid tag to the MSC. The call is connected.
d. When the call terminates, a CDR is created and sent to the prepaid service center.
e. The prepaid service center decrements the prepaid credit based on the received billing record. If the balance is negative, the prepaid service center instructs HLR to suspend prepaid service or delete customer's record.

III. MOBILE DATA BASE AND DATA MINING

A. *Mobile Databases:*

A Database is a collection of systematically stored records or information. Whenever a phone call is completed a call detail record (CDR) is created. Depending on the operation currently being performed the structure is as follows account number, telephone number, date and time of the call, the duration, the originating area, receiving area, and the cost of the call.

Premium rate services are used with both normal calls and SMS messages. Where the subscriber will get unexpected high bills. The Time frame of the Fraud calls coming in will be calculated. The different Countries Wangari Call Fraud effect is taken as the part of Analysis and found the following the graph obtained.

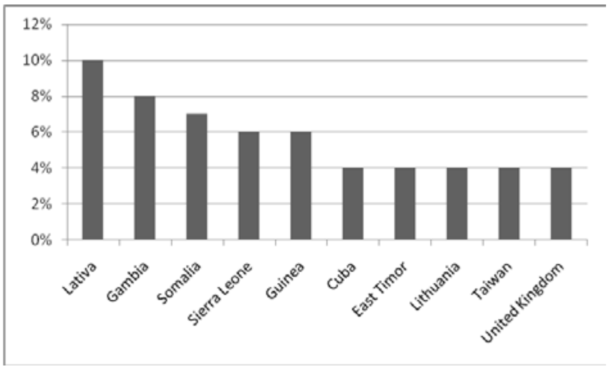

Figure 2.1 Wangari Call Fraud Analysis of Countries

The Database of Country, Country and International Standard Code of the Country is stored as the part of the Project. Where the PK is the Primary key of the Database where The Alphabet code and Numeric code is mentioned in the table, where Numeric code in the table is the International Subscriber Dialing Code. The Sample Database is given below

Table 2.1 Database of ISD Codes and Countries

Sl.no	PK	Country	CODE	Code
1	62	Sudan	SDN	249
2	63	Rwanda	RWA	250
3	64	Ethiopia	ETH	251
4	65	Somalia	SOM	252
5	66	Djibouti	DJI	253
6	67	Kenya	KEN	254
7	68	Tanzania	TZA	255
8	69	Uganda	UGA	256
9	70	Burundi	BDI	257
10	71	Mozambique	MOZ	258
11	72	Zambia	ZMB	260
12	73	Madagascar	MDG	261
13	74	Mayotte	MYT	262
14	75	Zimbabwe	ZWE	263

B. *Data Mining:*

The Data mining originated from database technology, statistics, machine learning, Artificial Intelligence, visualization and traditional techniques. The Data mining discovers the patterns and relationships hidden in the data. Combination of CIC (Circuit Identification Code), and OPC (Originating Point Code) & DPC (Destination Point Code) are used to identify a call. Rule based Data Mining Algorithms are used to identify the fraudulent behavior from the large databases of customer transactions.

The Data mining Techniques such as anomaly detection, Dependency modeling, clustering, Classification, Regression and summarization are used in fraud detection.

IV. FRAUD DETECTION

The fraud will depend upon the payment scheme used for the Premium Rate Service where receives a share of the revenue generated for the Network. For Prevention of the Fraud the Vodafone has created the following alerts for wangari frauds and SMS Frauds which are known as hot destination range they are how many calls attempted and in them what are inbound calls and SMS and how many customers are effected depending on that data base the

Wangari frauds are classified as Wangari –A, Wangari –B and Wangari –C. There are two methods they are Pre-call methods, which try to identify and block fraudulent calls as they are made and Post-call methods, which try to identify fraud that has already occurred on an account so that further fraudulent usage can be blocked.

The consumer problems by the Fraud calls are that the subscriber receives an unexpectedly high bill because of the subscriber was unaware of the tariff that applied to the call The length of the call is artificially by putting the caller on hold, or deceptively extended, example by answering so that charging starts yet applying a dial tone sound from the distant end. The subscriber was unaware that they can have premium rate calls barred or thought that a call bar applied when it did not. The call was made by another individual and was not authorised by the subscriber (the caller may have been unaware of the tariff or may have deliberately stolen the call). The call was made automatically by a computer activated, for example, by a virus without the subscriber being aware of what was happening, The subscriber is not aware of the nature of the service, for example they think that they are buying one-off service and yet they are initiating a subscription service with repeated charging that will continue until they unsubscribe.

A. Fraud Analytics Solution:

a. Alters or Alarm generation during the automatic dialing phase, clearly indicating that a Wangiri Fraud attack is underway.

b. Further linked follow up alarms if subscribers start to call these numbers back

c. Full visibility of the source of these attacks so these numbers can be hot-listed/blacklisted in case of future attacks

d. Automatic SMS delivery to affected subscribers warning them that they may be the target of such an attack provided an SMS interface is made available

e. Fraud Consulting Service will be provided as part of Customer Care Service which can help the customer giving information from where the origin of wangiri fraud attack and identifying the providers of International Revenue Share Number Providers and depending upon the level of Wangari Fraud and the possibility of Blocking of the Numbers will be informed and measures will be taken.

B. International Roaming Fraud:

The International mobile roaming is a service that allows mobile users to continue to use their mobile phone or other mobile device to make and receive voice calls and text messages, browse the internet, and send and receive emails, while visiting another country Roaming extends the coverage of the home operator's retail voice and SMS services, allowing the mobile user to continue using their home operator phone number and data services within another country. The seamless extension of coverage is enabled by a wholesale roaming agreement between a mobile user's home operator and the visited mobile operator network. The roaming agreement addresses the technical and commercial components required to enable the service.

V. BLOCK DIAGRAM

All International Calls from ISUP Messages Inserted into the CDR_INT table for storage of Call Level records and MAP Messages will also be inserted in the same table once the MAP decoder is ready. Ingestor will insert the Data Ingest Rates in terms of All Protocol Messages, ISUP and MAP Messages, Count of Calls and SMSs. Rule Engine will insert the Count of International Calls and SMSs.

Extensible Metadata Platform (XMP) in Memory database is a data model uses Streaming call data, hot list tables and Rule engine processing to handle workflow or process and finally Reporting summaries and Configuration parameters are processed where Rule Engine is a logical entity which is implemented across XMP DB for rule processing and Java Scripts for configuration parameters. To Handle the database My Sql is used for query processing for data retrieval, manipulation and updation.

The ISDN User Part (ISUP), a key protocol in the SS7signaling system, defines the protocol and procedures used to set-up, manage, and release trunk circuits that carry voice and data calls over the public switched telephone network (PSTN) between different switches. ISUP is used for both ISDN and non-ISDN calls. ISUP Messages which are sent between source and destination carries significant information between the call set up and the end of the call.

All Initial Address Messages have calling party number. (Calling Party Number is an optional parameter in IAM. Earlier days of ISUP, calling party number is sent in IAM for only International Numbers. Later it is mandated for all calls. And it is observed that all IAMs have Calling Party Number). All information we needed are available in IAM Message itself (Called Party number, calling party number, National or international call). No information other than CIC and message type is needed from the all other ISUP Messages. Time of each message is the time of capture of the packet. Call duration is given by the difference between the REL(Release Message) and ANM(Answer Message). So it is necessary to capture only CIC, Message type and time of capture of message for all other ISUP Messages other than IAM

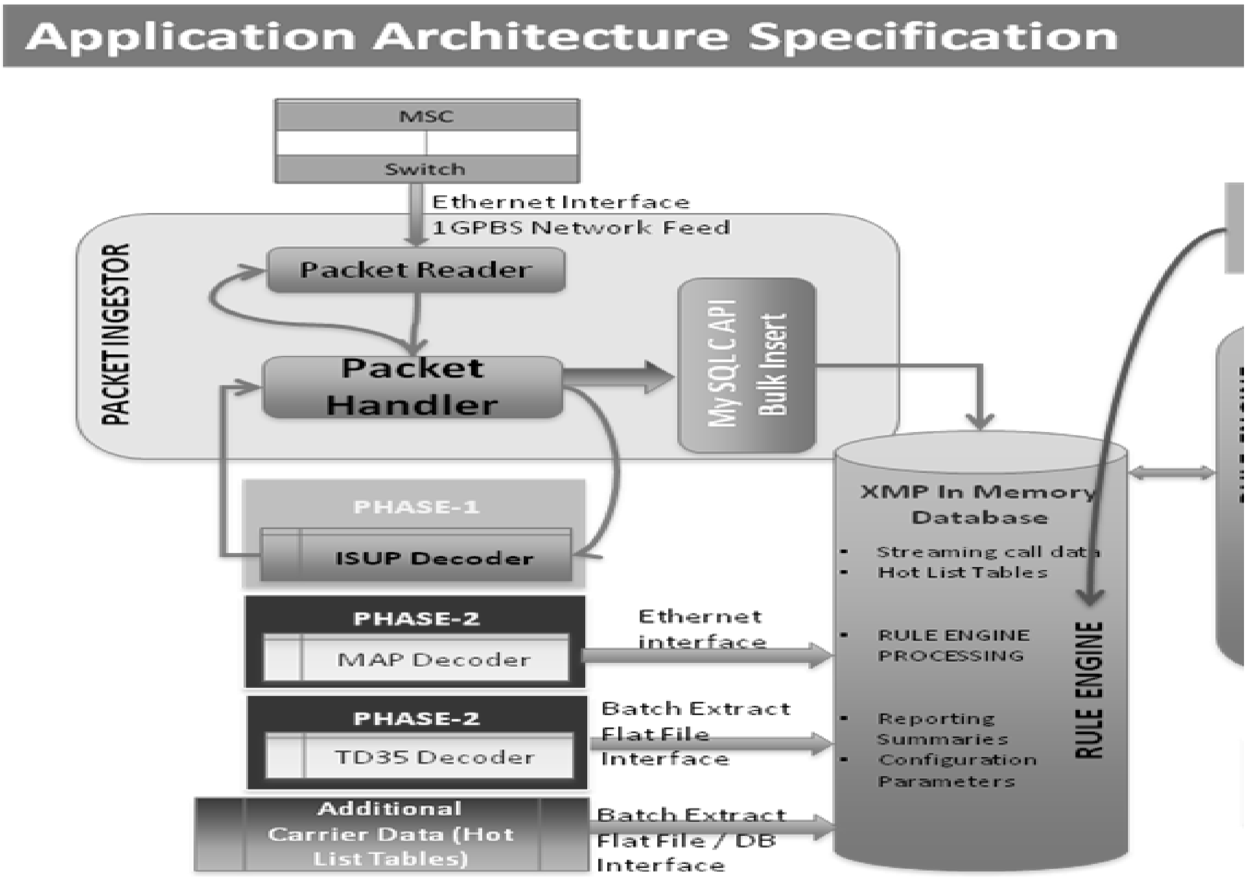

Figure 1: Block Diagram and Architectural Design of Software Tool for Fraud Detection

Signaling Transport(SIGTRAN) working group, standardize the messages and protocols necessary to carry mobile and PSTN signaling over IP networks that is SS7 over IP, the SIGTRAN working group has defined a new architectural model.

Upper Layer	ISUP
TCAP	
SCCP	
User Adoption Layer - M3UA	
Signaling Transport - SCTP	
Standard Internet Protocol - IP	

Figure 2: SIGTRAN Architecture

The ISDN User Part (ISUP), a key protocol in the SS7signaling system, defines the protocol and procedures used to set-up, manage, and release trunk circuits that carry voice and data calls over the public switched telephone network (PSTN) between different switches. ISUP is used for both ISDN and non-ISDN calls. ISUP Messages which are sent between source and destination carries significant information between the call set up and the end of the call.

An ISUP Message contains a fixed header which contains Circuit Identification Code (CIC) and the ISUP message type, followed by mandatory fixed length parameter part, mandatory variable length parameter part and optional variable length parameter part, as shown below;

Routing Label	
Circuit Identification Code (CIC) (2 bytes)	Message Type (1 byte)
Mandatory Fixed Length Parameter part	
Mandatory Variable Length Parameter part	
Optional Fixed Length Parameter part	

Figure 3: ISUP Message Architecture

Most common ISUP Messages are,

a. IAM (Initial Address Message): First message sent from source switch to destination switch which contains called party number, calling party number, type of service and some optional parameters
b. SAM (Subsequent Address Message): In-case of IAM did not contain full called party number, one or more SAM follows with the additional digits
c. ACM (Address Completion Message): Message returned from the destination switch from the source switch when the subscriber is reached and the phone starts ringing
d. CPG (Call Progress): Contains additional information about the progress of the call.
e. ANM (Answer Message): Sent when the subscriber picks up the phone
f. CON (Connect): Sent when the call is answered by automatic terminal. It replaces ACM, CPG and ANM

g. REL (Release): Sent when the subscriber goes on-hook. It is sent in the direction from which subscriber goes on-hook (either source or destination)

h. RLC (Release Complete): It is the acknowledgement of the release.

Packet Ingestor classifies network packets according to criteria given by user applications and conveys the accepted packets from a network interface directly to the designated applications. A packet Handler is most often installed at that point where the protected internal network connects to the internet. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. Packet Reader act by inspecting the "packets" which transfer between computers on the Internet. If a packet matches the packet Ingestor set of rules, the packet will drop (silently discard) the packet, or reject it (discard it, and send "error responses" to the source). It filters each packet based only on information contained in the packet itself (most commonly using a combination of the packet's source and destination address, its protocol, and, for TCP and UDP traffic, the port number).

Incoming Packet contains,

a. Ethernet Message

b. Internet Protocol Message

c. SCTP Message

  (a).Header

  (b). Chunk

d. M3UA + SS7 Message

The Interface is of two phases they are data interface and browser interface which are interrelated with different socket input output such as provision for adhoc Queries framework, Configuration parameters, visualizations and email alter interface. The SMS Fraud is mainly telecom -customer will get an SMS informing wining a Cash Prize, and asked to dial a Premium Rate Service for giving details.

VI. ALGORITHM APPROACH

Build a fraud detection system by classifying calls as being fraudulent or legitimate. All calls that would be unusual for one customer may be typical for another customer. At the level of the individual call, the variation is calling behavior is large, even for a particular user at a particular time.

A. *Stage 1: Rule Learning*

Rules are generated locally based on differences between fraudulent and normal behavior for each account, then they are combined in a rule selection step algorithm approach to generate rules with certain factors above user-defined threshold. Rule generation steps typically yields thousands of rule, if a rule is found in many accounts then it is probably worth using selection algorithm identifies a small set of general rules that covers the accounts. Resulting set of rules is used to construct specific monitors

Given:

Accts: Set of all accounts

Rules: Set of all fraud rules generated from Accts

T_{rules}: (Parameter) Number of rules required to cover each account.

T_{accts}: (Parameter) Number of accounts in which a rule must have been found.

Output

S: Set of Selected Rules

```
/*initialization*/
S={ };
For(a ε Accts)do cover[a]=0;
For(r ε Rules) do
Occur[r] = 0;
 /* Number of accounts in which r occurs*/
Accts Gen[r]={ };
/* Set of accounts Generating r */

Endfor /* Rules generated for Accts*/
End for /* Set up occur and Accts Gen */
```

B. *Stage 2: Profile Monitoring*

Resulting

Set of rules is used to construct specific monitors

Given: Rule Conditions from a fraud rule

Profiling: Air time of all calls is calculated; record the mean (μ) and Standard Deviation (σ)

Use: Calculation for Air time and output for Profile Monitoring

$$\text{Airtime} = \sum_{\text{Call}\in C} airtime(Call)$$

$$Output = \begin{cases} \text{Airtime} & \text{if } \sigma = 0 \\ \frac{\text{Airtime}-\mu}{\sigma} & \text{if Airtime} > \mu \\ 0 & \text{otherwise} \end{cases}$$

C. *Stage 3: Finding Evidence:*

Based on the Time and the Place according to the rule set Series of suspected numbers can be identified.

D. *Stage 4: Block the Fraudulent Numbers:*

At the Final State the Fraudulent numbers will be blocked.

VII. EXPERIMENTAL RESULTS

A. *General Description of Experimental Results:*

In order to validate the efficiency of proposed method of the Software tool, this was developed using Java based Graphic User Interface and XMP as database. As Experiment Results are of 92 Percent Accurate and leads to interest and concept in development of Commericial Software Tool.

Table of Fraud Analysis

Fraud Call Activity Analysis		
International Calls	Wangari Calls	Wangari Call Backs
23,320,878	2,147	422

The International Calls of 23,320,878 are observed where among them Wangari Calls are 2,147 detected and 422 Wangari Call backs are identified and The SMS are 18,110,820 are observed among them 1,754 are Wangari SMS and 817 Alters are given .

VIII.CONCLUSION

This paper presents an approach for Detection and Prevention of premium number fraud in mobile computing based on improved Architecture of SIGTRAN and ISUP Message Architecture where algorithm is used to build fraud detection system. The main contribution of this paper is a study of the avoidance of stagnation behavior and premature convergence by using distribution strategy of call detection and dynamic heuristic parameter updating based on entropy. Then emergence of local search solution is provided. The experimental results and performance comparison showed that the proposed system reaches the better search performance using algorithms. The proposed system is more in terms of convergence speed and the ability to finding better solutions.

IX. REFERENCES

[1]. “Classification, Detection and Prosecution of Fraud on Mobile Networks” by Phil Gosset and Mark Hyland - Vodafone Ltd, The Courtyard, 2-4 London Road, Newbury, Berkshire, RG14 1JX, England.

[2]. “Telecom Fraud Management” by A. P. Agarwal – Telecommunication Report India - 2010

[3]. “Internet Security and Privacy” – Communication Commission of Kenya – 2008

[4]. National Fraud Reporting Center – India 2014 Report

[5]. Telecommunications UK Fraud Forum -2014 (http://www.tuff.co.uk)

[6]. “The Detection of Fraud in Mobile Phone Networks” by N. Davey, G. McAskie. -BNR Europe Limited, London Road, Harlow, Essex, United Kingdom – 2014.

[7]. “International Fraud on Mobile Communications” by P. Barson, S. Field, R. Frank.- School of Information Sciences, University of Hertfordshire, United Kingdom – 2014.

[8]. “Detecting Fraud in Cellular Telephone Networks” by Johan H van Heerden, University of Stellenbosch, South Africa – 2012.