00-116

De Moor B., Verrelst H., ``Fraude en fraudedetectie in mobilofoon netwerken", *Het Ingenieursblad*, no. 12, 2000, pp. 33-38., Lirias number: 178734.

Frauderen is eigen aan de mens en manifesteert zich dus ook nu in nieuwe, immateriële vormen zoals het mobilofoongebruik. Fraudedetectiesystemen vertrekken van de veelheid aan gegevens in de klantendatabanken en verwerken die tot fraude-indicatoren. Op basis van klantenprofielen en met behulp van intelligente statistische technieken kan men afleiden of bepaalde gebruikers potentiële fraudeurs zijn.

Fraude en fraudedetectie in de mobilofonie

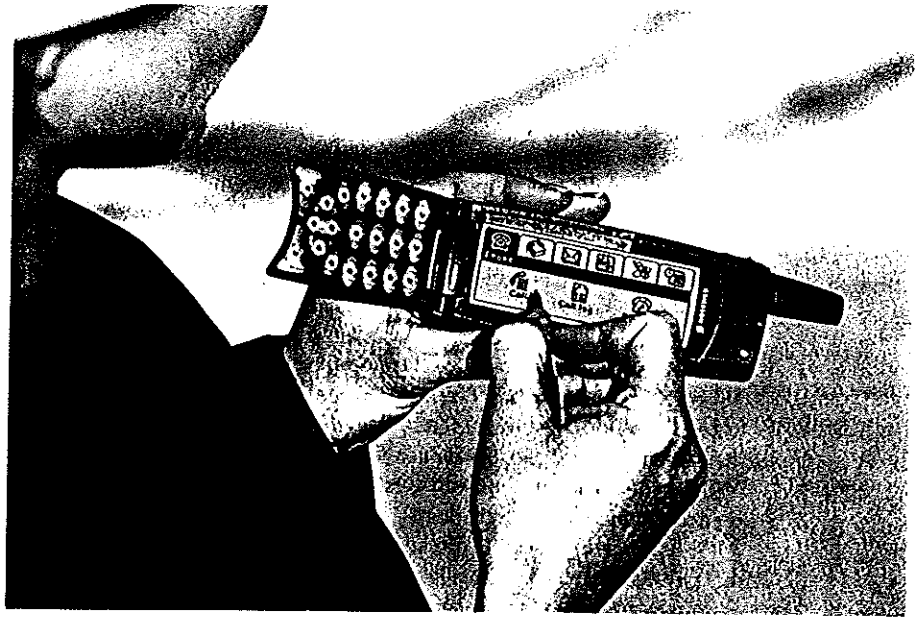
Bart DE MOOR, Herman VERRELST

Zonder twijfel is frauderen het tweede oudste beroep ter wereld. Frauderen is des mensen en daarom inherent aan elke menselijke activiteit. Denken we maar aan fraude in de sport (bv. doping), fiscale fraude, fraude met bankverrichtingen (het failliet van de Barings bank), beleggingsfraude (bv. Nigeriaanse netwerken, piramidesystemen), valsmunterij, fraude met brandstoffen, examenfraude, enz.... Frauderen is niets anders dan een moderne vorm van diefstal. Waar diefstal traditioneel geassocieerd wordt met het ontvreemden van materiële goederen, met name liquide geld, wordt fraude veelal in verband gebracht met zogenaamde witte-boordcriminaliteit. Hierbij wordt vooral gedacht aan de onrechtmatige toe-eigening van immateriële eigendommen. Voorbeelden zijn stelen van informatie, o.a. met het oog op chantage, of het vervreemden van geld via illegale financiële transacties. Deze vormen van diefstal zijn de laatste jaren prominent geworden, gekatalyseerd als ze zijn vanuit verschillende tendensen in de moderne kennismaatschappij.

Enerzijds is er een onmiskenbare ontwikkeling naar activering en waardering van immateriële zaken, zoals knowhow, kennis, expertise, ervaring, software, enz..., waarbij in vele gevallen niet alleen de daadwerkelijke waarde, maar ook het potentieel naar de toekomst toe de waarde uitmaakt. Precies omdat nu ook deze immateriële zaken een economische waarde krijgen, wordt het voor malafide geesten interessant om ze te ontvreemden.

Anderzijds is er een exponentiële toename van de graad van 'verwebbing' in onze informatiemaatschappij. Deze vindt zijn oorsprong in de groeiende dichtheid van netwerken ((mobiele) telefoon, internet, TV-kabeldistributie, multimedia- en breedbandnetwerken, pers- en andere informatiestromen, hard- en softwareplatformen in auto's, e.d.) en de toenemende mate van interactiviteit (tweerichtingsverkeer) die op elk van deze netwerken zal worden aangeboden. Naarmate onze samenleving evolueert van een biotoop naar een technotoop, nemen de opportuniteiten tot frauderen alleen maar toe. Zo bijvoorbeeld was er tien jaar geleden nauwelijks sprake van internetcriminaliteit (computerkrakers, elektronische sabotage, onderscheppen van informatie, computerterrorisme en chantage, computervirussen,...). Vandaag schat men dat voor het jaar 2000 de globale mondiale kosten veroorzaakt door internetcriminaliteit meer dan 70 miljard BEF zullen bedragen.

Maar, zoals we zullen beschrijven in dit artikel, komen er gelukkig genoeg ook betere en snellere technieken op de markt, waardoor fraudeurs efficiënter worden gedetecteerd en aangepakt. In die zin ontstaat er een soort wedloop tussen goeden en slechteriken, de fraudeurs en de bestrijders ervan.



Een artikel schrijven over fraude heeft iets inherents delicaats. Om voor de hand liggende redenen kunnen we immers de verschillende fraudemechanismen en fraudebestrijdingstechnieken niet in detail beschrijven. Dit artikel is dan ook geen wetenschappelijk exposé, waarvoor onze excuses aan lezers die wel wat meer detail hadden verwacht.

Diensten in de nieuwe economie

Hoewel we ons zullen toespitsen op fraudemechanismen en -detectie in mobiele telefonietoepassingen, zijn onze conclusies transplanteerbaar naar andere kennisdomeinen in de nieuwe economie. Voorbeelden hiervan zijn elektronische betaalsystemen, verrichtingen bij banken en kredietinstellingen via het internet, telefonisch of via betaalterminals, financiële en beurstransacties, internettoepassingen zoals e-business, zowel B2B (*business-to-business*, bv. veilingen van grondstoffen of energiebeurzen) als B2C (*business-to-customer*, bv. boodschappen via internet) en allerhande webgebaseerde diensten (zoals *Application Service Provider* diensten, waarbij software als het ware geleasd wordt, bv. medische diagnosesystemen).

Kenmerken van de kennisdomeinen

Elk van deze domeinen voldoet aan enkele typische karakteristieken:

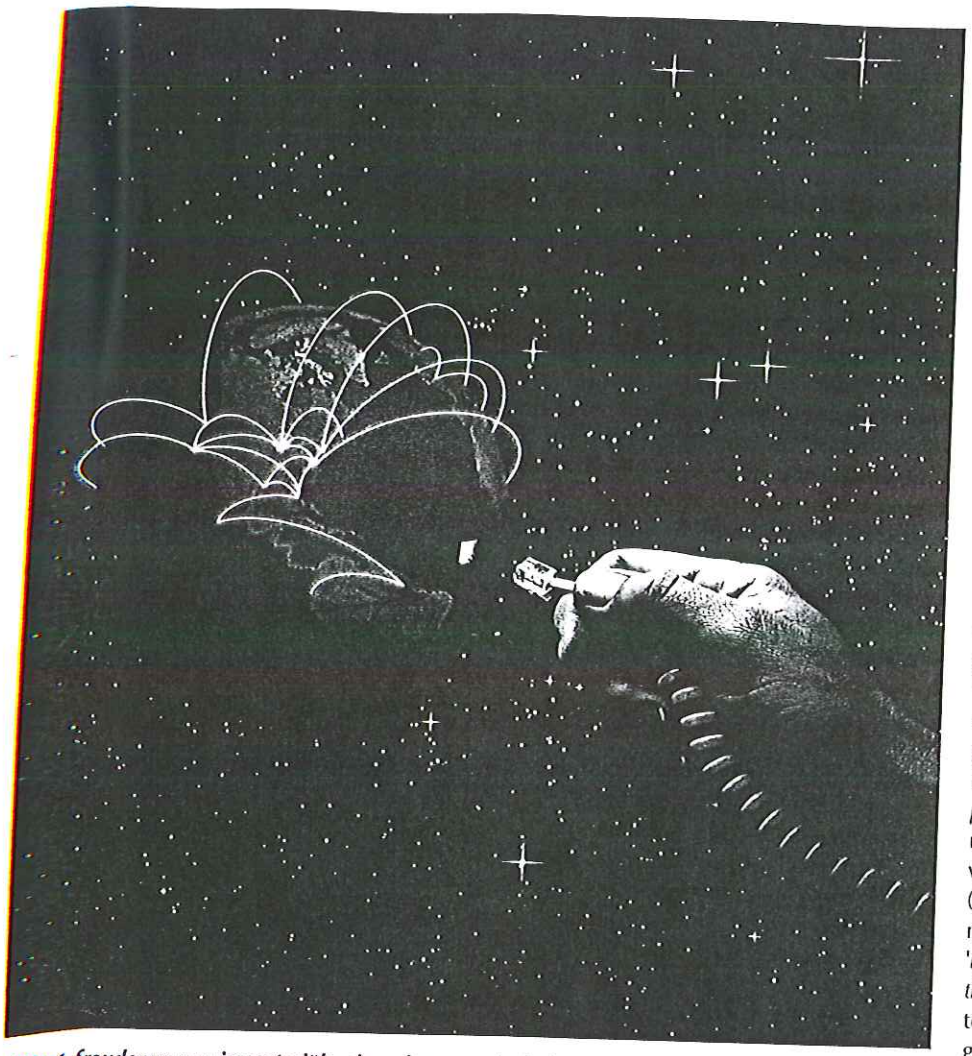
- *Grootschaligheid* : Vooreerst is er de typische grootschaligheid van het klantenbestand, dat meestal enkele tienduizenden tot honderdduizenden klanten bevat en soms wel honderdduizenden tot zelfs miljoenen potentiële klanten.
- *Registratie* : De gebruiks- en kooppatronen van elk van die klanten en geïnteresseerden wordt voortdurend en nauwgezet geregistreerd. Hierdoor wordt het mogelijk om, met behulp van allerlei numerieke technieken van 'datamining', 'clusters' van klanten te definiëren, d.w.z. groepen van klanten die binnen een groep allen een vergelijkbaar profiel hebben (bv. koopgedrag). Elke cluster kan vervolgens op een specifieke manier worden benaderd, door bijvoorbeeld verschillende tarifiëringen in te voeren voor verschillende marktsegmenten, en deze ook op gezette tijden te laten evolueren. Hierdoor behoudt men een duidelijk competitief voordeel ten opzichte van de concurrentie. In het meest extreme geval wordt er van elke individuele klant een individueel profiel bijgehouden, waardoor een volledig *'customised'* en gepersonaliseerde klantenbenadering mogelijk wordt. Het individuele profiel van de individuele klant bepaalt uiteindelijk het gamma van diensten en producten waarmee hij of zij in contact komt, bijvoorbeeld op een website. Dit wordt dan ook nog eens gekoppeld aan allerlei 'loyalty arrangements', zeg maar getrouwheidspremies, niet alleen van één enkele distributeur maar in de toekomst ook van verschillende bedrijven samen die hiertoe samenwerken.
- *On-line verwerking* : Een derde kenmerk is de snelheid en efficiëntie waarmee dit alles gebeurt, namelijk on-line. Via een telefoonlijn, een GSM-verbinding of een internetconnectie kan alles in reële tijd worden opgevolgd en eventueel gecontroleerd en wordt ook alles gestockeerd in zogenaamde *'real-time'* of *'quasi real-time databases'*.
- *Convergentie en integratie* : Een vierde kenmerk wordt best beschreven door de woorden convergentie en integratie, sinds enkele jaren de twee meest gehoorde *'buzzwords'* in de wereld van informatica, telecom en multimedia. Deze sterke trend tot het groeperen van de meest diverse functies in één apparaat of applicatie wordt gedreven door de *'technology push'* van doorgedreven miniaturisatie, betere batterijtechnologie, grotere en goedkopere data-opslagmogelijkheden, sterkere compressie-algoritmen, betere encrypterings- en beveiligingsalgoritmen.
- *Mobiliteit* : Een vijfde kenmerk is het streven naar de ultieme mobiliteit van informatie en informatiedragers. Waar Bill Gates in de jaren 80 nog het adagium lanceerde van *"A PC at every desk"*, heet het nu dat iedereen in de nabije toekomst wel drager zal zijn van een of ander *"portable device"*, *"and it is going to be wireless"* !

Mobiele telefonie als voorbeeld

Laten we nu even deze verschillende kenmerken illustreren aan de hand van de mobiele telefonie. Vooreerst is er de massiviteit van het klantenbestand. Alleen al in Vlaanderen heeft 1 op 2 mensen een GSM-toestel (GSM = *Global System for Mobile communication*). De projecties naar de nabije toekomst laten bovendien nog een forse toename zien.

Het gebruik van deze mobiele telefoondiensten wordt uiterst nauwkeurig bijgehouden door elke telecomoperator, omdat die natuurlijk in staat moet zijn om op gezette tijden facturen uit te sturen naar zijn klanten. Deze informatie bevat velden zoals het nummer van de abonnee en van de correspondent, de duur, het tijdstip en de tariefregeling van het gesprek (zonaal, interzonaal), enz.. Per GSM-gesprek worden op die manier verschillende getallen bijgehouden, wat bij de gemiddelde telecom provider een dagelijkse aangroei van de database met enkele Gigabytes vertegenwoordigt.

Niet alleen het aantal klanten groeit fors. Ook het aantal aangeboden diensten stijgt exponentieel, precies omdat dit een concurrentieel voordeel biedt. En tussen concurrenten wordt een heuse veldslag gehouden voor de meest gunstige tarifiëringen. In de goede oude tijd van de POTS (*Plain Old Telephony System*) was het allemaal eenvoudig: je haalde de hoorn van de haak, draaide een nummer en even later kreeg je je correspondent aan de lijn. Vandaag is POTS vervangen door CTI (*Computer Telephony Integration*), waarbij in een doorsnee mobiele telefoon een antwoordapparaatfunctie is voorzien, een bestand van correspondenten en nummers, een elektronische agenda en allerlei functionaliteiten om te faxen en te e-mailen. Mobiele telefoons zullen uitgroeien tot draagbare (misschien zelfs inplantbare) polyvalente *terminals*, waarbij nieuwe protocols en technologieën zoals WAP en de nieuwe UMTS-standaard deze tendens alleen maar zullen versnellen. Tegen het einde van 2000 nog zal Siemens een



Het frauderen van immateriële eigendommen is de laatste jaren gekatalyseerd door verschillende tendensen in de moderne kennismaatschappij. Enerzijds is er een onmiskenbare ontwikkeling naar activering en waardering van immateriële zaken, zoals knowhow, kennis, expertise, ervaring, software, enz... Anderzijds is er een exponentiële toename van de graad van 'verwebbing' in onze informatiemaatschappij. Deze vindt zijn oorsprong in de groeiende dichtheid van netwerken en de toenemende mate van interactiviteit (tweerichtingsverkeer) die op elk van deze netwerken zal worden aangeboden. (Foto : Belgacom)

nieuwe mobilofoon op de markt brengen die aangestuurd wordt met spraaktechnologie (*'voice dialing and command'*), WAP-functionaliteiten heeft en een infrarood modem bevat, alsook een ingebouwde mp3-speler voor muziekbestanden en een sleuf voor geheugenkaarten waarop je mp3-, Word-, Excel- en Powerpointbestanden kan bewaren, die uitwisselbaar zijn met je PC. Het hele ding weegt niet meer dan 88 gram en kan trouwens ook gebruikt worden als dictafoon.

Fraudemechanismen

Met het toenemende dienstenpakket via het globale mobilofoonnet stijgen ook de opportuniteiten tot frauderen zienderogen. Geschat wordt dat in de Verenigde Staten alleen al, per jaar 650 miljoen dollar aan inkomsten verloren gaan door fraude. Net zoals bij kredietkaarten, is diefstal van identiteit ook bij mobilofoon gebruikers een reëel risico. Het is ongelooflijk hoe onzorgvuldig mensen soms omspringen met hun toegangscode, door deze ergens zichtbaar te noteren. Dieven schrikken er ook niet voor terug om aan '*dumpster diving*' te doen, waarbij ze dergelijke confidentiële informatie gaan zoeken in iemands vuilnisbak. Een ander fraudescenario is het verkopen van telefoongesprekken tegen dumping-prijzen (bv. na diefstal van een GSM). In een stad als Parijs worden per dag enkele honderden GSM's gestolen. Meestal worden deze op straat doorverhuurd tegen een gunsttarief en, om de betrapkans te minimaliseren, na enkele uren gewoon ergens gedumpt. En zo zijn er nog verschillende andere fraudescenarios denkbaar zoals PABX (*Private Automatic Branch eXchange*) fraude (inbellen op een inbelpunt van een bedrijf van waar dan internationaal kan worden gebeld), klonen van SIM-kaarten, '*tumbling*' (multiple klonen met dan willekeurige keuze van het gebruikte nummer, ook om de betrapkans te minimaliseren), '*free phone fraud*', interne fraude (bv. misbruik van bedrijfstelefoon door werknemers), '*subscription fraud*' (veelvuldig bellen met de bedoeling nooit de eerste factuur te betalen), '*roaming fraud*' (zelfde als '*subscription fraud*', maar dan vanuit het buitenland, speculerend op een tragere doorstroming van de administratieve gegevens uit het buitenland) enz...

Fraudedetectie

Grosso modo wordt fraude opgemerkt door onverwachte en ongewone verrichtingen te detecteren. Hiertoe wordt van elke klant een bepaald profiel gemaakt, d.w.z. een statistisch model dat representatief is voor de typische gebruikerspatronen van die klant. Wanneer per gesprek 10 getallen worden bijgehouden, dan kan zo'n gesprek voorgesteld worden als een punt in een 10-dimensionale ruimte. Alle gesprekken die door een klant worden gevoerd, vormen dan een puntenwolk in die 10-dimensionale ruimte. De belangrijkste typische kenmerken van dergelijke puntenwolk worden dan berekend met behulp van geavanceerde statistische technieken en neurale netwerken.

In essentie is fraudedetectie niets anders dan het detecteren van plotse veranderingen in dergelijke voor één bepaalde klant representatieve gedragsprofielen. Wanneer iemands GSM-gebruik gekenmerkt wordt door vele, korte (enkele minuten) en lokale gesprekken rond Hasselt, dan is het abnormaal dat ineens gesprekken substantieel langer worden, vertrekkende vanuit Parijs, en dat de correspondent zich ergens in Zuid-Amerika bevindt. In dit voorbeeld zou het wel eens kunnen dat het betrokken GSM-toestel werd gestolen, en verhuurd wordt in de straten van Parijs. In een ander voorbeeld vertrekken we van een profiel van een klant die frequent interzonaal belt met gesprekken van gemiddeld enkele minuten. Plots wordt vastgesteld dat er zeer frequent wordt gebeld naar een lokaal nummer van

het vaste telefoonnet, met 'gesprekken' van slechts enkele seconden. Dit zou kunnen duiden op het feit dat het nummer van de eerlijke klant op een of andere manier ontvreemd werd door een computer hacker, die tracht paswoorden te raden van een computer waarin hij, via de GSM van de klant, tracht in te breken.

Fraudedetectie op basis van klantenprofiel

Beide voorbeelden zijn nogal extreem gekozen om de essentie van fraudedetectie duidelijk te maken: In beide gevallen wordt het profiel van de klant voorgesteld door een statistisch model dat representatief is voor de typische puntenwolk van die klant in de hoger dimensionale ruimte. Na de diefstal van identiteit, liggen de gesprekken zoals gevoerd door de fraudeur, plots in een totaal ander gebied. Deze 'migratie' wordt automatisch gedetecteerd met numerieke en statistische technieken, die hun oorsprong vinden in wat men zou kunnen noemen de 'klassieke statistiek' van hypothesetesten, classificatietechnieken en de daaruit volgende besluitvorming.
Maar moderne fraudedetectietechnieken maken vooral ook gebruik van meer geavanceerde methodes, zoals neurale netwerken of regelgebaseerde (*'rule-based'*) systemen. Vooral het incorporeren van a priori informatie, d.w.z. ervaring zoals die beschikbaar is bij fraude-experten, is van groot belang. Het zou immers nogal dom zijn om dergelijke informatie te negeren. Hiervoor worden zogenaamde Bayesiaanse netwerken gebruikt, waarvan de essentie terug te brengen is op de eeuwenoude regel van Bayes uit de waarschijnlijkheidsleer. Hierbij kan a priori informatie en kennis expliciet in rekening worden gebracht.

Lijsten van 'verdachten'

Typisch één of enkele keren per dag genereert het fraudedetectiesysteem een lijst van verdachte GSM-eigenaars. Of, beter gezegd, meestal is de eigenaar niet verdacht, maar is plots het gebruikerspatroon van zijn GSM veranderd, wat op zich verdacht kan zijn maar ook kan duiden op een veranderd gedragspatroon van een voor het overige eerlijke klant (zie verder). Vanzelfsprekend is de gegeneerde lijst van verdachte nummers typisch orde-groottes kleiner dan de lijst van alle GSM gesprekken van die dag. Het hoeft geen betoog dat de informatisering van deze methoden een must is. Voor een menselijke operator is het namelijk gewoonweg onmogelijk om visueel alle telefoongesprekken te 'screenen', gezien de dagelijkse informatietoevloed van verscheidene Gigabytes.
Wat tenslotte wél visueel wordt gescreend door de fraudeverantwoordelijke van het telecombedrijf, is de door het fraudedetectiesysteem gegenereerde lijst van verdachte nummers. In de meeste gevallen is er niets aan de hand omdat er een duidelijke aanwijsbare reden is voor een veranderd en veranderend profiel. In sommige gevallen zijn er duidelijke indicaties of vermoedens van frauduleus gebruik. Dit leidt dan onverbiddelijk tot een onmiddellijke stopzetting van de diensten voor deze bepaalde klant (*'Denial of service'*). In toenemende mate worden de beschikbare gegevens van fraudeurs ook gemeld aan de politie en andere telecomoperatoren.

Fraudedetectiesystemen = dynamische systemen

Geen enkel fraudedetectiesysteem kan statisch zijn, d.w.z. onveranderlijk in de tijd. Elk professioneel fraudedetectiesysteem moet op gezette tijden geactualiseerd worden. Twee oorzaken liggen hiervan aan de basis.
Een eerste oorzaak ontstaat in het feit dat fraudeurs niet stilzitten. Zowel op het gebied van fraudescenario's als in de gebruikte technologie is er een min of meer geleidelijke evolutie. Fraudeurs zijn bijzonder creatief in het ontwikkelen van nieuwe methodologieën om te frauderen. Deze evoluties kunnen worden opgevolgd door de statistieken van fraudescenario's aandachtig te bestuderen en ook door fraudedetectiemechanismen af en toe bij te stellen, vertrekkende van deze analyse. Telkens wanneer een

In essentie is fraudedetectie niets anders dan het detecteren van plotse veranderingen in voor één bepaalde klant representatieve gedragsprofielen. Wanneer iemands GSM-gebruik gekenmerkt wordt door vele, korte (enkele minuten) en lokale gesprekken rond Hasselt, dan is het abnormaal dat ineens gesprekken substantieel langer worden, vertrekkende vanuit Parijs, en dat de correspondent zich ergens in Zuid-Amerika bevindt. In dit voorbeeld zou het wel eens kunnen dat het betrokken GSM-toestel werd gestolen, en verhuurd wordt in de straten van Parijs.

geval van fraude wordt vastgesteld, volgt er ook een *'debrieling'* met de technische ploeg, zodat bepaalde parameters van het systeem kunnen worden bijgesteld. Wanneer zich nieuwe, voorheen ongeziene fraudemechanismen voordoen, worden deze vanzelfsprekend ook bestudeerd zodat men hun detectie kan incorporeren in het detectiesysteem.

Een tweede oorzaak ligt in het feit dat gebruikersprofielen van klanten kunnen veranderen in de tijd. Vooreerst zijn er de klassieke periodische fenomenen in elk gebruik: in de weekeinden vallen zakelijke telefoongesprekken weg, in typische vakantieperiodes wordt op andere manieren gebeld, en ook tijdens de dag zijn er pieken en dalen in het gebruik (zo bijvoorbeeld belt de schoolgaande jeugd niet tijdens de schooluren maar wel vlak ervoor en erna). Er zijn echter ook drastischer veranderingen. Het gebruikerspatroon van een schoolverlater die net aan zijn eerste job is begonnen, zal plotsklaps veranderen. Deze aspecten van tijdsvariatie stellen toch wel zeer specifieke eisen aan een fraudedetectiesysteem, omdat het voor de telecom operator ook bepaald delicaat is om iemand ten onrechte van fraude te verdenken. Paradoxaal genoeg impliceert dit dat een zeker niveau van fraude in het systeem altijd zal getolereerd moeten worden. Het is immers heel moeilijk om bepaalde, 'voorzichtige' fraudeurs te onderscheiden van soms goede klanten, op wiens profiel een grote variabiliteit aanwezig is. Het is dan ook zeer belangrijk om in fraudedetectiesystemen een zo groot mogelijke integratie na te streven van verschillende informatiebronnen. Zo kan bijvoorbeeld iemands gedragspatroon gecorreleerd worden aan zijn beroep, waardoor men het aantal valse alarmen kan beperken. Dit is een voorbeeld van zogenaamde 'differentiële analyse', waarbij alarmdrempels bepaald worden relatief t.o.v. een profiel. Dit staat dan tegenover 'absolute analyse', waarbij alarmdrempels absoluut zijn en de kans op valse alarmen bijgevolg groter.

Het opvolgen van de dynamica van klantenprofielen op korte en lange termijn is trouwens niet enkel belangrijk voor fraudedetectie. Wanneer iemands gebruikerspatroon verandert, kan dit ook duiden op het feit dat deze klant potentieel geïnteresseerd is in andere diensten. Vanuit het gezichtspunt van een telecom operator bestaat het gevaar dat zo'n klant overstapt naar de concurrentie die een beter dienstenpakket kan aanbieden. Dit noemt men 'churn'. Wanneer men een dergelijke klant detecteert, kan hij mogelijks benaderd worden met een meer gepersonaliseerd dienstenaanbod of een verleidelijker tarief. Het detecteren van klanten die gevoelig zijn voor 'churn' is een andere toepassing van de technologie die we hierboven beschreven. Gebruikers van deze technologie zijn dus niet alleen de fraude-experten, maar ook de marketing afdelingen van telecom operatoren.

Implementatie in een flexibele IT-omgeving

Een fraudedetectiesysteem kan men best implementeren in een IT-omgeving die snel, flexibel en gebruikersvriendelijk is en die bovendien naadloos geïntegreerd kan worden in het klantenopvolgingssysteem van een telecom provider. Snelheid is vanzelfsprekend essentieel. Het is immers zinloos om dagen te moeten wachten op de gehele verwerking van een databestand, om dan vast te stellen dat er fraudeurs aan het werk zijn geweest. Nochtans mag de uitdaging die uitgaat van het grote aantal gebruikers en dito gesprekken niet onderschat worden. De verwerking van verschillende Gigabyte aan getallen per dag, in quasi 'real time', is zeer rekenintensief en stelt speciale eisen aan de onderliggende numerieke algoritmen en technieken.

De 'naadloze integratie' slaat op het feit dat elke telecom provider vanzelfsprekend al eigen klantenopvolgingssystemen bezit, al was het maar om op gezette tijden te kunnen factureren. De flexibiliteit is nodig omwille van het hierboven beschreven tijdsvariante karakter van fraudemechanismen en -detectiesystemen, en natuurlijk ook omdat de veranderingen in de wereld van mobiele telefonie mekaar razendsnel opvolgen. Flexibiliteit impliceert ook dat men rekening kan houden met de specifieke vereisten en problematiek van elke telecom provider afzonderlijk. De gebruikersvriendelijkheid van het hele systeem tenslotte is uitermate belangrijk zodat snel, efficiënt en betrouwbaar kan worden opgetreden tegen fraudeurs.

Besluit

Frauderen is des mensen. Door de exponentiële toename van klanten en diensten bij de opeenvolgende generatie van mobilofoonsystemen (nu GSM, binnenkort UMTS - Universal Mobile Telephony System) wordt verwacht dat de mogelijkheden tot frauderen alleen maar zullen toenemen. De huidige integratie van beschikbare databases, geavanceerde algoritmen en detectietechnieken gebaseerd op neurale netwerken en een implementatie in een gebruikersvriendelijke software-omgeving maakt het mogelijk om betrouwbare, robuuste en op maat gemaakte fraudedetectiesystemen te ontwerpen. Hierdoor kan men het risico voor telecom operatoren en hun klanten minimaliseren.

De auteurs

Bart DE MOOR is elektro-werktuigkundig ir. (KUL 83) en doctor in de toegepaste wetenschappen (KUL 88). Hij is gewoon hoogleraar aan de K.U.Leuven en leidt er samen met 7 collega's de onderzoeksgroep SISTA/COSIC/DocArch van het departement Elektrotechniek (www.esat.kuleuven.ac.be/sista). Zijn onderzoek situeert zich in de numerieke lineaire algebra, in de systeemidentificatie en zgn. 'data-mining'-technieken, bio-informatica en de modelgebaseerde regeltechniek. Dit onderzoek werd bekroond met verschillende wetenschappelijke prijzen en werd ook gevaloriseerd in de oprichting van twee spin-off bedrijven (www.ismc.be, www.data4s.com). Bart De Moor is lid van binnen- en buitenlandse beroepsverenigingen en redactiecomité's. Hij is bestuurder van verschillende wetenschappelijke instellingen (VIB, SCK, VCBT, CLEA, Worldviews).

Herman VERRELST is elektro-werktuigkundig ir. (KUL 96). Na enkele jaren van onderzoek op het gebied van neurale netwerken, fraudedetectiesystemen en medische diagnosesystemen richtte hij de NV Data4s (www.data4s.com) op, als spin-off bedrijf van de K.U.Leuven. De activiteiten van Data4s situeren zich in het domein van de 'Customer Intelligence' (klantenprofilering en statistische gedragsanalyse in functie van CRM en fraude management) en bio-informatica (datamining van genoom databases en medische diagnosesystemen). Data4s werd opgericht begin 2000 en telt momenteel 17 medewerkers.