Johann Wolfgang Goethe-Universität
Frankfurt am Main

Fachbereich Informatik (20) *Praktische Informatik* PD Dr. R. Brause

Neuronales Data Mining zur Mißbrauchserkennung bei Kreditkartentransaktionen

R. Brause, T. Langsdorf, M. Hepp

Veröffentlicht in der englischen Version als "*Neural Data Mining for Credit Card Fraud Detection*, Proceedings of the IEEE International Conference on Tools for Artificial Intelligence ICTAI99, Chicago, Nov. 1999, IEEE Press 1999"

Neuronales Data Mining zur Mißbrauchserkennung bei Kreditkartentransaktionen

R. Brause,[1] T. Langsdorf [1], M. Hepp[2]

[1]J.W.Goethe-Universität, Frankfurt a. M.,
[2]Gesellschaft f. Zahlungssysteme GZS, Frankfurt a. M., Germany

Abstrakt

Die Verhinderung von Kreditkartenbetrug ist eine wichtige Anwendung für Vorhersagetechniken. Eines der Hauptprobleme bei der Anwendung von Techniken der Neuroinformatik ist die notwendige hohe Diagnosequalität: Da nur eine von 1000 finanziellen Transaktionen problematisch ist, kann ein Diagnoseerfolg von weniger als 99,9 % nicht als annehmbar angesehen werden.

Basierend auf diesen speziellen Verhältnissen für Kreditkartentransaktionen müssen deshalb völlig neue Konzepte entwickelt werden. Dieser Beitrag zeigt wie hochentwickelte Data Mining-Technik und neuronale Netzalgorithmen miteinander erfolgreich kombiniert werden können, um eine hohe Mißbrauchserkennung mit einer niedrigen Fehlalarmrate erreichen.

1 Einführung

Die Vorhersage des Verhaltens der Benutzer von Finanzsystemen ist in einer Vielzahl von Situationen vorteilhaft. Wenn man Kundenbewegungen, Kaufverhalten oder Kundenpräferenzen vorhersagen kann, ist es möglich, größere Geldsummen oder andere Ressourcen zu sparen. Eine der interessantesten Anwendungsfelder ist die Vorhersage von Mißbrauch bei Krediten, insbesondere der Mißbrauch bei Kreditkartenzahlungen. Für den hohen Datenverkehr von 400,000 Transaktionen pro Tag und einer Mißbrauchsschaden von ca. 18 Mill. DM pro Jahr ermöglicht eine Mißbrauchsreduzierung um 1% eine Ersparnis von 1,8 Millionen Mark pro Jahr.

Natürlich werden normalerweise alle Transaktionen, von denen Mißbrauch bekannt ist, nicht zugelassen. Allerdings gibt es Transaktionen von unbescholtenen Konten, bei denen Experten von vornherein sagen können, daß diese Transaktionen wahrscheinlich von gerade gestohlenen Kreditkarten oder betrügerischen Händlern herrühren und deshalb zu einem Mißbrauch führen werden. Die Aufgabe besteht also darin, einen Mißbrauch zu verhüten *bevor* er als solcher kenntlich wird.

Mit wachsender Zahl von Transaktionen ist es Menschen nicht mehr möglich, alle zu kontrollieren. Zur Abhilfe kann man die Erfahrungen der Experten in ein Expertensystem transferieren. Dieser traditionelle Ansatz hat den Nachteil, daß das Expertenwissen (falls man es überhaupt explizit fassen kann) schnell mit neuen Formen organisierter Kriminalität und neuen Mustern von Mißbrauch veraltet. Um mit dieser Entwicklung Schritt zu halten ist es nicht nötig, Mißbrauchsmodelle wie in [5] fest zu definieren, sondern sie dynamisch neu lernen und –anpassen zu lassen. Dieser Beitrag behandelt die speziellen Probleme dieser Data Mining Anwendung und versucht, sie mit einem kombinierten wahrscheinlichkeitstheoretischen und neuronal-adaptiven Ansatz zu lösen. Basis dafür sind die Kreditkartendaten, die von der GZS, einer Finanzinstitution, zur Verfügung gestellt worden sind.

Datenmodellierung

Die Transaktionsdaten werden durch besondere Proportionen charakterisiert:

- Die Wahrscheinlichkeit eines Mißbrauchs ist sehr gering (0.2%) und wurde noch durch spezielle Vorverarbeitung mit Hilfe eines konventionellen Mißbraucherkennungssy-

stems auf 0,1% erniedrigt.

- Die meisten der 38 Datenfelder (ungefähr 26 Felder) per Transaktion enthalten symbolische Daten wie Händlerkodierung, Kontonummer, Kundenname etc.
- Ein symbolisches Feld kann sehr wenige Werte (Ausprägungen) enthalten wie beispielsweise zwei (z.B. den Typ der Kreditkarte) als auch sehr viele,wie beispielsweise mehrere hunderttausend Händlercodes.
- Die Vertrauensschwelle für den Abbruch einer Transaktion ist sehr subjektiv und hängt von der aktuellen Kundenpolitik des Kreditkartenunternehmens ab. In unserem Fall wurde für alle Transaktionen mit einer Mißbrauchsvermutung von 10% oder höher auf Überprüfung oder Abbruch entschieden.

Diese Datenproportionen haben mehrere Implikationen. Bei der sehr geringen Mißbrauchsrate von 0,1% hat die konstante, „dumme“ Diagnose „Transaktion ist OK“ eine Erfolgsrate von 99,9%. Der Wert aller Diagnosen mit weniger als diesen 99,9% (z.B. [3] mit 92.5% oder [7] mit 50%) ist zweifelhaft.

Unser Hauptziel besteht also darin, den Prozentsatz korrekter Diagnosen zu maximieren und gleichzeitig den Prozentsatz der Fehlalarme und der nicht erkannten Mißbrauchsfälle zu minimieren.

2 Untersuchung der symbolischen Daten

Eine Transaktion kann als Datentupel $\mathbf{x} = (x_1,..,x_n)$ mit den Merkmalen x_i angesehen werden. Bei der Analyse unterscheiden wir zwischen kategorischen, symbolischen Merkmalen (wie z.B. Art der Kreditkarte: VISA oder MasterCard) und den analogen, numerischen Daten wie z.B. Zeitpunkt oder Betrag in DM. Betrachten wir nun zuerst die symbolischen Daten.

Unser Konzept zur Analyse von symbolischen Daten beruht hauptsächlich auf der Idee, alle Transaktionsdaten als eine Art von Regeln anzusehen: WENN gewisse symbolische Merkmale gegeben sind DANN liegt Mißbrauch vor. Kombinieren wir mehrere solcher Regeln, so können wir eine generalisierte, kürzere Regel erhalten, die weniger von den speziellen Ausprägungen der Ursprungsregeln abhängig ist. Wie erhalten wir nun einen solchen Generalisierungsmechanismus, bei dem die unwichtigen Merkmale weggelassen werden?

2.1 Generalisierung und Gewichtung der Assoziationsregeln

Im Unterschied zu den Standardmechanismen für eine Warenkorbanalyse [1], [2] besteht unser Ziel nicht darin, aus vielen kleinen einfachen Transaktionen (z.B. Bier gekauft, Windeln gekauft) eine möglichst lange Assoziationsregel (Bier und Windeln werden häufig zusammen gekauft) zu generieren. Statt dessen ist unser Ziel, die vielen langen Transaktionen auf möglichst wenige, kurze, allgemeine zu reduzieren. Obwohl Generalisierung typisch für symbolische KI ist, gibt es noch keine Standardalgorithmen für dieses Problem im Data Mining.

Wie können wir eine solche Generalisierung durchführen? Dazu starten wir bei den Basisdaten mit den Transaktionen, die als „Mißbrauch“ gekennzeichnet sind und vergleichen jede Transaktion mit allen anderen, um Paare von ähnlichen Transaktionen zu finden. Jedes solche Paar wird dann in eine generalisierte Regel transformiert, indem alle nicht übereinstimmenden Merkmale mit einem „egal“-Symbol „*“ ersetzt werden. Damit ergibt sich ein Generalisierungsprozeß, der in Abb. 2.1veranschaulicht ist. Links unten in der Zeichnung im gestrichelten Kreis wird die Generalisierung von zwei Transaktionen mit den Merkmalstupeln $\mathbf{x}_1$ = (F,D,C,D,A) und $\mathbf{x}_2$ = (F,D,G,D,A) zur Regel (F,D,*,D,A) und weiter zu (F,*,*,D,A) und zu (*,*,*,D,*) dargestellt.

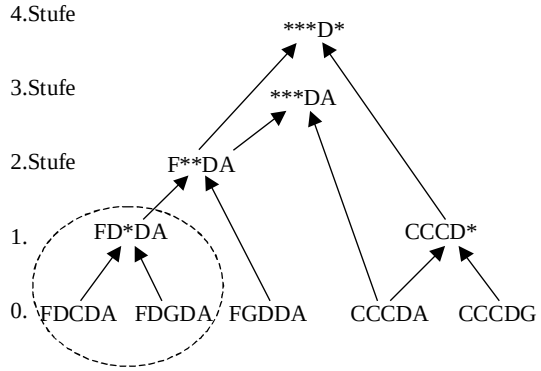

Abb. 2.1 *Der Generalisierungsgraph*

Jede Generalisierung erzeugt mindestens ein „egal"-Symbol für ein unwichtiges Merkmal, erhöht so die Stufe um mindestens eins und verkürzt entsprechend die Regel um mindestens ein Merkmal.

Alle generalisierten Regeln, die nicht selbst generalisiert wurden, bilden die Wurzel eines Untergraphen, speziell eines Baumes.

Beispiel

Bei den 5850 Mißbrauchstransaktionen gibt es vier generalisierte Regeln auf Stufe 16, gezeigt in Tabelle 1.

Rule	ACCT_NBR	TRN_TYP	CURR_CD	POS_ENT_CD	FAL_SCOR	CRD_TYP	ICA_CD	AID_CD	SIC_CD	ACT_CD	MSG_TYP	MER_ID	MER_CNTY_CD	CTY_1	POST_CD_1	CNTY_CD1	CR_LMT	ATV_IND	ACCT_STAT	CTY_2	POST_CD_2	ADDR_STAT	EMIT_NBR	INST_NBR	ISS_REAS	GEN_CD	CARD_TYP
1	*	EA	840	*	*	EM	2768	8403184	*	0	1100	*	0	*	*	*	*	*	I	*	*	*	0	*	*	N	*	*
2	*	EA	840	[1]	0	EM	*	*	563	0	1100	*	0	*	*	*	*	*	I	*	*	*	0	*	*	*	*	*
3	*	EA	840	*	0	EM	2768	8403184	*	*	1100	*	0	*	*	*	*	*	I	*	*	*	0	*	*	*	002	*
4	*	EA	840	*	995	EM	*	*	*	0	1100	*	0	*	0	*	*	I	F8	*	*	0	*	*	*	*	*	*

[1] ZZUTSZ1UZZZ1

Tabelle 1 *Generalisierte Transaktionen auf Stufe 16*

Die Merkmale sind am oberen Rand der Tabelle aufgetragen. Jede Regel unterscheidet sich von jeder anderen.

Im allgemeinen gibt es viele Regeln pro Stufe. Um die wichtigen darin zu charakterisieren, definieren wir uns als „**Abdeckung**" einer Mißbrauchsregel denjenigen Prozentsatz der Mißbrauchstransaktionen, der von dieser Regel erfaßt wird.

Dabei müssen wir allerdings auch beachten, daß es legale Transaktionen gibt, die von der Regel erfaßt werden und dabei einen Fehlalarm auslösen. Je mehr Transaktionen mit einer korrekten Diagnose wir haben um so größer ist unser Vertrauen in den Diagnoseprozeß. Wir können also das **Vertrauen** in den Diagnoseprozeß für eine Regel definieren als

$$\text{Vertrauen} = \frac{\text{Anzahl der Mißbräuche}}{\text{Gesamtzahl der Transaktionen}} \quad (2.1)$$

der durch diese Regel erfaßten Transaktionen.

Wir können zeigen, daß für die Wahrscheinlichkeit P(.) des Vertrauens gilt

$$\text{Vertrauen} = 1 - P(\text{Fehlalarm}) \leq 1 - P(\text{Fehlalarm} | \text{legale Trans.}).$$

Das Vertrauen wird also maximiert, wenn die Wahrscheinlichkeit eines Fehlalarms minimiert wird.

Für diesen Beitrag gilt also als Hauptziel, das Vertrauen in die Mißbrauchsprognose zu maximieren bei einer akzeptablen Wahrscheinlichkeit, Mißbrauch zu erkennen wenn er vorliegt. Der vollständige Algorithmus dafür ist in [4] beschrieben.

2.2 Ergebnisse

Zur Analyse verwendeten wir eine Menge von 5,850 Mißbrauchstransaktionen und 542,858 legale Transaktionen, nach Zeitmarken sortiert. Da der Generalisierungsalgorithmus eine hohe Laufzeitkomplexität hat, wählten wir eine Untermenge von nur 30.000 legale Transaktionen. Die dafür resultierenden Vertrauenswerte wurden anschließend an der Gesamtdatenmenge überprüft. In der folgenden Abb. 2.2 ist die Leistungsfähigkeit der Regeldiagnose als Funktion der Generalisierungsstufe gezeigt.

Für jede Generalisierungsstufe, also jede Zahl von „*", existiert eine Anzahl von gültigen, nicht-generalisierten Regeln. Sie sind mit „Regelanzahl pro Stufe" bezeichnet. Jedes Regelset pro Stufe bemerkt einen gewissen Teil der Mißbrauchstransaktionen, gemessen als „Abdeckung pro Stufe".

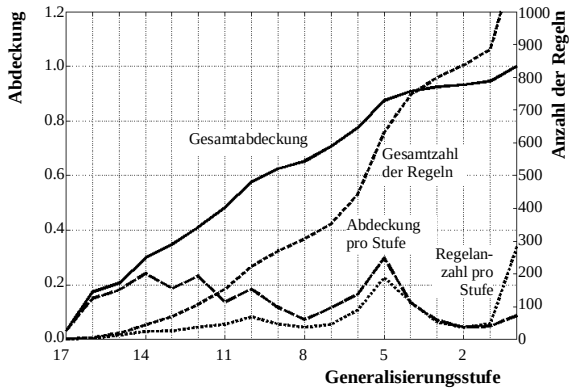

Abb. 2.2 *Die Leistungsfähigkeit der Regeldiagnose*

Wir können sehen, daß ein Großteil der Gesamtabdeckung durch die Regeln von Stufe 5 und höher erzielt werden kann.

Natürlich erhalten wir eine noch größere Abdeckung, wenn wir weitere Regeln aus tieferen Stufen dazu nehmen. Allerdings hängt mit immer weniger generalisierten Regeln die Leistungsfähigkeit immer stärker von den statistischen Fluktuationen der Datenbasis ab. Nehmen wir beispielsweise die 747 Regeln der Generalisierungsstufe 4 bis 17, so erhalten wir ein moderates Vertrauen in die Mißtrauenserkennung aller Transaktionen, siehe Tabelle 2.

#Regeln	**% korrekte Diagnose**			**Vertrauen**
	legale	Miß.	gesamt	%
747	99.73	90.91	99.64	25.14
			(99.72)	(25.2)
510	99.97	83.08	99.79	75.17
			(99.953)	(73.5)
0	*99.9*	*0.0*	*99.9*	*0.0*

Tabelle 2 *Mißbrauchserkennung vs. Vertrauen*

Wenn wir aber nur die Regeln auswählen, die das Vertrauen auf dem gesamten Datenbestand ausreichend bewahren, erhalten wir 510 Regeln. Natürlich mindert sich die Wahrscheinlichkeit, einen Mißbrauch zu entdecken, etwas ab, aber unser Hauptziel, die Akzeptanz einer automatischen Diagnose beim Kunden durch ein hohes Maß an Vertrauen zu bewirken, wird durch die Erhöhung des Vertrauens auf über 75% bewirkt, siehe Tabelle 2. Hauptgrund dafür ist die erhöhte Menge an legalen Transaktionen, die nicht mehr als Mißbrauch gewertet werden und keinen Fehlalarm mehr auslösen. Dieses Verhalten ist auch bei der echten Proportion von legalen vs. Mißbrauchsdaten von 1000:1 zu bemerken wie die Zahlen in Klammern in Tabelle 2 zeigen. Dabei ist die Leistungsfähigkeit der Diagnose besser als die „dumme“ Diagnose, die in der letzten Zeile zum Vergleich notiert ist.

3 Untersuchung der Analogdaten

Jede Transaktion ist durch symbolische und analoge Daten charakterisiert. Bisher haben wir nur die Information der symbolischen Daten genutzt. Besitz der analoge Teil, also die Informationen über Tageszeit, Kreditsumme, Kreditrahmen usw. verwendbare Information? Können wir damit die Mißbrauchsdiagnose verbessern?

Das Problem der Mißbrauchsdiagnose kann man als das Problem ansehen, in Transaktionen in zwei Klassen zu unterteilen: in die guten und die schlechten Transaktionen. Unser Problem ist also ein Klassifikationsproblem. Einer der Hauptansätze für eine dynamische, datengetriebene Klassifikation ist der Ansatz, die Klassifikationsparameter, also die Klassengrenzen, durch einen adaptiven Prozeß zu *lernen*. Dies ist die Domäne der künstlichen neuronalen Netze: Wir benutzten ein besonderes Modell daraus um die Aufgabe zu erfüllen.

3.1 Das Netzwerk

Es gibt mehrere mögliche Ansätze, dieses Ziel zu erreichen. In unserem Ansatz benutzten wir einen Experten pro Merkmalsgruppe (Zeit, Geld, usw.) und fusionierten alle Urteile zu einem Gemeinschaftsurteil zusammen. In Abb. 3.1 ist diese Architektur gezeigt.

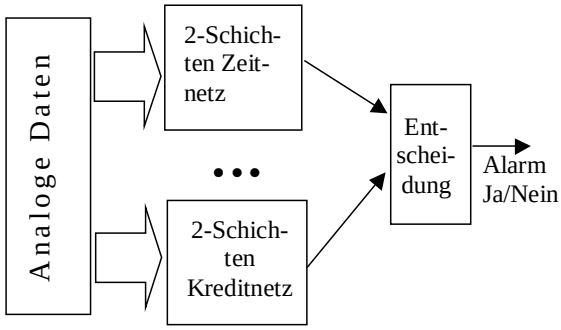

Abb. 3.1 *Das neuronale Netz zur Diagnose der Analogdaten*

Wir benutzen mehrere Netze vom RBF-Typ [8], jedes auf einen anderen Diagnosetyp spezialisiert.

3.2 Ergebnisse

Mit dem sehr geringen Mißbrauchsvorkommen von nur 0,1% haben wir mit der „dummen" Strategie „Transaktion ist immer OK" eine sehr gute Erfolgsrate von 99,9% korrekter Diagnosen. Es ist nicht einfach, mit dieser Trivialdiagnose zu konkurrieren. Benutzen wir nur die Analogdaten, so werden alle Transaktionen, die durch *n* symbolische und *m* analoge Merkmale charakterisiert werden, vom *n*+*m*-dimensionalen Raum in den *m*-dimensionalen Raum projiziert. Im allgemeinen bedeutet dies eine Überlappung der Klassen und damit einen Diagnoseerfolg von weniger als 99,9%. In Abb. 3.2 ist die typische Situation bei der Klassentrennung nur durch eine analoge Variable x verdeutlicht. Hierbei sind die beiden Wahrscheinlichkeitsdichtefunktionen p(x|M) für die Mißbrauchsdaten und p(x|L) für die legalen Daten gezeigt.

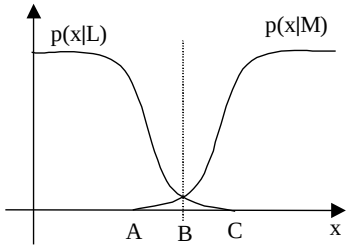

Abb. 3.2 *Diagnose bei überlappenden Klassen*

Für eine beste Trennwahrscheinlichkeit zwischen beiden Klassen ist die Klassengrenze an Punkt B in Abb. 3.2 wo beide Klassendichten gleich sind. Für unsere Ziele einer hohen Mißbrauchserkennung und eines hohen Vertrauens bemerken wir aber einen Interessenkonflikt: Wählen wir die Grenze bei Punkt A, so erhalten wir eine hohe Wahrscheinlichkeit der Mißbrauchserkennung und ein geringes Vertrauen (große Fehlalarmrate). Legen wir dagegen die Klassengrenze in Punkt C, so resultiert ein hohes Maß an Vertrauen in eine Entscheidung auf Mißtrauen (es gibt nur noch richtige Entscheidungen), aber die Wahrscheinlichkeit, überhaupt Mißbrauch festzustellen ist geringer.

Betrachten wir nun die Diagnose der Transaktionen mittels neuronaler Netze. Für diesen Zweck benutzten wir das neuronale Expertensystem, das in Abb. 3.1 gezeigt ist, und trainierten es mit unseren Mißbrauchsdaten. Wir führten 300 Trainingszyklen durch und analysierten danach den Zustand des Netzwerks, indem wir 250 legale und 250 Mißbrauchstransaktionen präsentierten. Die Proportion der legalen zu den Mißbrauchsdaten wurde dabei verändert und bewirkte ein unterschiedliches Diagnoseverhalten. Die Ergebnisse sind in Tabelle 3 gezeigt.

Proportion	**korrekte Diagnose %**			**Fehldiagnose %**		**Vertrauen %**
	total	legale	Mißb.	legale	Mißb.	
2:1	78.8	95.2	62.4	4.8	37.6	1.3
4:1	58.2	99.6	16.8	0.4	83.2	4.0
10:1	50.0	100	0	0	100	100

Tabelle 3 *Verschieben der Klassengrenze*

Wie wir sehen können wird die Klassengrenze durch die Erhöhung der Zahl der legalen Transaktionen beim Training zu Punkt C von Abb. 3.2 verschoben. Hier ist das Vertrauen groß, aber die Mißbrauchsentdeckung wird null.

4 Die Kombination analoger und symbolischer Information

Im vorigen Abschnitt wurden wir mit der Tatsache konfrontiert, daß die Analogdaten nicht

als ausreichendes Kriterium für eine Mißbrauchsanalyse dienen kann. Deshalb kombinierten wir die Diagnoseinformation des symbolischen, regelbasierten Assoziationssystems aus Abschnitt 2.1 mit der Experteninformation des neuronalen Netzes aus Abschnitt 3.1 in einem parallelen Netzwerk, das eine gemeinsame Entscheidungsstufe (Ausgabe) besitzt, siehe Abb. 4.1.

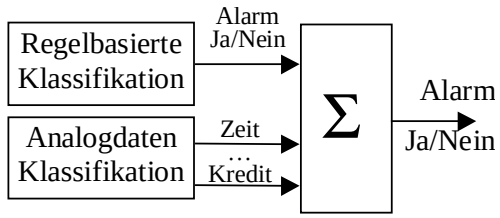

Abb. 4.1 *Paralleles Diagnosesystem*

Der Diagnoseeinfluß aller Expertensysteme ist initial der gleiche und konvergiert bei einem 1:1 Training im Grenzwert zu ihrem entsprechendem Wert. In allen Situationen kann der Einfluß des Analogsystems der des regelbasierten Systems „überstimmen“. Dies zeigt sich beim „kombinierten Parallelansatz“ in Tabelle 4.

Diagnost. Methode	**Wahrsch. korrekter Diagn.**		**Vertrauen %**	
Datenmengengröße	1000	11.700	1000	11.700
Regelbasiert	0,901	0,915	100,0	100,0
Analogdaten	0,853	0,817	1,55	93,1
komb. Par.	0,928	0,898	100,0	1,05
Komb. Seq.	0,845	0,876 (**0,999552**)	100,0	81,49 (**79,0**)

Tabelle 4 *Vergleich der Leistung zweier Diagnosesysteme bei zwei Datenmengengrößen*

Der parallel Ansatz bedeutet einen Diagnosefehler, der sich besonders bei den legalen Transaktionen auswirkt. Dies drückt das Vertrauen stark herab bis auf 1 %. Können wir dies ändern?

Dazu konstruierten wir ein zweites System in sequentieller Anordnung. Die Entscheidung auf Mißbrauch wird hier vom erfolgreichen regelbasierten Diagnosesystem zusätzlich durch das analoge neuronale Netz überprüft, siehe Abb. 4.2.

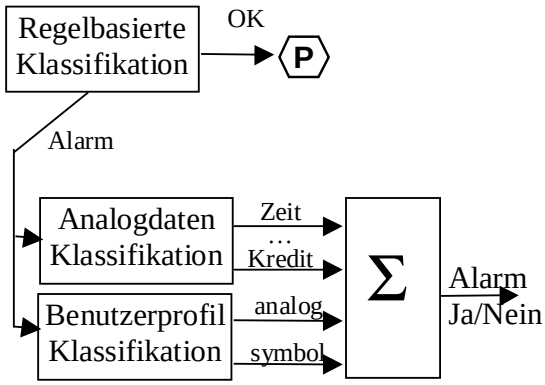

Abb. 4.2 *Sequentielles Diagnosesystem*

Natürlich drückt das nicht die Fehlentscheidung der ersten Stufe, Mißbrauch als „legal“ einzuordnen, aber es erhöht die Wahrscheinlichkeit, daß eine Mißbrauchsdiagnose der ersten Stufe auch korrekt ist und erniedrigt damit die Zahl der Fehlalarme, siehe Tabelle 4.

Nehmen wir nun noch die zeitliche Folge der Transaktionen eines Benutzers dazu („Benutzerprofile“, s. [4]), so erhalten wir zusätzliche Information. Für sich allein genommen reicht auch diese Information nicht aus, eine gute Diagnose zu erstellen, aber in Kombination mit den Regeln und den Analogdaten erhöhen sich die Wahrscheinlichkeiten für Mißbrauchserkennung und Vertrauen darin, siehe Tabelle 5.

Diagnosemethode	**Wahrsch. korrekter Mißbrauchsdiagn.**		**Vertrauen %**	
Datenmenge	1000	11,700	1000	11,700
510 R+A	0.69	0.75	100.0	81.5
747 R+A	0.80	0.82	28.6	49.0
837 R+A	0.82	0.84	29.0	62.1
510 R+A+P	0.85	–	100.0	–
747 R+A+P	0.87	–	100.0	–
837 R+A+P	**0.95**	–	**100.0**	–

Tabelle 5 *Leistung des sequentiellen. Systems bei unterschiedlicher Regelzahl*

Für das sequentielle System läßt sich eine weitere Leistungssteigerung dadurch erreicht werden, indem man die Vertrauensgrenze für die Regelgenerierung herabsetzt. Dadurch erhalten wir mehr Regeln (747 bzw. 837 statt 510), die

zwar mehr Mißbrauch erkennen, aber auch mehr Fehlalarm auslösen. In der sequentiellen Konfiguration werden die Mißbrauchsalarme aber nochmals durch das kombinierte Analog/Profilsystem geprüft, so daß im Endeffekt eine hohe Mißbrauchserkennung von 95% bei 100% Vertrauen resultiert, siehe Tabelle 5.

5 Diskussion

In diesem Beitrag entwickelten wir Konzepte für eine statistik-basierte Kreditkartenmißbrauchsdiagnose. Wir zeigten, wie dies für die sehr spezielle Situation eines sehr geringen Mißbrauchs von 1:1000 aufgebaut werden konnte.
Dabei zeigten wir, wie man durch algorithmische Generalisierung der Transaktionsdaten höhere Stufen von Diagnoseregeln erhalten kann. Kombinieren wir diese regelbasierte Information mit adaptiven Klassifikationsmethoden, so erhalten wir die sehr guten Ergebnisse einer Mißbrauchserkennung von 95% bei 100% Vertrauen in die Entscheidung. Dies bedeutet eine Ersparnis von ca. 17 Mill. DM pro Jahr.

Basierend auf diesen Ergebnissen ist nun für eine praktische Nutzung der Diagnosealgorithmen weitere Arbeit nötig, um sie im laufenden Betrieb einzusetzen. Dazu müssen sie für eine transaktionsbegleitende Überwachung eines *data warehouse* umstrukturiert werden zu *online*-Algorithmen, die die laufenden Änderungen des Mißbrauchsverhaltens automatisch in einer veränderten Regelbasis und veränderten Diagnosegewichten reflektieren.

Referenzen

[1] R. Agrawal, H.Mannila, R. Srikant, H. Toivonen, A.I. Verkamo: *Fast Discovery of Association Rules*. In: U. Fayyad, G. Piatesky-Shapiro, P. Smyth, R. Uthurusamy (eds.): Advances in Knowledge Discovery and Data Mining. Menlo Park, AAAI/MIT Press 1996

[2] R. Agrawal, R. Srikant: *Fast Algorithms for mining association rules*. Proceedings of the VLDB Conference, Santiago, Chile, 1994

[3] P. Barson, S. Field, N. Davey, G. McAskie, R. Frank*: The Detection of Fraud in Mobile Phone Networks;* Neural Network World 6, 4, pp. 477-484 (1996)

[4] R. Brause, T. Langsdorf, M. Hepp: *Credit Card Fraud Detection by Adaptive Neural Data Mining*, J.W.Goethe-Universität, Fachbereich Informatik, Interner Bericht 7/99, Frankfurt, Germany (1999), und in http://www.cs.uni.frankfurt.de/fbreports/ fbreport07-99.pdf

[5] S. Ghosh, D.L. Reilly: *Credit Card Fraud Detection with a Neural-Network*; Proc. 27th Annual Hawaii Int. Conf. on System Science, IEEE Comp. Soc. Press, Vol.3, pp.621-630 (1994)

[6] R.J. Hildermann, C.L. Carter, H.J. Hamilton, N. Cercone: *Mining Association Rules from Market Basket Data using Share Measures and Characterized Itemsets;* Int. J. of AI tools vol.7, No.2, pp.189-220, 1998

[7] Y. Moreau, H. Verrelst, J. Vandwalle: *Detection of Mobile Phone Fraud using Supervised Neural Networks: A First Prototype;* Proc. ICANN ´97, Lecture notes on computer science LNCS 1327, Springer Verlag 1997

[8] R. Brause: *Neuronale Netze*, Teubner Verlag, 2.Auflage, Stuttgart 1995

[9] R. Srikant, R. Agrawal : *Mining generalized association rules*. Proc. VLDB Conference, Zurich, Switzerland, 1995

Korrespondenzadresse

PD Dr. R. Brause,
J.W.G.-Universität
Fachbereich Informatik
60054 Frankfurt

Tel. 069-798-23977
Email: Brause@Informatik.Uni-Frankfurt.de