

George Huitema

TNO Informatie- en Communicatietechnologie

Postbus 15000

9700 CD Groningen

g.b.huitema@telecom.tno.nl

Vakantiecursus 2003

Nieuwe generatie telecommunicatietechnieken

Gebruikers van mobieltjes realiseren zich zelden hoe ingewikkeld het apparaat is waar ze mee bellen. Wiskundig gezien wordt gebruik gemaakt van uiteenlopende disciplines, zoals netwerktheorie, coderingstheorie en cryptografie. George Huitema, onderzoeker bij TNO en hoogleraar telematica bij de Rijksuniversiteit Groningen, beschrijft in dit artikel, dat eerder in de serie Vakantiecursus 2003 van het CWI verscheen, recente ontwikkelingen.

Het is meer dan honderd jaar geleden dat Bell de telefoon uitvond. Sinds die tijd heeft telecommunicatie de wereld veroverd. De com-

municatiemogelijkheden in het dagelijkse leven zijn door de invoering van digitale transmissietechnieken en de opkomst van internet enorm toegenomen. Dankzij de nieuwste technieken is het mogelijk om wereldwijd vanaf elke locatie met elke andere locatie te communiceren.

De wereld van telecommunicatie

Tegenwoordig staat huidige gebruikers een groot aantal informatie- en datadiensten ter beschikking. In de nabije toekomst zullen de nieuwe generatie vaste en mobiele breedbandige diensten de gebruikers een nog groter scala aan nieuwe communicatiediensten verschaffen. Consumenten krijgen dan beschikking over een grote diversiteit aan randapparaten en communicatiemiddelen. Door de technologische ontwikkelingen vloeien communicatie, informatie, commercie en entertainment samen in een nieuwe industrie.

Om daadwerkelijk telecommunicatiediensten te gebruiken zullen klanten zich eerst aan het netwerk kenbaar moeten maken. Hierbij wordt geverifieerd of de persoon is wie hij zegt te zijn, en of hij in kwestie gerechtigd is om van de dienst gebruik te mogen maken (*authenticatie* en *autorisatie*). Tenslotte — slechts de zon gaat voor niets op — zal ook het telecommunicatiegebruik van klanten moeten worden geregistreerd en verrekend (*accounting* en *billing*).

Telecommunicatie

Technisch gezien is telecommunicatie de overdracht van informatie over afstand, van een zendende partij (*transmitter*) naar een ontvangende partij (*receiver*). Deze overdracht gebeurt in een aantal achtereenvolgende stappen. Bij elk van deze stappen spelen wiskundige methoden en technieken een belangrijke rol. Op het eerste gezicht zou men niet denken dat bijvoorbeeld een mobiel telefoon-toestel zo veel wiskunde in zich draagt. De voortgaande ontwikkelingen van mobiele telecommunicatie maken het straks nog zo dat een mobiel meer rekenkracht in zich draagt dan de meest geavanceerde zakrekenmachine van tegenwoordig!

Om een idee van de wiskundige toepassingen bij telecommunicatie te krijgen lopen we de verschillende stappen bij het transport van informatie nu bij langs. Eerst wordt de informatiestroom omgezet in een gecomprimeerde, digitale gegevensstroom (*digitalisering* en *coding*). Daarna worden aan de datastroom allerlei redundante gegevens toegevoegd zodat foutdetectie en foutcorrectie op de te transporteren gegevens mogelijk is (*foutdetectie* en *foutcorrectie*). Vervolgens wordt de datastroom versleuteld (*encryptie*) ter voorkoming van af luisteren en ongewenste veranderingen. En tenslotte wordt voordat het signaal daadwerkelijk verzonden wordt, dit aan een geschikte zogeheten draaggolf



Figuur 1 Wereldwijde communicatie

toegevoegd (*modulatie*). Na versturing van het signaal op basis van een *communicatie-protocol*, vindt bij de ontvangende partij het omgekeerde proces plaats: het signaal wordt van de draaggolf gescheiden (*demodulatie*), de gegevens worden ontcijferd (*encryptie*) en tenslotte in de voor de ontvangende partij weer in begrijpelijk vorm teruggebracht (*encoding*).

Naast technische oplossingen voor het transporteren van informatie in netwerken, wordt in de telecommunicatiewereld ook veel techniek ingezet voor het verdelen van schaarste. De exploitatie van een communicatienetwerk wordt namelijk gekenmerkt door het zoeken naar de meest economische manier van het beheren van schaarste aan bandbreedte en transport- en dienstencapaciteit voor gebruikers. Immers gebruikers willen vanaf elke locatie, op elk tijdstip, in elke gewenste kwaliteit en met voldoende beveiliging en privacy, met andere gebruikers communiceren. Het opzetten en onderhouden van een goed telecommunicatienetwerk kost veel geld. De kunst voor een telecommunicatie-aanbieder is dan ook om tegen lage kosten een zo hoog mogelijke kwaliteit aan gebruikers te leveren. Dat hier veel wiskunde bij komt kijken, moge duidelijk zijn.

Voortdurende groei

De voortdurende groei aan communicatiemogelijkheden kent een tweetal belangrijke oorzaken. Een daarvan is de continue miniaturisatie van de micro-elektronica. De ander is het feit dat het gebruik van een bepaald medium aantrekkelijker wordt indien meer personen gebruik maken van dezelfde communicatiemiddelen. Deze twee bekende waarnemingen

gaan door het leven als de wetten van Moore en Metcalfe.

De wet van Moore

In 1965 constateerde Moore, medeoprichter van de chipfabrikant *Intel*, dat ieder jaar het aantal transistoren per cm^2 op een chip verdubbelde. Moore voorspelde dat dit in de toekomst gewoon door zou gaan. In de daarop volgende jaren is het tempo wel een beetje afgenomen maar de dichtheid verdubbelt nog steeds elke 18 maanden (vergelijk figuur 2). Een soortgelijke verdubbelingsnelheid zien we bij opslag- en geheugencapaciteit van computers, en bij telecommunicatiebandbreedte. Dit is nu wat de wet van Moore ons zegt: *Voor verschillende elementen uit de ICT-wereld geldt een exponentiële groei. Verdubbelingstijden lopen uiteen van 0,7 jaar tot 3 jaar.*

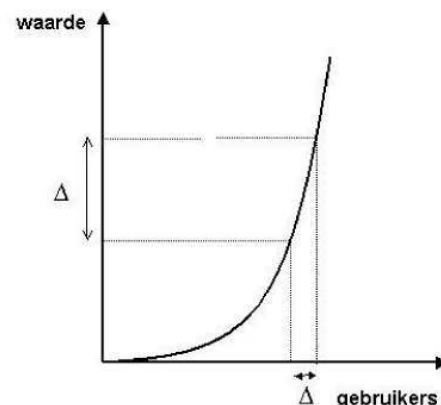
Experts verwachten dat deze 'wet' nog enkele decennia zal blijven gelden.

Door de Wet van Moore wordt het steeds aantrekkelijker voor zowel consumenten als voor bedrijven om de juiste elektronische middelen te hebben voor communicatie en voor handel te bedrijven.

De wet van Metcalfe

Metcalfe, ontwerper van het veel gebruikte Ethernet-protocol voor computernetwerken en oprichter van 3COM, leverancier van netwerksystemen, ontdekte de volgende wetmatigheid (vergelijk figuur 3): *De waarde van een communicatienetwerk is gelijk aan het kwadraat van het aantal gebruikers.*

Het versturen van mobiele tekstberichten (SMS) is hier een goed voorbeeld van. Een SMS-je versturen is van beperkt nut als er



Figuur 3 Wet van Metcalfe: De waarde van een communicatienetwerk is gelijk aan het kwadraat van het aantal gebruikers.

weinig mensen in je vrienden- of relatienetwerk zijn die er gebruik van maken. Maar als het merendeel van je relaties een mobiele telefoon heeft met deze mogelijkheid, wordt het ineens veel interessanter. Dit verklaart de snelle doorbraak van SMS de afgelopen jaren.

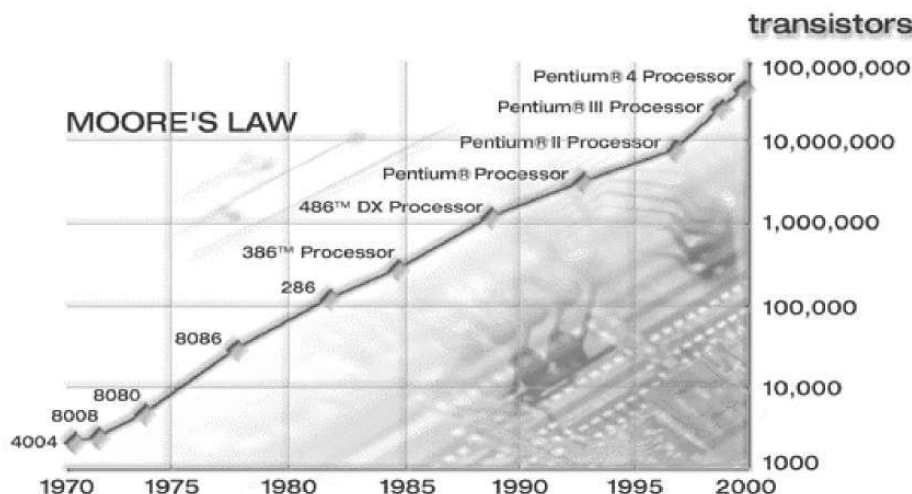
Bij de introductie van een nieuwe communicatietechnologie zal in het begin niet veel meer te merken zijn dan dat er een toenevend aantal gebruikers is. Maar als de technologie eenmaal gemeengoed geworden is, zullen er ook economische en sociale veranderingen volgen. Dit fenomeen wordt *disruption* genoemd. Bekende voorbeelden uit het verleden zijn de invoering van radio en tv. Moore's wet voorspelt dat in onze huidige digitale maatschappij het bereiken van de kritische massa steeds sneller gaat. Heden ten dage kunnen we dit met onze eigen ogen en oren constateren bij het gebruik van de pc en de mobiele telefoon.

Nieuwe generatie netwerken

In het algemeen bestaat een telecommunicatienetwerk uit een verzameling van systemen die met elkaar kunnen communiceren. Voorbeelden van telecommunicatienetwerken zijn de traditionele telefoonnetwerken en de moderne mobiele netwerken. In dit laatste geval zijn de communicerende systemen mobiele telefoons (*handhelds*). Op het gebied van netwerken zijn een aantal belangrijke ontwikkelingen te noemen.

Pakketgeschakelde netwerken

Telefoonnetwerken werken op basis van *circuitschakeling*. Wanneer een abonnee een andere abonnee belt, wordt tussen de twee telefoons een vaste geschakelde verbinding tot stand gebracht. Tijdens het bellen blijft de verbinding open staan en geen enkele andere beller kan gebruik maken van deze verbinding.



Figuur 2 De groei van de dichtheid van transistoren is exponentieel

ding voordat een van beide bellers het lopende gesprek beëindigt. Tegenover deze technologie staat *pakketschakeling*. Hierbij kan elke verbinding in het netwerk tegelijkertijd gebruikt worden door meerdere gebruikers. Er is geen specifieke, open verbinding tussen twee gebruikers, het netwerk is *connectionless*. De stroom informatiegegevens tussen gebruikers wordt opgeknippt in losse pakketjes, die elk een eigen weg door het netwerk volgen. Bij aankomst bij de ontvangende partij worden de pakketjes weer in de goede volgorde gezet tot de oorspronkelijke gegevensstroom.

Het voordeel van pakketschakeling is dat het de bandbreedte van de verbindingen beter benut (efficiëntie) en dat het goedkoper en eenvoudiger valt te implementeren. Circuitschakeling biedt in het algemeen betere beveiliging daar verbindingen niet gedeeld worden met anderen. Pakketschakeling wordt in bijna alle nieuwe generatie netwerken toegepast. Hét voorbeeld hier is het *internet* dat bestaat uit een netwerk van pakketgeschakelde netwerken.

Lokale en persoonlijke netwerken

Wireless Local Area Networks (WLAN's) zijn lokale netwerken waarbij draadloze dataoverdracht tussen gebruikers, plaatsvindt door middel van gestandaardiseerde netwerktechnologie. Momenteel wordt veelal de *IEEE 802.11b* communicatiestandaard (WiFi (Wireless Fidelity)) gebruikt die theoretisch een overdrachtssnelheid van 11 Mbps mogelijk maakt. Via kleine pc-insteekkaartjes kunnen

zo laptops en *Personal Digital Assistants* (PDA's, kleine handcomputertjes) draadloze verbindingen met internet opbouwen. Deze tekst van ongeveer 400kB zou in een fractie van een seconde van internet gehaald kunnen worden. WLAN's, ook wel *hotspots* genoemd, zijn momenteel al te vinden op vliegvelden, zakenhotels en bij sommige ketens van coffeshops.

De vrij nieuwe naam *Personal Area Network* (PAN) wordt gebruikt voor het netwerk van persoonlijke communicatie- en informatiesystemen dat in een straal van ongeveer tien meter rondom een persoon valt te onderscheiden. Hieronder vallen bijvoorbeeld de verbindingen (al of niet draadloos) tussen printers, mobiele telefoons, digitale camera's en PDA's. De communicatie bestaat doorgaans uit het overbrengen van files (onder andere plaatjes) en de synchronisatie van gegevens. De communicatietechniek *Bluetooth* is hierbij sterk in opkomst doordat de bijbehorende communicatiechips relatief goedkoop zijn en weinig energie verbruiken. De netwerken in deze categorie hebben meestal een ad-hoc-karakter, dat wil zeggen dat per gelegenheid er een netwerkconfiguratie ontstaat die het mogelijk maakt dat applicaties op de verschillende apparaten met elkaar communiceren. Hiervoor is wel een vereiste dat apparaten van verschillende leveranciers goed op elkaar aansluiten. Veel lezers zullen onder tussen wel eens in hun eigen omgeving hebben meegemaakt dat laptops, mobiele telefoons of camera's niet altijd goed samenwerken. Ondanks dat dezelfde standaarden zijn gebruikt, blijken er helaas soms verschillende implementaties door producenten gebruikt te worden.

Sinds de eerste mobiele toepassingen waarbij de communicatie tussen apparaten niet via een vaste draad verliep maar via draadloze transmissie, zijn er ondertussen al drie verschillende generaties mobiele netwerken te onderscheiden.

De *eerste generatie* (1G) is de naam voor de analoge mobiele netwerken uit het midden van de jaren 1980. Deze netwerken waren nationaal van karakter en ondersteunden slechts spraakdiensten of daaraan gerelateerde diensten zoals doorschakelen. In Nederland kenden we deze mobiele netwerken onder de naam *Auto Telefoon* (ATF). Door het nationale karakter waren deze netwerken incompatibel met elkaar en mobiele communicatie werd meer beschouwd als een bijzonderheid, zie figuur 4.

Door de steeds groeiende behoefte aan mobiele communicatie werd echter ook de



Figuur 5 Nieuwe 3G-telefoon

behoefte aan een globaal mobiel netwerk groter. Door inspanningen van internationale standaardisatie-organisaties is vanuit Europa het huidige GSM-netwerk (Global System for Mobile communications) ontstaan. Deze tweede generatie mobiele digitale communicatietechniek is een groot technisch en commercieel succes geworden. Vergeleken met de lappendekens aan mobiele netwerken in Amerika die niet goed op elkaar aansluiten, is GSM een grote Europese verworvenheid.

De *derde generatie* mobiele netwerktechnologie, 3G, is ontworpen als een volledig overkoepelend mobiel netwerk voor globale mobiele communicatie. In Europa is het *Universal Mobile Telecommunication System* (UMTS) de 3G-standaard geworden. In 3G worden zowel spraak als multimedia ondersteund, zie figuur 5. Bovendien omvat 3G internetsdiensten.

Recentelijk zijn met name in de Aziatische wereld de ontwikkelingen voor 4G al opgestart, zie [1]. Deze volgende generatie mobiele netwerken moet 3G weer verder brengen en alle vormen van spraak en datadiensten in mobiele context omvatten.

Doordat mobiele technologie steeds kleiner en goedkoper wordt, vinden we in allerlei apparaten en gebruiksvoorwerpen steeds vaker mobiele *devices* geplaatst die onderling communiceren. De verwachting is dat deze specifieke communicatie tussen apparaten (we spreken hier van *Machine-2-Machine* communicatie) op den duur ruimschoots de omvang van mobiele communicatie tussen personen overtreft. Voor een visie op deze onzichtbare mobiele ontwikkelingen zie [16].

Wiskunde voor mobiele netwerken

Vergeleken met de traditionele vaste netwerken kennen mobiele netwerken geheel eigen specifieke wiskundige problemen. Zo zijn



Figuur 4 ATF-telefoon Carvox 2453 uit 1985 (Museum voor Communicatie, Den Haag)

One-way algorithmes

Een one-way algoritme

$$H(m) = h$$

berekent aan de hand van een input m op eenvoudige en snelle wijze het resultaat h . De weg terug, het berekenen van de input m bij een gegeven resultaat is praktisch onmogelijk. Bovendien geldt dat het praktisch onmogelijk is om bij een input m een andere input m' , $m \neq m'$ te vinden met $H(m) = H(m')$.

bijvoorbeeld voor de realisatie van eerste en tweede generatie mobiel netwerken uitgebreide netwerkplanningstools ontwikkeld, die aangeven waar mobiele masten moeten worden geplaatst opdat mobiele gebruikers volledige en uniforme dekking hebben van hun mobiele telefoon. Doordat het gebruik van 3G-netwerken een geheel andere verdeling van dataverkeer over het netwerk laat zien dan bij de huidige 2G-netwerken, worden momenteel geheel nieuwe 3G-specifieke planningstools ontwikkeld [10]. Verder zijn er ook nieuwe toegangstechnieken ontwikkeld, onder de naam *Wideband Code Division Multiple Access* (WCDMA). Op basis van lineaire algebra wordt er voor gezorgd dat gebruikers in een 3G-netwerk elkaar zo weinig mogelijk storen.

Een andere nieuwe ontwikkeling is dat 3G-Netwerken ook verschillende kwaliteitsklassen voor diensten mogelijk maken, zoals het bekijken van videobeelden bij verschillende bandbreedten. Het toekennen en garanderen van bepaalde kwaliteitsniveaus (*Quality of Service*, QoS) berust op geavanceerde wiskundige technieken, zie [14, 22].

Voor de nieuwe generatie mobiele netwerken valt in het algemeen op te merken dat steeds méér verschillende wiskundedisciplines worden toegepast. Om enkele gebieden te noemen:

- Security (complexe cryptografische algoritmen),
- Op internet gebaseerde communicatie (verkeersmodellering), zie [15],
- Bestellen van goederen via mobiele telefoon (digitale handtekeningen en sleutelsystemen),
- Op locatie gebaseerde diensten (snelle geometrische algoritmen),
- Systeemspecificaties en prototypen (wiskundige modelleringstechnieken),
- Beheer van mobiele toestellen en van de dienstenplatformen in het mobiele net-

werk (management van complexe softwaresystemen).

Een scala aan nieuwe communicatie- en informatiediensten

De wereld van nieuwe telecommunicatiediensten kan op verschillende manieren worden ingedeeld. Hieronder volgt een eenvoudige, brede indeling (zie [3]), die een duidelijk beeld geeft van de verschillen tussen de soorten diensten, zoals wie communiceert met wie, welke transacties vinden er plaats, et cetera.

- Interpersoonlijke communicatie
- Informatie en entertainment (Infotainment)
- Zakelijke diensten
- Persoonlijk ondernemen

Bij Interpersoonlijke communicatie vindt het communiceren plaats tussen personen onderling, tegenwoordig ook vaak *Person-2-Person* (P-2-P) genoemd. De communicatie gebeurt via telefoongesprekken, e-mail en het naar elkaar sturen van mobiele tekstberichten (SMS). Opkomende diensten in deze categorie zijn onder andere het sturen van mobiele multimedia berichten (MMS), zoals een foto'tje dat gemaakt is met de mobiele telefoon zelf.

Diensten die informatie verschaffen of de gebruiker enig vermaak geven, vallen onder de categorie infotainment. Tot dit gebied behoren onder andere nieuwsdiensten, spelletjes (games), moppen, muziek en informatie over sport. Een groot marktaandeel in deze categorie vormen de sexinformatiediensten

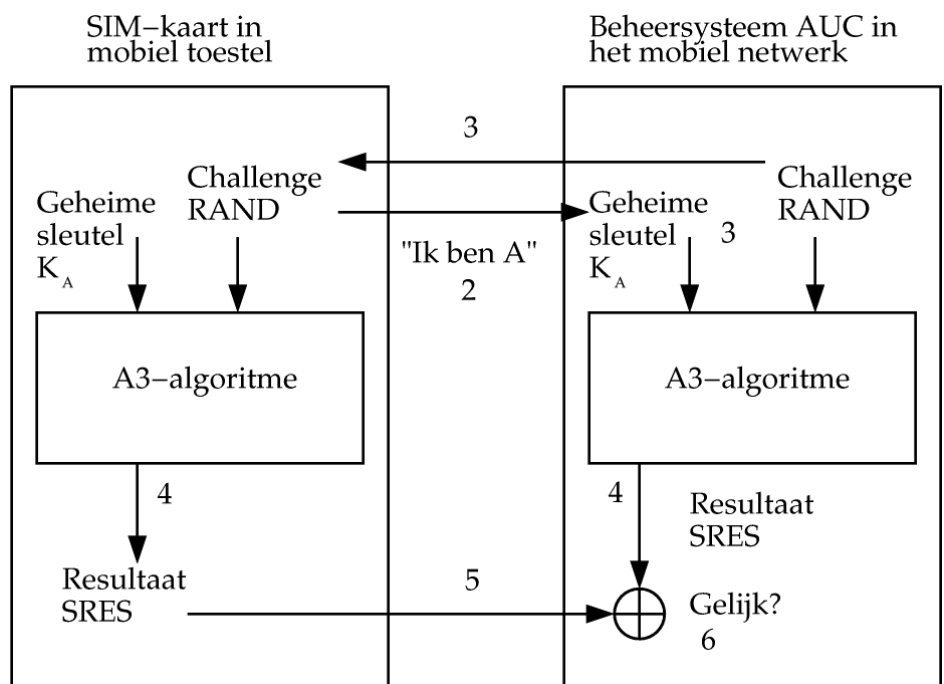
(adult content).

De belangrijkste zakelijke diensten zijn e-mail en toegang tot bedrijfsnetwerken. Andere diensten in deze categorie hebben betrekking op het raadplegen van lijsten met informatie zoals adressen en plaatjes en verder het beheer van elektronische agenda's.

Tot de categorie persoonlijk ondernemen rekenen we diensten waarmee individuele personen financiële transacties uitvoeren. Voorbeelden hiervan zijn het overboeken van geld tussen rekeningen, bijvoorbeeld het gebruik van girofoon en het doen van betalingen vanuit een soort elektronische portemonnee, de *wallet*, die op een pc of mobiel toestel is geïnstalleerd. Per betaaldienst zal de mate van security verschillend zijn. Bij betalingen van grote bedragen zal het hogere incasso-risico natuurlijk afgedekt moeten worden door een strengere vorm van security (lees: complexere cryptografische technieken). Verder behoren tot deze categorie ook financiële groepsdiensten zoals het opwaarderen van de prepaidtegoeden van de kinderen vanuit het vaste telefoonabonnement van één van de ouders. Veel diensten uit de financiële categorie zijn gekoppeld aan diensten uit de andere categorieën. Zo zijn bijvoorbeeld veel infotainment-diensten gekoppeld aan betaaldiensten, zie [2].

Aanbieden van diensten aan klanten

Telecommunicatiediensten kunnen niet zomaar door klanten gebruikt worden. Voordat de klant toegang krijgt zal hij eerst zijn iden-



Figuur 6 Authenticatie van mobiele gebruiker

titeit kenbaar moeten maken. Dan kan de dienstaanbieder eerst verifiëren of de klant is wie hij zegt te zijn en of hij geautoriseerd is om de dienst te gebruiken. Deze verificatiestappen heten respectievelijk *authenticatie* en *autorisatie*. Een andere belangrijke stap bij het aanbieden van diensten is het registreren van hoe klanten precies de diensten gebruiken. Dit zogenaamde *accountingproces* is een belangrijke bron van gegevens voor de verrekening met de klant van het dienstgebruik. In totaal spreken we van een *AAA-proces* (Authenticatie, Autorisatie, Accounting).

De voorbeelden hieronder zijn gekozen uit de mobiele wereld. Immers, juist bij mobiele netwerken spelen AAA-processen een belangrijke rol vanwege de mobiliteit van de gebruikers, het gebruik van de radioweg voor transmissie en het niet nagelvast zijn van mobiele toestellen. Er is zo des meer kans op het aannemen van een andere identiteit door gebruikers. Bij elk van de AAA-processen spelen wiskundige methoden en technieken een rol.

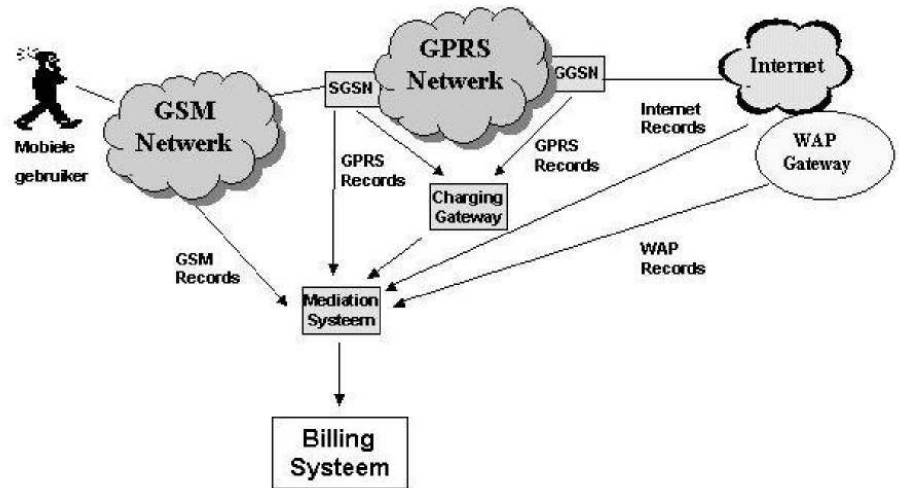
Case: authenticatie en autorisatie

Het authenticatie- en autorisatieproces kent twee fasen:

- *Toegang krijgen tot het mobiele toestel* Dit is een eenvoudige stap. Voordat een gebruiker zijn mobiel toestel kan gebruiken dient hij eerst een *Personal Identification Number* (PIN) in te voeren. Dit nummer wordt vergeleken met de code die de gebruiker ooit in zijn toestel op de zogenaamde SIM-kaart (*Subscriber Identity Module*) (een klein chipkaartje dat een klant krijgt van zijn mobiel bedrijf) heeft opgeslagen. De PIN dient alleen maar om lokaal de toegang tot het mobiele toestel te autoriseren en wordt niet over de radioweg gezonden.
- *Toegang krijgen tot het mobiele netwerk* Na PIN-controle zal verder voordat een klant diensten kan gebruiken, de identiteit van de klant door middel van zijn SIM-kaart gecheckt worden. Basis van dit authenticatieproces is het rekenalgoritme A_3 dat zowel in de SIM-kaart als in een beheersysteem, het *Authenticatie Centrum* (AUC), van het mobiele netwerk bevindt, zie [4]. Het A_3 -algoritme is een zogenaamd *one-way* algoritme (zie inzet).

Het authenticatieproces verloopt in een aantal stappen:

1. Na de PIN-controle zoekt het mobiele toestel automatisch contact met het mobiele netwerk.
2. De identiteit A die in de SIM-kaart zit, wordt door het toestel automatisch naar het mo-



Figuur 7 Accounting van GPRS-diensten

biele netwerk gestuurd. In de SIM-kaart bevindt zich ook een geheime sleutel K_A .

3. Het beheersysteem AUC zoekt vervolgens in een klanteninformatiesysteem de bij A behorende geheime sleutel K_A . In het AUC wordt bij deze gebruikerssessie random een 128-bitsgetal RAND gegenereerd die het mobiele netwerk op haar beurt weer naar het toestel stuurt.
4. Zowel het AUC als de SIM-kaart berekenen met het A_3 -algoritme aan de hand van de input RAND en K_A het resultaat SRES (Signed Result).
5. Het mobiel toestel stuurt het berekende getal SRES naar het mobiele netwerk.
6. In het AUC wordt het daar berekende getal SRES vergeleken met het ontvangen getal SRES. Indien beide getallen overeenkomen krijgt het mobiele toestel (gebruiker A) toegang tot het netwerk om de beschikbare mobiele diensten te gebruiken. Bij elk gebruik van een dienst kan deze authenticatie-procedure opnieuw doorlopen worden.

Door het one-way karakter van het A_3 -algoritme is het gebruik van de radioweg voor het versturen van de identiteit A en de getallen RAND en SRES zonder veel risico. Omdat het mobiele toestel door het netwerk uitgedaagd wordt om SRES te berekenen heet het getal RAND hier een 'challenge'. Voor een zeer lezenswaardige inleiding over het beveiligd toegang krijgen tot netwerken en systemen, zie [8].

Nadat de gebruiker in het netwerk bekend is geworden vindt er nog een nadere autorisatie plaats. Zo wordt onder andere voor prepaid gebruikers gecheckt of er voldoende beltegoed is.

Accounting

Bij elk telefoongesprek, of meer in het algemeen, bij elke telecommunicatiedienst die een klant gebruikt, worden in het netwerk gebruiksgegevens vastgelegd over, onder andere, wie de dienst gebruikt, op welk tijdstip, hoe lang de sessie duurt en specifieke technische netwerkgegevens. We spreken hiervan *accounting* of *metering*. (Opmerking: de term *accounting* wordt in andere contexten ook wel gebruikt om aan te duiden dat er tussen twee partijen een verrekening plaats vindt, zoals bij internationaal belverkeer.)

Een belangrijk aspect van accounting is het vastleggen van informatie over wat gebruikers doen in het telecommunicatienetwerk om de afgenomen diensten te kunnen verrekenen. De geregistreerde gebruiksgegevens zijn echter bovendien uitgangspunt voor een groot aantal andere bedrijfsinterne beheerprocessen, zoals het dynamisch configureren van netwerken naar actuele behoeften, het tijdig signaleren van noodzakelijk onderhoud, het beheren van service-afspraken met klanten en het maken van data-analyses voor onder andere fraudebestrijding, prijsstelling en marketing.

De accountinggegevens worden op allerlei plaatsen in het netwerk gegenereerd. Dat kan zijn in specifieke netwerkelementen zoals een centrale (*switch*), *router*, of *gateway* maar ook in specifieke servers die deel uitmaken van dienstenplatformen voor het leveren van informatiediensten. Bij een gewoon telefoongesprek wordt na afloop van het gesprek softwarematig een blok van gegevens aangemaakt, een *Call Detail Record* (CDR). Dit gespreksrecord is ongeveer 150 bytes groot en bevat, onder andere, het nummer van degene die belt (A-nummer), het gebelde nummer (B-

nummer), het begintijdstip en gespreksduur. Bij accounting van telefoniediensten gaat het om gigantische hoeveelheden informatie die uiteindelijk verwerkt moeten worden tot nota's voor klanten. Naar schatting worden er in Nederland dagelijks alleen al meer dan honderdmiljoen gewone, mobiele telefoongesprekken en SMS-jes verrekend.

Geldt de accounting van telefoniediensten al als een behoorlijk omvangrijk dataverwerkingsproces, het registratieproces bij nieuwe generatie telecommunicatiediensten is nog complexer. Ten eerste worden bij het gebruik van zo'n dienst vaak tegelijkertijd op meer-

dere plaatsen in het netwerk gegevens aangeemaakt. Immers bij deze, meestal internetachtige diensten zijn vaak simultaan meerdere dienstaanbieders betrokken die allemaal een bepaalde dienstcomponent leveren, zie [13].

Verder vraagt de aard van de dienst doorgaans om registratie van geheel nieuwe record-parameters. Zo is de registratie van verstreken tijd niet altijd meer aan de orde maar is juist de hoeveelheid getransporteerde bits of de waarde van de opgehaalde beltoon relevant.

Ook is de registratie complexer omdat bij deze nieuwe generatie van diensten niet slechts één gegeven wordt geregistreerd maar een continue stroom van internetgegevens (events en loggings) wordt gegenereerd. Deze stroom aan gebruiksgegevens kan oplopen tot tientallen gegevens per seconde.

Verder geldt in het bijzonder voor mobiele diensten dat de klant deze overal wil gebruiken en hij dus ook terecht kan komen in de netwerken van andere (buitenlandse) telecommunicatieaanbieders. Dit kan leiden tot ingewikkelde accountingsituaties. Indien bijvoorbeeld een mobiele abonnee in het buitenland belt (we spreken van *roaming*), wordt in dat bewuste buitenlandse netwerk een call record aangemaakt dat vervolgens naar het thuisnetwerk van de mobiele beller wordt gestuurd.

Nadat de accountinggegevens zijn gegenereerd worden deze vervolgens centraal in het netwerk verzameld om daarna uiteindelijk in het *facturering*- of *billingsysteem* tot nota's verwerkt te worden.

Ter illustratie staat in figuur 7 een schematisch overzicht van de diverse plaatsen in het huidige mobiele GPRS-netwerk (General Packet Radio Service) waar accountinggegevens worden gegenereerd. Het GPRS-netwerk bestaat uit het GSM-netwerk waaraan een pakketgeschakeld datanetwerk is toegevoegd. Het GPRS-netwerk vormt daarmee een generatie mobiel netwerk (2.5G) tussen GSM en 3G in.

Bij GPRS-diensten worden er op minstens vijf verschillende netwerklocaties gebruiksgegevens in de vorm van call records aangeemaakt. Te weten:

1. De *Gateway GPRS Support Node* (GGSN); informatie over de verbindingen vanuit het GPRS-netwerk met het internet.
2. De *Serving GPRS Support Node* (SGSN); registratie van het gebruik van het GPRS-netwerk.
3. De *Charging Gateway*; gecombineerde gegevens van de informatie uit de SGSN en GGSN

4. Internet; registratie van gebruik van specifieke internet-componenten
5. *WAP Gateway* (Wireless Access Protocol); registratie van het gebruik van specifieke informatie voor mobiele gebruikers.

Verzamelen van accountinggegevens

De accountinggegevens die op diverse plaatsen in een telecommunicatienetwerk zijn geregistreerd worden door een centraal verzamelstelsel bij elkaar gebracht om tenslotte in een billingsysteem tot rekeningen voor klanten verwerkt te worden. Het verzamelstelsel, ook wel *Mediation* geheten, verzamelt niet alleen de gegevens maar checkt deze ook nog op formaatfouten, corrigeert ze eventueel en brengt alle gegevens op een uniform formaat zodat de verdere verwerking gemakkelijk wordt. Het verzamelen kan op twee manieren gebeuren. Ten eerste kunnen de netwerksystemen die gegevens hebben gegenereerd deze zelf opsturen naar de Mediation, of de Mediation zelf vraagt om de gegevens, het zogenaamde *pollen*. Afhankelijk van de soort verrekening die door klanten of aanbieder gekozen wordt zal een verzamelwijze worden gekozen. Hier wordt verder ingegaan op het *pollen* van de accountinggegevens.

Pollen van accountinggegevens

Er wordt uitgegaan van het verzamelstelsel Mediation, dat de verschillende netwerklocaties om de beurt vraagt hun gegenereerde accounting- of gebruiksgegevens op te sturen. Dit *pollen* van de verschillende netwerklocaties kost echter tijd. Deze tijd is, onder andere, afhankelijk van de hoeveelheid gegevens die in een bepaalde periode op deze locatie worden gegenereerd. We zoeken nu naar een efficiënt polling-schema waardoor in het billingsysteem zo actueel mogelijk het gebruik (lees: saldo) per klant bijgehouden kan worden. Daar de gegevens van de Mediation direct doorgestuurd worden naar het billingsysteem, definiëren we de volgende doelstelling: *vind een polling-schema zodanig dat de accountinggegevens zo weinig mogelijk verouderd in de Mediation terechtkomen.*

Veel kwantitatieve aspecten van telecommunicatienetwerken- en systemen worden bestudeerd als toepassingsgebied van de theorie van wachtrijen en prestatieanalyse, zie bijvoorbeeld [18]. De algemene theorie van pollingmodellen is hierbinnen weer een geheel eigen wiskundige discipline, zie bijvoorbeeld [19–20]. Het klassieke polling-model gaat uit van een aantal wachtrijen waar klanten arriveren die door een gemeenschappelijke bediende om de beurt bezocht

Het Poissonproces

Een stochastisch proces van gebeurtenissen (aankomsten) heet een Poisson-proces met intensiteit λ als geldt dat voor elke $t > 0$ de stochastische variabele X die het aantal aankomsten telt in T seconden, een Poisson-verdeling heeft met parameter $\alpha = \lambda T$.

Dat wil zeggen, voor de kansen p_i geldt

$$p_i = P\{X = i\} = \frac{\alpha^i e^{-\alpha}}{i!} \text{ voor } i = 0, 1, 2, \dots$$

Simpel is na te gaan dat het verwachte aantal aankomsten in T seconden gelijk is aan

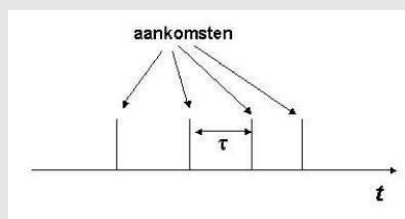
$$EX = \sum_{i=0}^{\infty} i p_i = \alpha = \lambda T.$$

Equivalent met de eis dat X een Poisson-verdeling heeft, is de eis dat de tijdsintervallen Y tussen de aankomsten van het stochastische proces (zie figuur 8) onafhankelijke stochastische variabelen zijn met een negatief-exponentiële verdeling gegeven door de kansdichtheid

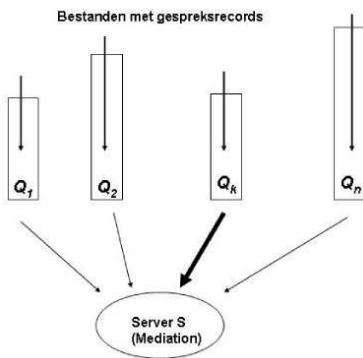
$$f_Y(\tau) = \lambda e^{-\lambda \tau} \text{ voor } \tau \geq 0.$$

Het is eenvoudig na te gaan dat de verwachte waarde EY gelijk is aan

$$EY = \int_0^{\infty} \tau f_Y(\tau) d\tau = \frac{1}{\lambda}.$$



Figuur 8 Een Poisson-aankomstproces



Figuur 9 Netwerklocaties Q_k wordt gepold

worden. Van belang is nu de volgorde van de wachtrijen die de bediende afloopt, het *polling-schema*. Daarnaast is de *service discipline* van belang hoeveel klanten bediend worden tijdens een bezoek en is van belang de tijd die het kost om te schakelen tussen de verschillende wachtrijen.

Er zijn diverse manieren om een polling-schema voor accountinggegevens op te stellen. Een eenvoudige manier is om cyclisch elk netwerkllocatie aan te doen en alle daar gegenereerde gegevens op te halen. De volgorde van te bezoeken locaties kan vast liggen (*statische polling*) of voortdurend aangepast worden. Zo kunnen we bijvoorbeeld na elke pollingssessie van een locatie de volgende te polen locatie bepalen (*dynamische polling*) of pas een nieuwe tabel met volgorden opstellen na het doorlopen van de huidige pollingtabel (*semi-dynamische polling*). In het algemeen geldt dat de gemiddelde wachttijd (*veroudering*) van files bij statische polling-schema's groter is dan bij semi-dynamische en dynamische schema's.

Hier bespreken we echter specifieke statische polling-schema's waarbij het polling-schema bestaat uit vaste tijden waarop de locaties met gebruiksgegevens worden aangedaan. Dit zijn de zogenaamde *Fixed Time Polling-schema's* (zie inzet verderop). Deze schema's zijn van belang omdat mediationsoftware soms alleen zulke schema's ondersteunen. Fixed Time Polling-schema's worden ook in bredere context gebruikt op het gebied van communicatieprotocollen, computerarchitecturen, roostering van personeel en taken en dienstregelingen in het openbaar vervoer gebruikt.

Case: Fixed Time Polling-schema's

We volgen de notaties en concepten uit [5–6]. Uitgangspunt is een server S die de wachtrijen $Q_1, \dots, Q_n$ bedient. In de context van het verzamelen van accountinggegevens is S de Me-

diation en zijn de Q_i de netwerkllocaties waar de gebruiksgegevens opgehaald moeten worden, zie figuur 9. De gegevens worden niet per stuk opgehaald maar per bestand (*file*). Als de gespreksrecords binnenkomen worden deze eerst in bestanden opgeslagen. Als het bestand een vaste lengte heeft bereikt, wordt het bestand afgesloten en is vervolgens beschikbaar om gepold te worden. De klanten in de wachtrijen Q_i zijn zo deze afgesloten databestanden.

We veronderstellen dat de wachtrijen Q_i oneindige opslagcapaciteit hebben. Immers in de praktijk hebben de netwerkllocaties, meestal centrales, een grote opslagcapaciteit welke voldoende is voor meerdere dagen. Verder veronderstellen we dat gesprekken op een centrale aankomen volgens een *Poisson-proces* (zie inzet).

De aankomsttijden op de netwerkllocaties van deze accountingbestanden worden bepaald door de tijd die het kost om een bestand te vullen met de geregistreerde gespreksrecords. De bedieningstijd van een wachtrij hangt af van de lengte van deze bestanden en van de transportsnelheid tussen de netwerkllocatie en de Mediation.

We nemen aan dat de server S de wachtrijen volgens de *gated procedure* bedient: alle bestanden die tijdens het begin van een pollingssessie afgesloten waren op deze netwerkllocatie, worden opgehaald. Merk op dat voor een pollingtabel met vaste tijden hierdoor wel eens een conflict kan ontstaan indien de server nog niet klaar is bij een wachtrij. In de praktijk gaan we ervan uit dat de Mediation altijd meerdere communicatiekanalen heeft en dat dit probleem zich dus niet voordoet. Zie de inzet.

Stel λ_i ($i = 1, \dots, n$) is de aankomstintensiteit bij wachtrij i . EW_i is de gemiddelde wachttijd (exclusief bedieningsduur) van een willekeurige klant bij wachtrij i . Er geldt dat voor de bezettingsgraad ρ_i van wachtrij i , $\rho_i = \lambda \beta_i$, waarbij β_i de verwachte bedieningsduur is van een klant in i . Definieer λ de totale aankomstintensiteit, dan is

$$\lambda = \sum_{i=1}^n \lambda_i.$$

Voor EW , de gemiddelde totale wachttijd voor een willekeurige klant, geldt dat

$$EW = \sum_{i=1}^n \frac{\lambda_i}{\lambda} EW_i$$

Zij C de totale cyclustijd die de server nodig heeft om één keer de gehele pollingtabel

te doorlopen. Verder definiëren we de deelcyclustijden C_k ($k = 1, \dots, m$) als de k^e deelcyclustijd, de tijd tussen de start van het k^e bezoek aan de netwerkllocatie P_k en de start van het volgende bezoek aan dezelfde locatie. Hier geldt dat $m + 1$ gelijk is aan 1, etc.

Er geldt dan dat de cyclustijd C gelijk is aan het totaal van de bezoektijden

$$C = \sum_{l=1}^m T_l.$$

Eenvoudig is in te zien dat de cyclustijd ge-

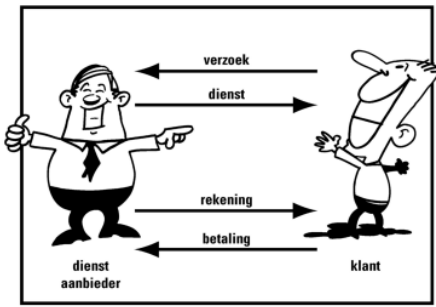
Fixed Time Pollingschema's

Nummer de te pollen netwerkllocaties $Q_1, \dots, Q_n$ van $1, \dots, n$. Een Fixed Time Polling-schema is een paar (P, T) met de vector $P = (P_1, \dots, P_m)$, de pollingtabel van te pollen netwerkllocaties, en de vector $T = (T_1, \dots, T_m)$ de tussenbezoektijden van het polling-schema. Hier is $P_k \in \{1, \dots, n\}$ en T_k is de tijd tussen de start van het k^e bezoek en de start van het $(k+1)^e$ bezoek voor $k = 1, \dots, m$. Na m keer is de gehele pollingtabel doorlopen en wordt de tabel weer van voren af aan opnieuw doorlopen. Op basis van de tussentijden T_k kunnen zo vanaf een gegeven begintijdstip de exacte tijdstippen van het polling-schema worden vastgesteld.

In figuur 10 staat een voorbeeld. Er zijn vier netwerkllocaties die volgens de tabel gepold worden. Zo wordt bijvoorbeeld de locatie Q_3 per cyclus drie keer gepold en wel op de eerste, vierde en zesde keer.

Index pollings- tabel (i)	Netwerk- locatie (P_i)	Tussen- bezoek- tijd (T_i)
1	3	T_1
2	1	T_2
3	4	T_3
4	3	T_4
5	2	T_5
6	3	T_6
7	4	T_7
8	1	T_8
9	2	T_9
10	4	T_{10}

Figuur 10 Voorbeeld van een Fixed Time Polling-tabel ($m = 10$, $n = 4$)



Figuur 11 Het verrekenen van diensten

lijk is aan het totaal van alle deelcyclustijden corresponderend bij elke keuze van een netwerkllocatie i

$$C = \sum_{\{k:P_k=i\}} C_k \text{ voor } i = 1, \dots, n.$$

Tenslotte, definieer de bezoekfrequenties m_i aan locatie i

$$m_i = |\{k : P_k = i\}| \text{ voor } i = 1, \dots, n$$

Er geldt dan voor de lengte m van de polling-tabel

$$m = \sum_{i=1}^n m_i$$

Gemakkelijk valt na te gaan dat voor de pollingtabel uit figuur 10 geldt $m_1 = 2, m_2 = 2, m_3 = 3$ en $m_4 = 3$.

We komen tot de volgende probleemstelling: *Construeer een Fixed Time Polling-schema zodanig dat EW , de gemiddelde totale wachttijd voor een willekeurige klant minimaal is.*

Oplossing

We zoeken een geschikt paar (P, T) . Dat wil zeggen we bepalen de lengte m van de tabel, de bezoekfrequenties voor elke wachtrij, de bezoeksvolgorde en de bezoektussentijden.

Dit optimaliseringsprobleem is uiterst complex, echter door middel van een heuristische aanpak, uitgaande van een aantal benaderingen, blijkt in drie opeenvolgende stappen een bijna optimale oplossing gevonden te kunnen worden.

1. Bepaling van de bezoekfrequenties $m_1, \dots, m_n$ voor elke wachtrij $1, \dots, n$. Op basis van de volgende benadering van de gemiddelde totale wachttijd EW

$$EW \approx C \sum_{i=1}^n \frac{\lambda_i(1 + \rho_i)}{2m_i}$$

vinden we de bezoekfrequenties.

2. Bepaling van de bezoeksvolgorde van de netwerkllocatie $P_1, \dots, P_m$.

Om de bezoeksvolgorde vast te stellen, wordt gebruik gemaakt van een methode die op basis van de Gulden Snede zo goed mogelijk de bezoeken aan de verschillende wachtrijen gelijk spreidt. Dat wil zeggen, zij X_k het aantal bezoeken tussen de start van het k^e bezoek aan netwerkllocatie P_k en het volgende bezoek aan deze netwerkllocatie, dan verdeelt deze methode zo goed mogelijk de bezoeken opdat de getallen X_k gelijk zijn. Voor meer details zie [7].

3. Bepaling van de tussenbezoektijden $T_1, \dots, T_m$.

Tenslotte, leiden we de tussenbezoektijden af uit een stel lineaire vergelijkingen waarvan de coëfficiënten bepaald zijn door de aankomstintensiteiten λ_i , de transmissietijden en de omschakeltijden tussen de wachtrijen i .

Uit numerieke simulaties met echte data van een aantal telefooncentrales is gebleken dat ten opzichte van de standaard mediationsoftware, het volgens bovenstaande stappen geconstrueerde Fixed Time Polling-schema, een reductie van 80% van de gemiddelde totale wachttijd opleverde.

Verrekenen van telecommunicatiediensten

Verrekening of *billing* is de financiële afhandeling van het leveren van diensten aan klanten, zie figuur 11.

De afrekening met klanten is voor bedrijven hét belangrijkste gereedschap om de behoeften van klanten te begrijpen, en om in te schatten hoe goed daaraan voldaan wordt, zie [11].

Typerend voor de billing van telecommunicatiediensten is dat van veel gebruikers, verspreid over een uitgestrekt netwerk, gebruik makend van veel verschillende randapparaten, de gebruiksgegevens worden geregistreerd. Dit is precies de situatie die we ook aantreffen bij veel andere bedrijfstakken. Denk daarbij bijvoorbeeld aan de afrekening van utiliteitsdiensten zoals gas-, water- of energiebedrijven, de betaling van reizen en ondersteunende diensten bij openbaarvervoerbedrijven en de verrekening door de overheid van het gebruik van tolwegen.

In het totale billingproces zijn een vijftal voor de hand liggende stappen te onderscheiden. De eerste twee zijn boven al besproken.

- de registratie van het gebruik (accounting)
- het verzamelen van alle geregistreerde verbruiksgegevens,
- het tarifieren van de gegevens,
- het op de nota plaatsen van de getarifeerde

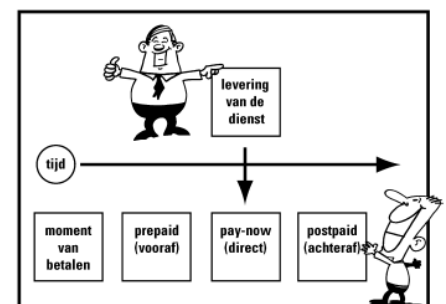
de gegevens,

- het presenteren van de nota aan de klanten en tot slot
- het incasseren van de verschuldigde bedragen.

Het verrekeningsproces is in totaal een complex bedrijfsproces doordat er een hele verzameling van technische en organisatorische processen mee gemoeid is, die geïntegreerd uitgevoerd moeten worden. Deze deelprocessen strekken zich uit door alle beheerlagen van het bedrijf en hebben directe interactie met soortgelijke processen in het domein van klanten en businesspartners.

Juist bij de nieuwe generatie telecommunicatiediensten zullen business partners nauwgezet op billinggebied moeten samenwerken. Dit heeft tot gevolg dat allerlei billingprotocollen en -interfaces gestandaardiseerd moeten worden en op elkaar afgestemd. Een voorbeeld van zulke samenwerking is de huidige veel voorkomende situatie waarbij dienstaanbieders (De Telegraaf, ANWB, KNMI, etc.) meeliften op de nota van de grote telecommunicatiebedrijven. De telecombedrijven hebben reeds een verrekeningsrelatie met klanten. Op deze nota wordt naast het aandeel van het telecombedrijf (netwerkaccess en datatransport) ook het informatie- of contentdeel van de dienst de klant in rekening gebracht en geïncasseerd. Na aftrek van commissie, immers het telecombedrijf draagt het incassorisico, worden de opbrengsten van de informatie aan de dienstaanbieder gegeven.

Als grote billinguitdaging geldt het kunnen correleren van de gebruiksgegevens van het datatransportdeel van een dienst en het informatiedeel. Anders gezegd, precies te weten welke britten bij welke dienst hoort. Met deze functionaliteit zouden aanbieders aantrekkelijke prijsplannen aan klanten kunnen aanbieden, zoals happy hours waarbij klanten slechts een stukprijs betalen voor een opgehaald plaatje maar niet het benodigde datatransport. Het correlatieprobleem is momenteel een open probleem op het gebied



Figuur 12 Soort verrekening is afhankelijk van het moment van betalen

van gegevens- en procesmodellering. Dit probleemgebied vereist nader onderzoek naar simultane internet accountingprocessen bij aanbieders van diensten en telecomoperators. In het bijzonder wordt gezocht naar snelle matchingsalgoritmen voor grote hoeveelheden data.

Soorten van verrekeningsmethoden

Er zijn diverse soorten van verrekening mogelijk afhankelijk van de betalingswijze door klanten, vooraf aan het daadwerkelijke gebruik van de dienst (*prepaid*), direct (*paynow*) of achteraf (*postpaid*), zie figuur 12.

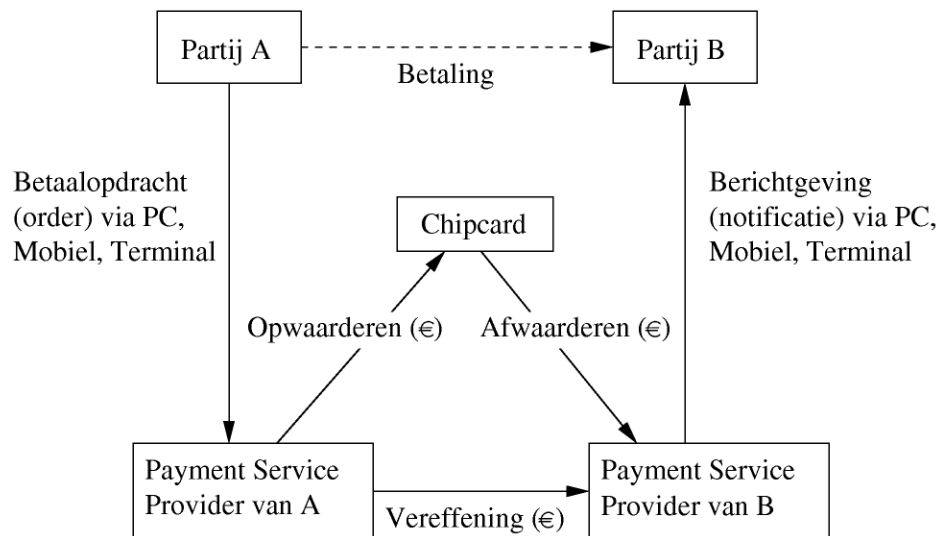
Moment van betalen

In gang gezet door *Telecom Italia* deed 'prepaid-bellen' vanaf 1995 zijn intrede in de telecomwereld. Mobiele operators boorden in rap tempo nieuwe marktsegmenten aan door naast een gewoon standaardabonnement de mogelijkheid te bieden om te bellen op basis van een beltegoed. Prepaid-bellen is erg cultureel bepaald, zo wordt in Scandinavische landen en in Japan nauwelijks prepaid gebruikt. Doordat belbedrijven aantrekkelijke abonnementen en toestellen bieden bij de invoering van nieuwe telecommunicatiediensten lijkt het aandeel prepaid-bellers in het algemeen af te nemen.

Voor de volledigheid van dit overzicht geldt dat er ook telecommunicatiediensten zijn waar klanten niet voor betalen. Voorbeelden van deze gratis diensten zijn de gratis 0800-telefoonnummers en veel gratis internetdiensten. De kosten van het gebruik worden hierbij door derden betaald. Voor het 0800-nummer is dat de eigenaar van het nummer en voor veel gratis internetdiensten zijn dat de adverteerders.

Mobiele- en internetbetalingen

Onderdeel van het billingproces is het incasso-proces waarbij de klant gevraagd wordt om te betalen. Het gebied van mobiele- en internetbetalingen wordt gekenmerkt door telkens opduikende nieuwe initiatieven, proeven en systemen, zie voor de aardigheid [9]. Er wordt driftig gezocht naar eenvoudige, veilige en goedkope betalingssystemen. Tot nu toe is er nog steeds niet een algemeen geaccepteerd elektronisch betaalmiddel op de markt verschenen. Er is ondertussen een kip-ei-situatie ontstaan waarbij on line aanbieders geen grote omzetten hebben door het ontbreken van een grootschalig betaalsysteem. En er is geen alom beschikbaar betaalsysteem omdat niemand wil investeren in de bijbehorende introductie. Bij billing via inter-



Figuur 13 Afhandeling van elektronische betalingen via Payment Service Providers

net, ook wel *e-billing* genaamd, kunnen klanten hun gebruiksgegevens en nota's via een vaste of mobiele terminal direct opvragen en eventueel betalen. Klanten hebben hierdoor sneller, altijd en overal inzage in hun telecommunicatiekosten.

Het betalingsproces omvat een aantal stappen, zie figuur 13. Voor meer details en een goede inleiding over beveiliging van netwerken en diensten, zie [21].

Stel dat Partij A geld wil overmaken naar Partij B op elektronische wijze via een mobiel toestel, een pc of een geldterminal in een winkel of op straat.

1. Partij A geeft een betaalopdracht door middel van een van de genoemde terminals aan zijn *Payment Service Provider*. Veelal is dit zijn eigen bank maar het kan ook een andere gespecialiseerde financiële partij zijn.
2. De *Payment Provider* van A zoekt nu contact met de *Payment Provider* van de begunstigde Partij B. De *Payment Provider* van B verhoogt nu het banksaldo van B met het bedrag dat A wil overmaken.
3. Tenslotte ontvangt Partij B een bevestiging van zijn *Payment Provider* dat Partij A een bepaalde hoeveelheid geld naar hem heeft overgemaakt.

Een andere manier om elektronisch geld over te maken is het gebruik maken van elektronisch geld (*digital money*) dat gebruikers op bijvoorbeeld een chipcard hebben staan.

Het gebruik van elektronisch geld en mobiel- internetbetalingen vereist dat deze financiële methoden beschermd zijn tegen fraudeurs en hackers. Het moet bijvoorbeeld onmogelijk zijn om nieuw geld aan te maken, geld dubbel uit te geven of geld van

andermans rekeningen te plukken. Hiervoor zijn uitgebreide beveiligingstechnieken ontwikkeld die sterk gebaseerd zijn op wiskundige cryptografische technieken, zie onder andere [8, 21].

Hieronder wordt nader ingegaan op het gebruik van openbare-sleutelsystemen (*public-key cryptosystem*) om bij de betalingsstappen 1, 2 en 3 te verifiëren dat het verzonden betalingsbericht niet veranderd is en van de genoemde partij afkomstig is. Dit wordt toegelicht aan de hand van het bekende RSA-algoritme. Dit algoritme is genoemd naar de ontdekkers Rivest, Shamir en Adleman (1978) van het bekende onderzoeksinstituut MIT in Boston.

Case: Openbare-sleutel algoritme RSA

Het algoritme is een voorbeeld van de eerder genoemde one-way methoden. De gebruikte grote priemgetallen maken het praktisch onmogelijk om het algoritme te kraken. Het algoritme bestaat uit de volgende stappen.

1. Kies twee grote priemgetallen p en q .
2. Op basis hiervan bereken de getallen $n = p \times q$ en $z = (p - 1) \times (q - 1)$.
3. Kies een getal d dat relatief priem is met het getal z .
4. Tenslotte, bereken het getal e zodanig dat $e \times d = 1 \mod z$.

Stel nu dat de *Payment Service Provider* van A, PSP_A een vertrouwelijk betalingsbericht m wil sturen naar de *Payment Service Provider* van B, PSP_B . PSP_A wil dat alleen PSP_B het bericht m kan lezen.

Neem aan dat de lengte van het bericht m kleiner is dan n . Deel anders het bericht m eerst op in kleinere stukken. PSP_A versleutelt nu het bericht m met de openbare coderings-

sleutel E_B van PSP_B door te berekenen

$$c = E_B(m) = m^e \pmod n$$

Het bericht c wordt nu verzonden door PSP_A naar PSP_B en daar door PSP_B ontcijferd door het toepassen van zijn eigen geheime decodingssleutel D_B

$$D_B(c) = c^d \pmod n$$

Door de getaltheoretische eigenschappen van het RSA-algoritme geldt nu

$$D_B(c) = D_B(E_B(m)) = m$$

De Payment Service Provider PSP_B heeft hiermee het oorspronkelijke bericht van PSP_A kunnen ontcijferen.

In de praktijk is het gebruik van RSA behoorlijk langzaam (7,4 kbit/s bij 1024-bits priemgetallen p en q). Het gebruik van een ander algoritme, DES (*Data Encryption Standard*), levert bij een geschikte implementatie duizenden factoren snelheidswinst op, zie [17].

Rekenen aan verrekening

Vergeleken met veel andere bedrijfsprocessen is billing een omvangrijk, complex en daardoor duur proces. De meeste kosten voor het leveren van diensten zitten in de kosten van billing. Voor sommige dienstaanbiede-

ders is het onmogelijk om bepaalde diensten aan te bieden omdat de kosten voor billing meer zouden bedragen dan het bedrag van de dienst zelf.

Billing vereist dat op een kosteneffectieve manier gebruiksgegevens worden gegenereerd en verzameld. Voor informatiediensten waarbij gebruikers steeds maar kleine hoeveelheden informatie (*content*) opvragen is onderzoek naar geschikte, betaalbare billing-mechanismen, de zogenaamde micro payments zeer gewenst. De huidige situatie leidt tot een dilemma. Enerzijds moeten content-items juist zeer laag geprijsd zijn willen gebruikers het afnemen, terwijl anderzijds de waarde van het item niet te laag moet zijn wil de registratie en de verwerking van betalingsgegevens nog rendabel zijn.

Mogelijke oplossingsrichtingen zijn het aan gebruikers beschikbaar stellen van elektronische portemonnees en het registreren van gebruik op handhelds in plaats van in het netwerk. Een geheel andere oplossingsrichting is *statistische billing*. Hierbij worden niet precies alle giga-hoeveelheden gebruiksgegevens in netwerken bijgehouden, dat is juist te kostbaar, maar worden, gegeven een zeker betrouwbaarheidsniveau, slechts schattingen gemaakt over het verbruik. Ook kan, in plaats van kostbare real-time transacties, kosten worden bespaard door het opsparen op netwerkklocaties van accountinggegevens. Een kenmerkend voorbeeld vormen de voor

de detailhandel goedkopere chipbetalingen dan pinbetalingen.

Klanten zoeken naar lage tarieven

Naast dat billing geld kost levert billing juist ook geld op. Marketeers in bedrijven bepalen de hoogte van de tarieven en de verschillende soorten prijsplannen en tariefstructuren. Ook hier zal er veel gerekend moeten worden om de meest geschikte (lees: lucratieve) tarieven, ook in vergelijking met andere aanbieders te vinden. In de praktijk worden veel simulaties met de verschillende voorstellen gedaan op verzamelingen met echt netwerkverkeer (gebruiksgegevens van klanten).

Voor klanten geldt het omgekeerde. Zij zijn ook geïnteresseerd in de tarieven maar willen juist de meest voordelige tarieven bepalen, in het bijzonder tussen de verschillende aanbieders. Om klanten een goed advies te geven, verzamelt de succesvolle internetondernemer Ben Woldering (op 14-jarige leeftijd al begonnen!), alle tariefgegevens van telecommunicatieleveranciers (mobiel, gewone telefonie, internet). Bezoekers van zijn sites (onder andere www.bellen.nl) krijgen zo gemakkelijk antwoorden op vragen welke aanbieder de goedkoopste is. ←

Dankwoord

Ik dank Jan van Maanen en Rob van der Mei voor het kritisch doorlezen van deze tekst.

Literatuur

- 4G. Zie website <http://users.ece.gatech.edu/~jxie/4G/#NEW>
- T.T. Ahonen, *m-Profits, Making Money from 3G Services*, Wiley, 2002.
- T.T. Ahonen, J. Barrett, *Services for UMTS, Creating Killer applications in 3G*, Wiley, 2002.
- R. Bekkers, *GSM in detail*, Kluwer, 1999.
- S.C. Borst, *Polling Systems*, Proefschrift Katholieke Universiteit Brabant, 1994.
- S.C. Borst, O.J. Boxma, J.H.A. Harink, G.B. Huitema, 'Optimization of fixed time polling schemes', *Telecommunication Systems*, (3) (1994), p. 31–59.
- O.J. Boxma, H. Levy, J.A. Westrate, 'Optimization of polling systems', in: P.J.B. King, I. Mitrani, R.J. Pooley (eds.), *Proc. Performance '90*, North-Holland, Amsterdam, 1991, p. 349–361.
- J. van de Craats, *Pasjes en pincodes*, Aramith Uitgevers Bloemendaal, 1991.
- Electronic Payment Schemes. Zie www.w3.org/ECCommerce/roadmap.html
- E. Fledderus, 'Wiskundig modelleren in Mobiele Telecommunicatie', *ITW Nieuws* 1 (10) (2000).
- G.B. Huitema, *Van de nota een deugd maken*, Oratie Rijksuniversiteit Groningen, 2002. Voor een pdf-file, zie www.research.kpn.com/headline.bekijk.asp?hid=1758.
- R.E. Kooij, R.D. van der Mei, J.G. Beerends, 'Internet Telefonie', *Natuur & Techniek*, juli 2001, p. 66–72.
- M. van Le, B.J.F. van Beijnum, G.B. Huitema, *Flexible Real-time Service Accounting Architecture*, Technische Universiteit Twente, 2003.
- R.D. van der Mei, 'Verkeersmodelleren van netwerken', *Nieuw Archief voor Wiskunde* 5/1, december 2000, p. 390–396.
- R.D. van der Mei, 'Wiskunde in Telecommunicatienetwerken', Vakantiecursus 2001, Experimentele Wiskunde. *CWI Syllabus* 49 (2001), p. 111–123.
- R. Meijer, *De Telerevolutie*, Oratie Universiteit van Amsterdam, 2002.
- RSA Fast (1999). www.rsasecurity.com, RSA Laboratories.
- F.C. Schoute, *Prestatie-analyse van telecommunicatiesystemen*, Kluwer, 1989. Voor een pdf-file, zie <http://mmc.et.tudelft.nl/presan/pab.html>.
- H. Takagi, *Analysis of Polling Systems*, The MIT Press, Cambridge, 1986.
- H. Takagi, 'Queueing analysis of polling models: an update', in: H. Takagi (ed.), *Stochastic Analysis of Computer and Communication Systems*, North-Holland, Amsterdam, 1990, p. 267–318.
- A.S. Tanenbaum, M. van Steen, *Distributed Systems*, Prentice Hall, 2002. In het bijzonder Hoofdstuk 8 over Security en sectie 8.7 over Electronic Payment Systems.
- R. Vranken, R.D. van der Mei, R.E. Kooij, J.L. van den Berg, 'Performance of TCP with Multiple Priority Classes', *Proceedings International Seminar Telecommunication Networks and Teletraffic Theory*, 2002, p. 78–87.