Detection of Fraud in Mobile Telecommunications

By John Shawe-Taylor, Keith Howker and Peter Burge, Royal Holloway, University of London

Introduction

Under the CEC's ACTS[1] programme, the collaborative R&D project ASPeCT[2] was set up to look at the problems and possible solutions for security in future mobile telecommunications systems to follow on from GSM. The project consortium consisted of Network Operators (Vodafone, Panafon), equipment suppliers (Siemens ATEA, Siemens AG, Giesecke and Devrient) and academic institutions (Royal Holloway, University of London and Katholieke Universiteit Leuven). While the greater part of the project focused on protection of the communication between users — mainly related to cryptographic mechanisms and services — a substantial section addressed the problems of fraud and abuse of the networks, looking at possible tools for detection and management, but also examining the legal implications.

We are concerned here with fraud-related work and report on the viability of the tools implemented and give an overview of some of the legal findings.

It is estimated that the mobile communication industry loses many millions of Euros per year to fraud, so prevention and early detection of fraudulent activity is an important goal for network operators. It is clear that the additional security measures taken in GSM and in the future UMTS system make these networks less vulnerable to fraud. Nevertheless, certain types of commercial fraud are very hard to preclude by technical means. Some examples of these types of fraud are described below. The use of sophisticated fraud detection techniques can assist in early detection and help reduce the effectiveness of technical frauds.

It is probably true that it is impossible to totally eliminate fraud. The fraudster will always seek a way to beat the system and any fraud detection mechanism has to be cost-effective. *Figure 1* shows the relationship between the cost of fraud and countermeasures versus the performance of the fraud detection tool. As efforts are increased to counter fraud, the cost of countermeasures becomes increasingly expensive to the point where they cost the company more than the remaining fraud. The thicker Total Cost Curve shows the two graphs summed to indicate an optimum, most cost-effective level.

The power of Neural Networks (NN) as tools for discrimination, recognition and

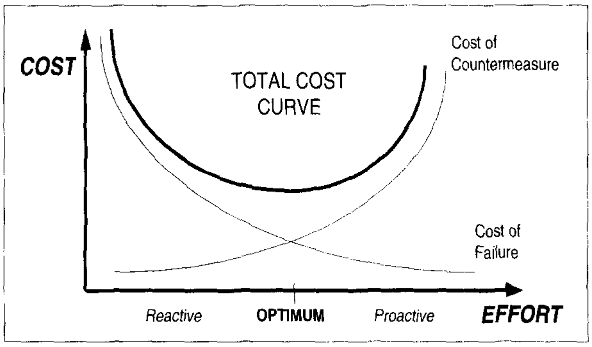


Figure 1. Cost Analysis of anti-Fraud Measures

[1] Advanced Communications, Technologies and Services (DG XIII/B).

[2] Advanced Security for Personal Communications Technologies — completed 31 January 1999.

0167-4048/99/$20.00 © 1998, Elsevier Science Ltd

classification is well known, therefore, this seems a natural technique to apply to the problem of detecting and identifying fraudulent activity. The technique is based on the fact that attempts at fraud or other abuse of the network's services by a user are always going to display some significant change of behaviour from previous legitimate activity. The recognition, and possibly classification, of such change is the challenge the project set itself.

Fraud Scenarios

Many new frauds have appeared since the project began in late 1995. Much of this has been due to the introduction of pre-payment schemes. We outline a few more important scenarios below, and list some of the others. Non pre-payment fraud includes the following:

Subscription Fraud

This is by far the most common fraud encountered on the GSM network. A person uses false identification to obtain a service. Subscription fraud can be further subdivided into two categories. The first is for personal usage by the fraudster, or someone he passes the phone on to. The second is for real profit; here the fraudster claims to be a small business to obtain a number of handsets for Direct Call Selling purposes. The fraudster, who has no intention of paying his bill, now sells-on the airtime, probably for cash, to people wishing to make cheap long distance calls.

PABX Fraud

Many companies provide a dial-on service through their PABX system so that authorized employees can use it for international purposes from wherever they may be located. This service is open to abuse if a fraudster obtains a password for such a system. Fraudsters often try to guess these PABX passwords by making many short duration back-to-back calls. These calls tend to occur out of office hours and are to fixed landline numbers.

Freephone Fraud

This occurs when a person uses a calling card service to dial onwards. In some countries, this is illegal in itself. More often though, it is the fact that these services tend to attract fraudulent mobiles.The fingerprint of such activity tends to be back-to-back calls and long duration calls.

Premium Rate Fraud

This involves the abuse of the premium rate services and can occur in different ways. For example, a person could set up a premium rate line with a national operator. The operator is obliged to pay the owner of the line a proportion of the revenue generated. The fraudster then uses a fraudulent mobile to dial this number for long periods. He may also get other people to do the same. The fraudster then pockets the revenue without paying for his own calls. A further way in which premium rate services can be abused is by setting up a fraudulent mobile to divert calls to a popular premium rate line. The caller then only pays normal rates whilst the fraudulent mobile picks up the tab at the premium rate. Characteristics are again long back-to-back calls.

Handset Theft

With many subscribers using their phone only intermittently or for emergencies, a stolen phone may go unnoticed whilst heavy fraudulent usage occurs.

Roaming Fraud

This is when a fraudster makes use of the delays in the transfer of Toll Tickets through roaming on a foreign network or through using a foreign SIM on, for example, a UK network. (technically, the latter should be called 'visitor fraud'). Weekend usage presented a very reliable delay in the past. Such delays are fortunately being reduced by modern billing systems.

Other scenarios include fax-back and malicious call-back fraud, technical internal fraud, mobile to mobile fraud, tumbling fraud, and hijacking. More information on these and other aspects of this fraud may be found on the project's Web site[3].

In addition, a new family of scenarios has grown around pre-payment — which in itself was meant as a counter to some of the situations above. Due to the infancy of this technology there are a number of obvious and not so obvious loopholes that enable fraudsters to make money. This mainly revolves around the voucher scheme whereby a person walks into a shop and purchases air-time via a physical voucher. The voucher contains a code number that when entered into the phone enables calls to be made; our fraudster is in business again. Identified instances include cheque fraud, credit card fraud, voucher theft, voucher ID duplication, faulty vouchers, network access fraud, network attack, long duration calls, handset theft, and roaming fraud.

The Fraud Detection Environment

There are three main roles that need to be considered in the Fraud Detection Environment. The first is the User, the entity that makes calls on the network. The User has a contractual relationship with the second entity, the Service Provider (SP), who charges the User for the calls made. The third entity is the Network Operator (NO), who sells blocks of air-time to the SP for selling on to the User. There is no direct contract between the NO and the User.

The purpose of a fraud detection system, or more specifically the Fraud Detection Tool (FDT) is to detect fraudulent behaviour of Users from their usage data, before the cost of such activity becomes too great. To achieve this, it is clear that the tool should be placed where it can receive this usage data as quickly as possible. This means that the FDT should optimally be closely connected to the network.

Within the network, there are two possible sources of usage data that can be employed for fraud detection. The first source is the Toll Tickets (or Call Detail Records — CDRs), the records of the calls produced for billing purposes, generally constructed immediately the call has finished. The second source is the Signalling Data produced in the network.

The advantage of using Signalling Data is that it makes more usage information available. For example, the location of the User at every Location Update would be available, as well as the opportunity to monitor the set-up of a call when it happens, rather than only once the call is finished. However, the disadvantage is the sheer volume of output, one or two orders of magnitude greater than that produced for billing, which would make impossible filtering and processing demands on our monitoring system.

The advantage of using the Toll Tickets (TTs) is that the information that is produced for billing also contains the usage behaviour information valuable for Fraud Detection. However, billing data needs to be gathered securely, and not necessarily quickly, so data may be a day old before it is processed. To allow for hot billing, where bills can be created very rapidly, and also to minimize this fraud risk window, a mediation device may be included in the network that polls the switches for their TTs on a regular basis.

[3] http://www.esat.kuleuven.ac.be/cosic/cosic.html

The data thus collected can be considered to be near real-time, as the difference between real-time delivery and polled retrieval can be made as small as practicable.

Once the TTs are processed, action needs to be taken in response to any alarms that are raised by the FDT. Such responses could be to question the Users to see if the activity had some benign rationale. However, there is a problem: there is no direct contract between the User and the NO[4], so the alarms need to be distributed to the relevant SPs, who will take appropriate action.

System Requirements

Performance

To minimize fraud losses, it is important that the FDT operate as close to real-time as possible. Using a mediation device to provide such a feed has another consequence, that of smoothing processing requirements. However, the usage of the Network varies throughout the day, and there will be a 'busy hour' in the day which may contains 15% of the day's traffic. The system will need to process tickets at a rate in line with this value.

Customization

The FDT must be easily tuneable for customization of fraud detection sensitivity and for alarm filtering.

Scalability and Flexibility

The FDT must be scaleable and adaptable in the fast growing mobile network environment. That would mean that any thresholds set during the initialization period should not reduce because of the network expansion. The FDT must also be flexible towards new and changing fraud methods and characteristics (i.e. behaviour changes) that are expected to manifest themselves in the future.

ASPeCT Choice of Technology

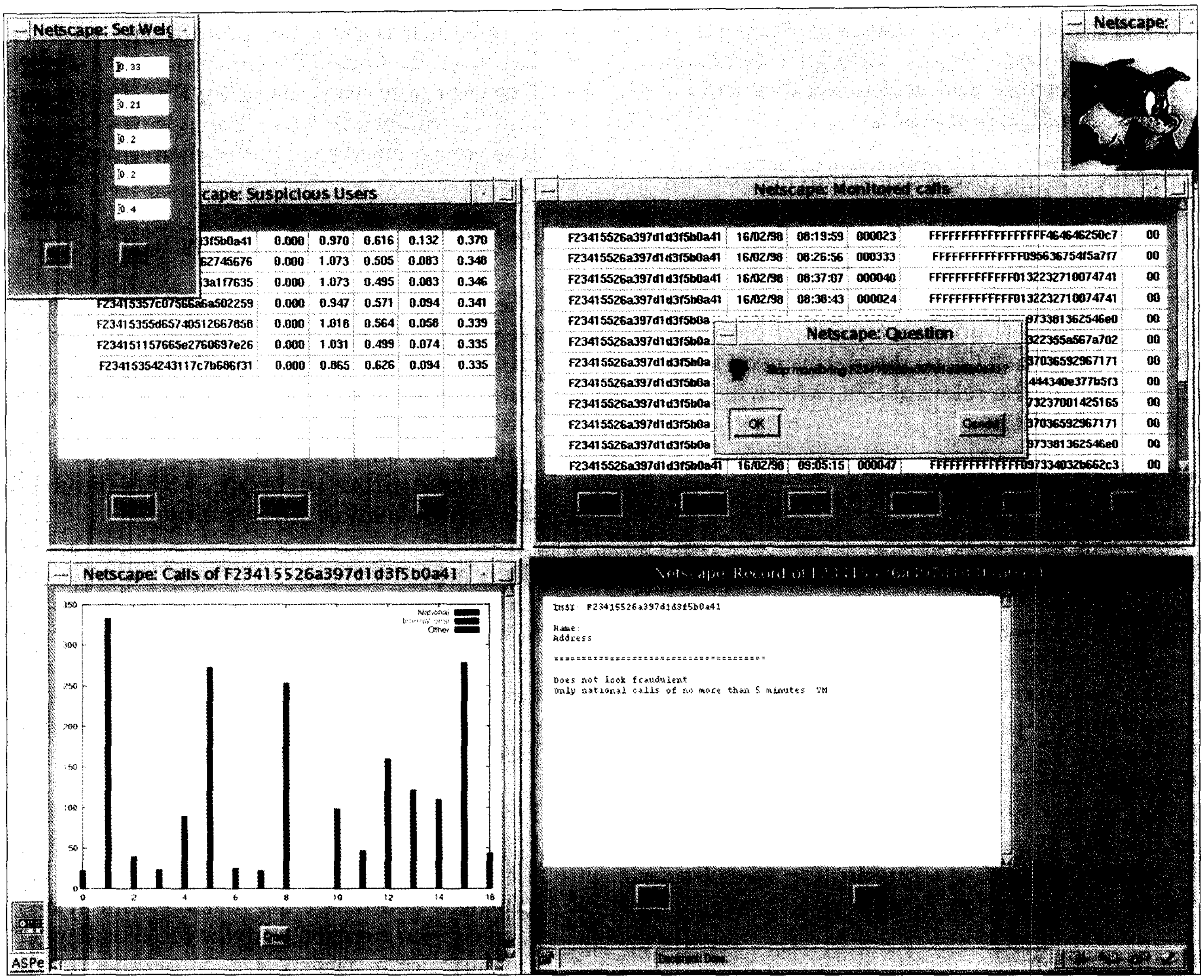
The ASPeCT tool did not set out to provide a flexible interface, strong database technologies, user friendliness and case management, which marketable products have, but in the later stages of the project a number of these issues were tackled. The effort required to bring ASPeCT-based products to market is not enormous.

There are currently over 30 fraud management products on the marketplace. Few appear to have performed a rigorous examination of the artificial intelligence technologies that could be applied to reducing fraud. ASPeCT carried out a thorough survey of options and possibilities in this area.

From our analysis, it was clear that a Rule-Based tool is a vital component of the tool-kit for identifying certain frauds. It is a white box approach and hence the management system can be given a reason why the tool has flagged an alarm for a particular user — essential for the legalities of barring the user from the network.

However, a Rule-Based tool on its own is not sufficient to deal with the complexities and intricacies of mobile telecoms fraud. Some form of 'fuzzy' soft-computing technique is required to handle scenarios that cannot be precisely specified by rules (a situation that is prevalent in mobile fraud, but perhaps less common in other fraud detection areas, such as credit cards). Neural Networks provide just this sort of technology which is able to deal with novel or abnormal instances or scenarios.

[4] The organization of the Network Operator is now tending to have Service Supplier operations.



0.33
0.21
0.2
0.2
0.4

3f5b0a41	0.000	0.970	0.616	0.132	0.370
62745676	0.000	1.073	0.505	0.083	0.348
3a1f7635	0.000	1.073	0.495	0.083	0.346
F23415357c07566a6a502259	0.000	0.947	0.571	0.094	0.341
F23415355d657405126678 58	0.000	1.018	0.564	0.058	0.339
F23415115766 5e2760697e26	0.000	1.031	0.499	0.074	0.335
F234153542431 17c7b686f31	0.000	0.865	0.626	0.094	0.335

F23415526a397d1d3f5b0a41	16/02/98	08:19:59	000023	FFFFFFFFFFFFFFFFF464646250c7	00
F23415526a397d1d3f5b0a41	16/02/98	08:26:56	000333	FFFFFFFFFFFFFFF0956367541f5a7f7	00
F23415526a397d1d3f5b0a41	16/02/98	08:37:07	000040	FFFFFFFFFFFFFF013223271 0074741	00
F23415526a397d1d3f5b0a41	16/02/98	08:38:43	000024	FFFFFFFFFFFFFF013223271 0074741	00
F23415526a397d1d3f5b0a				9733813 62546e0	00
F23415526a397d1d3f5b0a				322355a567a702	00
F23415526a397d1d3f5b0a				37036592967171	00
F23415526a397d1d3f5b0a				444340e377b5f3	00
F23415526a397d1d3f5b0a				7323700 1425165	00
F23415526a397d1d3f5b0a				37036592967171	00
F23415526a397d1d3f5b0a				9733813 62546e0	00
F23415526a397d1d3f5b0a41	16/02/98	09:05:15	000047	FFFFFFFFFFFFFF097334032b662c3	00

Netscape: Record of F23415526a397d1d3f5b0a41

```
IMSI  F23415526a397d1d3f5b0a41

Name:
Address

====================================

Does not look fraudulent
Only national calls of no more than 5 minutes  YM
```

Figure 2. Screenshot of the graphical user interface of the integrated fraud detection system

Four discrete FDT components were developed by the project:

- A rule-based tool;
- A neural network-based tool using supervized learning;
- An unsupervized learning tool utilizing neural networks looking at A-number (call originator) data in the toll tickets;
- An unsupervized learning tool utilizing neural networks looking at B-number (call recipient) data in the toll tickets.

The four component tools were integrated into a single system FDT which we called Brutus[5]. We also built a graphical user interface

[5] The original rationale for the Brutus acronym has been mislaid, but it seemed a nice name to keep for the GUI guard-dog.

illustrated in *Figure 2*, which displays the monitoring information and alarms, and provides management of the rules and parameters of the system.

User Profiling

The fraud detection tool uses a completely data-driven approach. All the information gathered by the tool comes only from the individual user-specific toll tickets. A method must be found to profile each user and to extract relevant information from the Toll Ticket to try to detect any fraudulent use. It should be noted that no geographical information was used; this could be used to further strengthen the system at a later stage.

Absolute or Differential Analysis

Toll Tickets are data records containing details of each mobile phone call attempt that is made. Toll Tickets are transmitted to the network operator by the cells or switches that the mobile phone was communicating with at the time.

In addition to providing necessary billing information, Toll Tickets contain additional information that can be used to identify a fraudster. Existing fraud detection systems tend to interrogate sequences of Toll Tickets comparing a function of the various fields with fixed criteria known as triggers. A trigger, if activated, raises an alert status that cumulatively would lead to an investigation by the network operator. Such fixed trigger systems perform what is known as an absolute analysis of the Toll Tickets and are proficient at detecting the extremes of fraudulent activity.

Another approach to the problem is to perform a differential analysis. Here, behavioural patterns of the mobile phone are monitored by comparing its most recent activities with a history of its usage. Criteria can then be derived to use as triggers that are activated when the usage pattern of a mobile phone changes significantly over a short period of time. A change in the behaviour pattern of a mobile phone is a common characteristic in nearly all fraud scenarios excluding those committed on initial subscription where there is no behavioural pattern established.

There are many advantages to performing a differential analysis through profiling the behaviour of a user. Firstly, certain behavioural patterns may be considered anomalous for one type of user, and hence potentially indicative of fraud, but would be considered acceptable for another. With a differential analysis, flexible criteria can be developed that detect any change in usage based on a detailed history profile of user behaviour. This takes fraud detection down to the personal level comparing like with like, enabling detection of less obvious frauds that may only be noticed at the personal usage level. An absolute usage system would not detect fraud at this level. In addition, because a typical user is not a fraudster, the majority of criteria that would have triggered an alarm in an absolute usage system will be seen as a large change in behaviour in a differential usage system. In this way, a differential analysis can be seen as incorporating the absolute approach.

The Differential Approach

Most fraud indicators do not become apparent from an individual Toll Ticket. With the possible exception of a velocity trap, confidence can only be gained in detecting a real fraud through investigating a fairly long sequence of Toll Tickets. This is particularly the case when considering more subtle changes in a user's behaviour by performing a differential analysis. All the tools adopt an approach based on analysis of user profiles based on comparison of recent and longer-term behaviour histories derived from the toll ticket data.

A differential usage system requires information concerning the user's history of behaviour plus a more recent sample of the mobile phones activities. An initial approach might be to extract and encode information from Toll Tickets and to store it in record format. This would require two windows or spans over the sequence of transactions for each user. The shorter sequence is called the Current User Profile (CUP) and the longer sequence, the User Profile History (UPH).

Both profiles could be treated and maintained as finite length queues. When a new Toll Ticket arrives for a given user, the oldest entry from the UPH would be discarded and the oldest entry from the CUP would move to the back of the UPH queue. The new record encoded from the incoming Toll Ticket would then join the back of the CUP queue. Clearly, it is not optimal to search and retrieve historical information concerning a user's activities prior to each calculation, on receipt of a new Toll Ticket. A more suitable approach is to compute a single cumulative CUP and UPH for each user, from incoming Toll Tickets that can be stored as individual records in a database. To maintain the concept of having two different spans over the Toll Tickets without retaining a database record for each Toll Ticket, both profiles need to be decayed before the influence of a new Toll Ticket can be taken into consideration. A profile for each user can then be represented as a probability distribution by normalising the data in the profile. As well as being a very natural approach for the NN components, user profiling helps the rule-based component to overcome its most criticized drawback, the inflexibility of one set of rules applied to all users; user profiles allow a far more flexible, user-specific treatment.

The neural network-based tools use only differential analysis; the rule-based tool also allows absolute analysis against fixed criteria.

The FDT Components

The Rule-Based Tool

The rule-based tool must be initialized with manually set parameters — the rules. It can work in two ways: examining the toll ticket data against fixed criteria (absolute mode) and examining them against variations from previous observations (differential mode).

Neural Network-Based Tool Using Supervised Learning

The Supervised learning tool needs to be educated to set up the appropriate configuration of neurons and controlling parameters. Before exposure to the data for investigation, the system is provided with training data to initialise the system, and then fed validation data to confirm the correctness of the set-up. The system is now ready to process the operational toll tickets.

Unsupervised Learning Tool Utilising Neural Networks

An unsupervised Neural Network is used to look at how a user's behaviour changes over time, and needs no prior knowledge of fraud, unlike the previous two tools. There are two Unsupervised Neural Networks used in Brutus. An A-Number analysis, which detects changes in the user's behaviour on the phone, and an international B-Number analysis, which looks at specific changes in behaviour of a user making international calls.

Brutus

These four AI tools are integrated together to form the complete ASPeCT Fraud Detection

Tool — Brutus as in *Figure 3*. Each tool can detect separately suspicious looking or unusual behaviour and raise an alarm appropriately. A GUI has also been implemented for easy user management. For the prototype system it is run via a Web browser. The GUI can keep track of suspicious users and allows the operator to look at a specific user's calls to give the final decision whether they should be subject to further action.

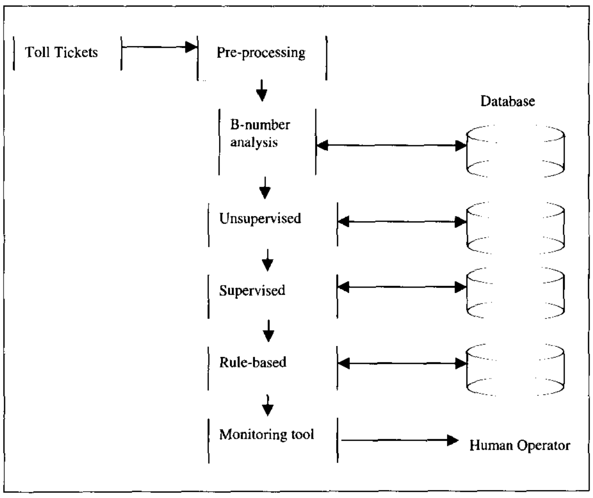


Figure 3. Brutus architecture schematic

The system operates by cascading the input data stream through the sequence of tools:

- The Unsupervised NNs — very good for novelty detection; good negative predictive value, which means that they can eliminate those users very easily for which certainly nothing is untoward, therefore used as a first filter to all incoming calls; a further reason for putting these modules high up in the chain is that their profiling could possibly also be used as input to the Supervised NN. Two unsupervised NNs are deployed:

  B-number analysis: adding information on the destination of international calls will boost the already reported performance capability of the individual tools; this module comes first because it adds information to the data-stream that could easily be used by all three subsequent tools.

  - A-number analysis: carries out the general surveillance of toll tickets for significant fluctuations in user behaviour; as there is no training or rule set-up, this tool can also recognise genuinely novel activity, possibly characteristic of a new type or variant of attack.

- The Supervised NN - efficiently pinpoints users whose behaviour is similar to previously observed and recorded fraudulent behaviour; its training routines can be tuned to bias the performance towards a high positive predictive value, i.e. when it puts a fraudulent label on a user, the subsequent modules and/or human operator can be confident that there really is something of concern.

- The Rule Based system – a good explanation for why alarms have been raised; it could, for example, be extended with extra rules to investigate why previous modules had raised an alarm; in this fashion, new fraud scenarios can possibly be identified; it can also be used to define hyper-rules based on alarms raised by other tools and not only on its own profiling/information.

The outline operation of the integrated tool is shown in *Figure 4*. Outputs are passed via the database and monitoring evaluation unit to the monitoring tool which displays its alarms to the human operator.

The ASPeCT Trial

One of the difficulties of running a convincing user-trial of our prototype system was

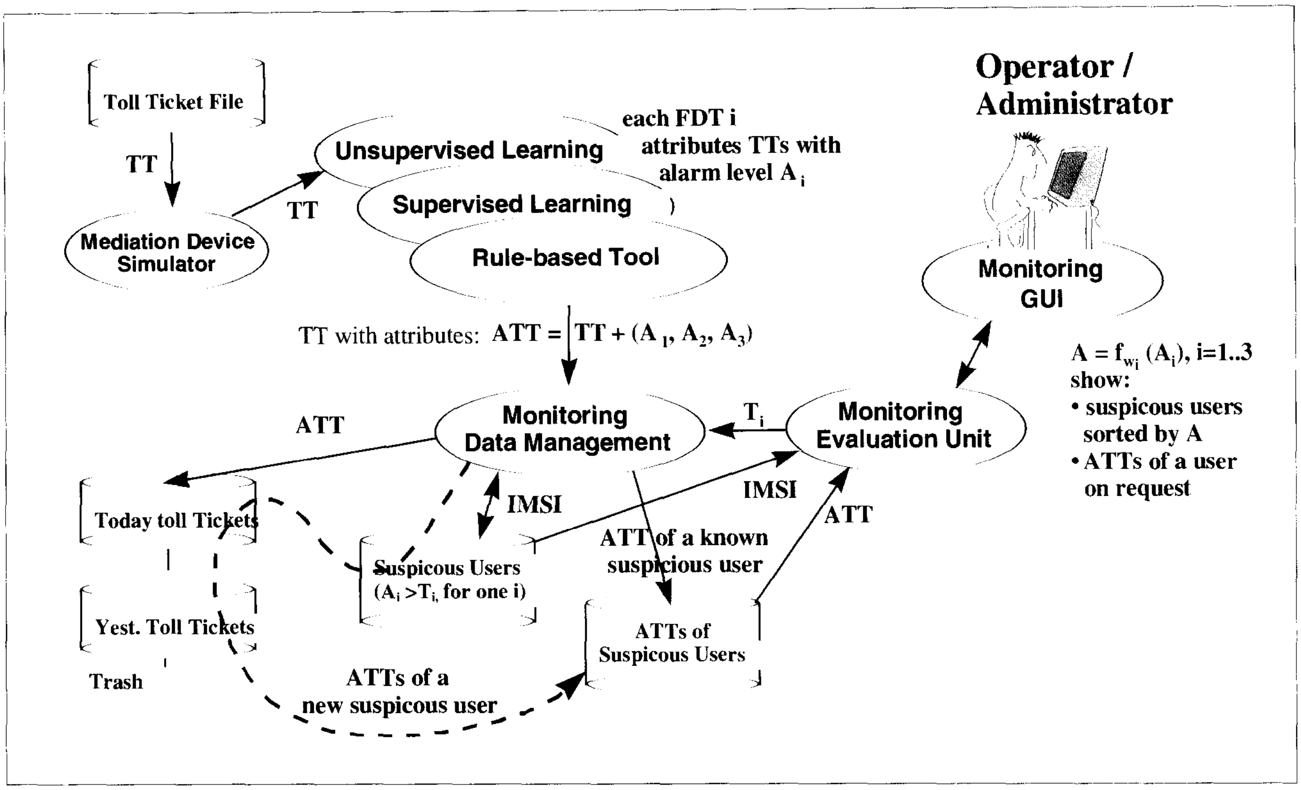

Toll Ticket File
TT
Mediation Device Simulator
TT
Unsupervised Learning
Supervised Learning
Rule-based Tool
each FDT i attributes TTs with alarm level A_i
Operator / Administrator
Monitoring GUI
TT with attributes: ATT = TT + (A_1, A_2, A_3)
$A = f_{w_i} (A_i)$, i=1..3
show:
• suspicous users sorted by A
• ATTs of a user on request
ATT
Monitoring Data Management
T_i
Monitoring Evaluation Unit
IMSI
IMSI
ATT
Today toll Tickets
Yest. Toll Tickets
Trash
Suspicous Users ($A_i > T_i$, for one i)
ATT of a known suspicious user
ATTs of Suspicous Users
ATTs of a new suspicous user

Figure 4. Monitoring within the Integrated Fraud System

obtaining sufficient toll ticket data. Great care had to be taken by network operators in sanitizing all data passed to us in order to safeguard the complete anonymity of the call records while ensuring that any feedback provided to the operators would be of use.

The data used in the trial are GSM toll tickets in an ASPeCT-specific subset of the archived Eurobill format. This particular format contains 25 fields, among which the ASPeCT tools can isolate the particularly important ones for fraud detection: A- and B-numbers (call originator and call recipient subscriber numbers), the call starting time, the duration of the call.

We obtained a set of data containing approximately four months worth of toll tickets for approximately 20 000 users. The users were chosen as a series of charged-imsi groupings to capture an expected wide range of behaviour within the data. The toll tickets were collected and stored on a daily basis. Once collected, they were merged into approximately 100 files for distribution, training and processing. From this data it would also be possible to select a smaller subset of the users to further reduce the size of the data set.

All subscriber information contained in the respective toll ticket fields, and also all information that allows distinction between individual users, was encrypted whilst preserving the 25-field format. Thus, the confidentiality of personal data was protected while the case individuality was retained. Any suspicious users that were identified could be investigated by the operators by reversing the sanitization process.

The trial system was that shown in *Figure 3* and *Figure 4*.

A billing mediator was simulated to give the effect of the near-real-time arrival of toll tickets collected from all operators.

User profiles must be swapped between disk and main memory each time a new toll ticket arrived at the fraud detection tool. The performance requirements were severe, as peak performance must exceed 30 toll tickets per second. We obtained such performance by using a simple, but optimized database tool called GDBM. The database was accessed by a key, which was the IMSI of the user and provided a content which was the concatenation of the Current User Profile and User Profile History.

Combination of the Different Tools

The common alarm level $A_{com} = f(w_1, w_2, w_3, A_1, A_2, A_3)$ was used for the ordering. The function f was used for combining the thresholds computed by all tools to a common alarm level. The weights w_i allowed users manually to adjust the influence of each tool on the common result. One of the main tasks of the trial was to determine a well-suited function on combining the results.

We opted for a well-known approach from statistical theory: logistic regression modelling. The combination function had the form $f = 1/(1+\exp(-\Sigma\, w_i A_i))$. The advantages of this combination function were as follows:

The determination of the parameters w_i was straightforward. The necessary optimization could be based fully on the individual results of the different tools (B-number analysis, unsupervised neural network, supervised neural network, and rule-based system) on a training-set similar to the one used in the development of the supervised neural network.

The number of parameters that had to be estimated was low and the optimization procedure was guaranteed to converge to an optimal solution.

The resulting parameters w_i were also statistically meaningful in that contributions with large parameter values contributed exponentially more to the probability of fraud than contributions with low parameter values. This interpretation means that our integrated tool is building an estimate of the probability of fraud on the basis of the behaviour of a user.

This logistic regression modelling provides a start estimate of the relative weighting of the individual tools. Adjusting the weights during the daily operation of the fraud detection engine would be a task for an administrator. The same holds for changing the thresholds for a minimum suspicion. An adjustable global threshold T_{com} would allow the raising of an alarm, if A_{com} exceeds T_{com}. This is meant for the critical cases where the tool should alert an operator and in a later stage, proactively propose countermeasures. In our software implementation of the fraud detection tool, the operator used a simple Web browser interface to adapt these weights manually.

From the three million or so toll tickets processed, 27 possible fraudsters were identified. Further analysis was able to clear all but four of these from operational data (mainly hire phones, changes of SIM — identity module — in the phone, and unbarring of international calling).The remaining four were to be pursued by the operators.

This performance was seen as encouraging by the operators. The ratio of false-positives to true-positives was good. Given the greatly reduced incidence of fraud resulting from GSM, the tool would be effective in identifying a significant portion of the abuse.

Legal considerations

An extensive report was written in the context of the ASPeCT-project. Its objective was the determination of the legal rules applying in the various fields of law affected by the use of fraud detection systems by mobile communications operators or service providers.

Mobile telecommunications operators use call data records for fraud detection purposes. They contain details relating to every mobile phone call attempt. Toll tickets are transmitted to the network operator by the cells or switches that the mobile phone was communicating with. The tickets are used to determine the charge to the subscriber, but they also provide information about customer usage, and thus facilitate the detection of any possible fraudulent use.

We examined four legal questions with regard to the use of fraud detection systems:

- Do operators monitoring calls on the network for fraud detection purposes, act against the fundamental principle of the confidentiality of private telecommunications? The confidential character is not limited to the content of the calls but extended to all kinds of data with regard to the call, such as the identity and location of the calling and the called parties, the time and the duration of the call, etc.
- Are operators processing call data for fraud detection purposes, controllers of the processing of personal data in the legal sense? If so, what are the consequences of the application of personal data protection rules? Which law will be applicable to the processing of call data, when more than one country is involved, as is often the case in the context of mobile communications[6]?
- Given the fact that the results of the fraud detection system are always computer-readable data, how should this data be presented as evidence in court? Will the courts in the EU Member States accept the data resulting from fraud detection systems as admissible evidence?
- If the data resulting from the fraud detection system are accepted and there is no doubt that fraud has been committed, how will the different fraud types identified in mobile telecommunications be legally qualified? Is telecommunications fraud considered as a specific type of crime or do we have to use general qualifications such as theft?

Each of these questions were dealt with in a separate chapter of the full report[7].

As far as the issue of telecommunications privacy is concerned, there seem to be three types of national legislation with regard to the possibility for network operators or service providers to process call data concerning their subscribers.

A first type of legislation does not explicitly grant an exception to network operators or

[6] This is particularly difficult to resolve: consider user a subscribing to network in country A travelling (roaming) in country X calling user b subscribing to network in country B travelling (roaming) in country Y - who has legal jurisdiction?

[7] ASPeCT Deliverable D25 – WP2.6: Legal Issues – Final Report (to be available on http://www.esat.kuleuven.ac.be/cosic/cosic.html).

service providers to process call data but accepts such practices implicitly.

A second type of legislation explicitly grants an exception to network operators to register call data as far as this is necessary for the proper functioning of the network or the provision of the telecommunications service.

A third type of legislation explicitly grants an exception to network operators or service providers to register call data for fraud detection purposes but may submit this exception to specific conditions.

It is evident that the data protection laws of the EU Member States, enacted over a period of more than 20 years, contain a wide variety of solutions, which is the precise reason why the European Commission took the initiative to propose a Directive in this field. This Directive (95/46/EC) - was enacted on 24 October 1995. All Member States of the EU were required to transpose the provisions of this Directive into their national law by 24 October 1998 at the latest.

At this time, all the Member States are changing their data protection law in order to make it compatible with the provisions of the European Directive.

An essential principle of the European data protection Directive is the so-called finality principle stating that personal data collected for a certain purpose (i.e. billing), should not be used for other — secondary — purposes, unless certain conditions have been fulfilled. One of the conditions is the duty to inform the data subject about the secondary use.

The European data protection directive also contains very specific rules regarding which law has to be applied when personal data are processed in more than one Member State. The criterion set forward by the Directive is the 'establishment of the controller'. Export of personal data outside the European Union is forbidden to countries without an 'adequate level' of personal data protection.

Electronic data is admissible as evidence in all the EU Member States. Legislation enacted in 1984 (UK) and 1992 (Ireland) ensure the admissibility of such evidence in the common law jurisdictions while the principle of free proof is used in the civil law jurisdictions to guarantee the admissibility of data as evidence. In addition, civil law courts sometimes have a broad discretion regarding what they will accept as evidence.

The report also examines the issue of how one legally qualifies various types of mobile telecommunications fraud. Does the law of the EU Member States contain a legal qualification of telecommunications fraud as a specific incrimination. Is there a specific criminal treatment of telecommunications fraud. Or do we have to fall back on traditional criminal categories such as theft, deceit, forgery, etc.

The task of qualifying different types of cellular fraud does not fit neatly into one particular field of law. In addition to qualifying the different types of cellular fraud, the report also contains the relevant legislation used to prosecute cellular fraud and the possible legal remedies available to counteract mobile fraud in the relevant member states.

Conclusions

The project produced a number of achievements, which may (individually or collectively) be taken up commercially to combat what will continue to be a significant threat to the revenues of the mobile industry, as well as being a threat to the operational well-being of a service upon which we are becoming increasingly dependent.

- Refinement of state-of-the-art AI techniques to address the specific problem of fraud detection.
- Incorporation of an unsupervised behaviour profiling component.
- Successful implementation and demonstration of individual tools, discovering their relative strengths at detecting aberrant activity in a communications network.
- Subsequent integration of the tools to combine the strengths of the individual components.
- Performance is such as to be easily scaleable to the online handling of toll tickets in near real time.
- Trials successfully identified a number of previously undetected suspicious subscribers.
- Flexible JAVA-based GUI and modular environment to facilitate development of a commercial product.
- An analysis of the current legal situation and constraints which provides a basis for future rationalisation of law and guidance to current operators and services providers.

Interest has been expressed in the commercial development of our results into fraud detection products. There is further scope for the techniques in the surveillance and management of complex systems, notably behaviour of communications networks. Even further afield, one of the academics provides consultancy on the applicability of the techniques we developed to the processing of medical diagnostic data.