PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1121 — 2006
Pozyskiwanie wiedzy i zarządzanie wiedzą

Maciej Wasiak

Akademia Ekonomiczna we Wrocławiu

WYKORZYSTANIE MOBILNYCH AGENTÓW PROGRAMOWYCH W ELEKTRONICZNYM REJESTRZE USŁUG MEDYCZNYCH

1. Wstęp

Informatyzacja polskiej służby zdrowia jest od wielu lat przedmiotem ogólnokrajowej dyskusji. Niestety, mimo perspektywy ogromnych oszczędności związanych z jej wprowadzeniem, podejmowane działania mają charakter fragmentaryczny; brak jest nawet oficjalnych założeń. Problem ewidencjonowania danych medycznych w Polsce oraz późniejszej ich analizy i weryfikacji wiąże się ściśle z projektem utworzenia Rejestru Usług Medycznych. Mimo braku determinacji kolejnych rządów do realizacji rejestru, można się spodziewać, że akcesja do Unii Europejskiej, wymusi wkrótce wprowadzenie ogólnopolskiego systemu informatycznego dla służby zdrowia. Jednym z głównych skutków wprowadzenia elektronicznego Rejestru Usług Medycznych (e-RUM) będzie zlikwidowanie wielu oszustw i nadużyć, które obecnie są bardzo łatwe do popełnienia, a trudne do wykrycia (patrz raport NIK z 2005: [*Raport*... 2005]). Jak pokazują doświadczenia innych państw oraz ogólnie wdrożenia systemów informatycznych, zlikwidowanie jednych rodzajów oszustw powoduje zazwyczaj powstawanie innych. Niniejszy artykuł porusza problem nadużyć, które mogą powstać po wprowadzeniu e-RUM-u, oraz sposobów zapobiegania im za pomocą zaawansowanych narzędzi informatycznych, m.in. z wykorzystaniem agentów programowych.

Przykładów zastosowania agentów programowych w detekcji oszustw i nadużyć nie ma zbyt wiele. Niektóre koncepcje i wdrożenia można odnaleźć w pracach: [Prodromidis, Stoflo 1999] (karty kredytowe), [Wang, Mylopoulos, Liao 2002] (inwestycje finansowe), czy [Wu, Park 2001] (nadużycia telekomunikacyjne). W wielu przypadkach sięganie po technologię autonomicznych i mobilnych programów nie znajduje uzasadnienia, szczególnie, gdy analizowane dane znajdują się w jednym miej-

scu. Najbardziej jednak prawdopodobna koncepcja e-RUM-u zakłada zastosowanie modelu rozproszonego na wiele województw, co może spowodować znaczne utrudnienia w efektywnym wykorzystaniu tradycyjnych metod *Data Mining*.

2. Historia informatyzacji Rejestru Usług Medycznych i stan obecny

Na początku lat 90. rozpoczęto prace nad Rejestrem Usług Medycznych (RUM), który miał stanowić zamknięty obieg dokumentów, umożliwiać kontraktowanie usług oraz stanowić podstawę do rozliczeń finansowych. W 1996 r. wdrożono w Gdańsku pierwsze rozwiązanie wykorzystujące rozległą sieć komputerową [Strug 2002] łączącą biura terenowe zlokalizowane w ZOZ-ach. Zbierane dane umożliwiały uporządkowanie wielu informacji oraz częściową ich kontrolę. W listopadzie 1999 r. resort zdrowia podpisał umowę z firmą ComputerLand oraz konsorcjum firm Kamsoft i Spin na informatyzację 16 kas chorych. Kamsoft i Spin rozpoczęły również informatyzację Branżowej Kasy Chorych.

W roku 2001 Śląska Regionalna Kasa Chorych wdrożyła system START (autorstwa ComputerLandu). Jest to, jak dotąd, system o modelu funkcjonowania w największym stopniu zbliżonym do projektu elektronicznego RUM. Wszyscy pacjenci w regionie mają karty elektroniczne, którymi autoryzują wykonywanie świadczeń medycznych. Wdrożenie systemu w krótkim czasie przyniosło oszczędności wielokrotnie przekraczające kwotę wydaną na jego utworzenie.

W latach 2002 i 2003 zrealizowano różne fragmentaryczne projekty, jak m.in. komputeryzacja 300 największych szpitali. W 2003 r. wpisano na listę B projektów offsetowych plan wprowadzenia elektronicznego RUM. System miało wykonać i wdrożyć konsorcjum firm ComputerLand, Prokom oraz Lockheed Martin. Projekt ten został skreślony z listy offsetowej na początku roku 2005. Minister zdrowia – Marek Balicki, argumentował tę decyzję tym, że o ile sama idea RUM-u jest słuszna, o tyle strona formalna, zaangażowane podmioty oraz cena skłaniają do poszukania innej drogi realizacji systemu.

Mimo kilku podejść do informatyzacji służby zdrowia, stan aktualny jest wysoce niezadowalający. Sprawozdawczość oraz kontrola przez NFZ operacji dokonywanych przez świadczeniodawców w zasadzie nie istnieje. Na przykład, na Dolnym Śląsku w 2004 r. skontrolowano 4,8% placówek. Nieprawidłowości stwierdzono w 79% z nich (!) – zob. [Przybyłka 2002].

Zakłady opieki zdrowotnej oraz inne podmioty świadczące usługi medyczne nie przestrzegają wielu zasad dotyczących prowadzenia dokumentacji. W roku 2004 NFZ praktycznie nie dokonywał kontroli aptek w zakresie realizacji recept refundowanych [Przybyłka 2002].

Fundusz nie stosuje jednolitych zasad gromadzenia, przekazywania między pionami oraz analizowania informacji o faktycznie wykonanych świadczeniach.

Ma to bezpośredni, niestety – negatywny wpływ na planowanie i kontraktowanie świadczeń, ich dostępność, proces sporządzania planu finansowego oraz zarządzanie wolnymi środkami. W efekcie centrala funduszu nie dysponuje wiarygodnymi informacjami o wykonanych świadczeniach zdrowotnych finansowanych ze środków publicznych.

Ostatecznie, NIK w raporcie z lipca 2005 NIK sformułował dwa wnioski pokontrolne skierowane do prezesa Narodowego Funduszu Zdrowia. Jednym z nich jest zalecenie stworzenia „systemu pozwalającego na wiarygodną weryfikację danych przekazywanych przez świadczeniobiorców, dotyczących liczby wykonanych świadczeń zdrowotnych, w tym ponadlimitowych".

3. Projekt e-RUM

Obecnie nie istnieje oficjalnie zatwierdzona koncepcja e-RUM-u. Przypomnijmy strukturę danych, które miał zbierać RUM w swojej oryginalnej wersji, wstępnie zaprojektowanej przez A. Horocha oraz M. Jarosza. Otóż jest to rekord danych zawierający (za [Strug 2002]:

- identyfikację pacjenta,
- identyfikację instytucji i lekarza zlecającego usługę,
- identyfikację instytucji i lekarza wykonującego usługę,
- kod usługi medycznej,
- przyczynę medyczną udzielenia usługi,
- datę zlecenia usługi,
- datę wykonania usługi,
- dane dotyczące finansowania usługi.

Nawet tak prosta struktura danych umożliwiłaby drastyczne ograniczenie nadużyć w służbie zdrowia.

W aktualnych rozważaniach na temat RUM-u, najczęściej pojawiająca się koncepcja zakłada wykorzystanie komputerów (lub terminali) u każdego świadczeniodawcy oraz bezpieczną identyfikację zarówno świadczeniodawcy, jak i pacjenta – mowa tu o kartach chipowych lub procesorowych.

Rozważane są dwie możliwości: stworzenia systemu scentralizowanego, gromadzącego w jednym miejscu wszystkie dane medyczne, lub systemu zdecentralizowanego na kilkanaście serwerów, które do centralnego systemu przesyłałyby jedynie wyselekcjonowane dane. System scentralizowany jest określany jako funkcjonujący na granicy aktualnych możliwości technologicznych, ale oferuje korzyści związane m.in. ze spójnością, bezpieczeństwem oraz możliwością analiz. System zdecentralizowany jest oceniany jako znacznie tańszy w budowie, niesie jednak ze sobą pewne niedogodności – przeciwieństwa zalet systemu scentralizowanego (za [Krupa 2003]). Obserwując toczącą się w mediach dyskusję na ten temat, można stwierdzić przewagę głosów za systemem zdecentralizowanym.

Ostrożne szacunki wskazują, że możliwe oszczędności w skali roku związane z wdrożeniem systemu mogą stanowić równowartość kosztu wdrożenia. Bardziej optymistyczne, choć autor niniejszego opracowania tego optymizmu nie podziela, wskazują, że kwota ta może wynosić 3, a nawet 6 mld zł (por. [Piński, Trębski 2005]).

Niezależnie od przyjętej struktury danych oraz architektury systemu, znane są cele jego wdrożenia. Można więc określić jego podstawową funkcjonalność oraz metody umożliwiające analizę danych medycznych m.in. w celu wykrywania nadużyć. Po wdrożeniu systemu część oszustw po prostu zniknie. Placówka nie będzie mogła sfałszować dokumentacji, dopisując fikcyjne wizyty bez wiedzy pacjenta, gdyż proces ten będzie odbywał się elektronicznie. Niestety, sama informatyzacja nie wystarczy do całkowitej likwidacji wyłudzeń. Doświadczenia z innych dziedzin gospodarki, a także systemów zdrowotnych funkcjonujących za granicą, wskazują na dużą pomysłowość, żeby nie powiedzieć desperację, w poszukiwaniu możliwości ominięcia barier systemu.

4. Zapobieganie nadużyciom w systemach ochrony zdrowia

Podstawową metodą zapobiegania nadużyciom w systemach ochrony zdrowia jest wykorzystywanie reguł tworzonych na podstawie wiedzy ekspertów. Na przykład: „Jest wysoce podejrzane, gdy pacjent jest trakcie leczenia szpitalnego i odbywa równocześnie badanie w przychodni". System, korzystając z tak utworzonej bazy wiedzy, monitorowałby zarejestrowane operacje i sygnalizował kontrolerom/analitykom zaistnienie takich sytuacji.

Kolejną grupą metod analitycznych są techniki OLAP (*online analytical processing*). Umożliwiają one wszechstronną i wielowymiarową analizę danych, tworzenie zapytań *ad hoc* w celu uzyskania syntetycznych zestawień, tworzenie tabel przestawnych oraz wizualizację wyników. OLAP są grupą narzędzi znakomicie usprawniających odszukiwanie nadużyć, ale mają swoje liczne ograniczenia. Przede wszystkim nie jest to proces automatyczny – analizy dokonywane są przez specjalistę i skuteczność wykrywania zależy w dużym stopniu od jego doświadczenia oraz umiejętności. Niemniej jednak analizy OLAP są niezbędne również jako etap badań przygotowujący do dalszych badań.

Do najbardziej zaawansowanych metod zapobiegania nadużyciom należą analizy *Data Mining* z wykorzystaniem sztucznej inteligencji. Przykładem ich wykorzystania do tego celu może być system opisany przez J. Wanga i in. w pracy [Wang, Graco, Hawkins 1997]. Jest to typowe użycie sieci uczonej wsteczną propagacją błędu do klasyfikacji danych finansowych z systemu zdrowotnego. Największą zaletą sieci neuronowych jest trafność wnioskowania. Przy odpowiednio przygotowanych danych jest to jedna z najskuteczniejszych technik AI. Niestety, wiąże się z nią kilka niedogodności, m.in. wymaga danych numerycznych, nie ma dobrych algorytmów selekcji zmiennych oraz jest mało czytelna. Oznacza to, że

zweryfikowanie sensowności wnioskowania sieci neuronowej przez człowieka jest w zasadzie niemożliwe. Algorytmy ekstrakcji czytelnych reguł z sieci neuronowych znajdują się dopiero w fazie opracowywania i nie wiadomo, czy w ogóle z niej wyjdą.

Wysoce skuteczną metodę wykrywania oszustw medycznych zaproponowano w 1998 r. (zob. Hongxing i in. 1998]). Jest to system hybrydowy oparty na algorytmie genetycznym oraz CBR (*cased based reasoning*), czyli porównywaniu nowych danych z dotychczas znanymi przypadkami nadużyć. Metody oparte na tej technice należą do najskuteczniejszych nie bez powodu – odbywa się to kosztem ogromnej liczby obliczeń **w trakcie** wnioskowania. Jest prawdopodobne, że system taki przy dużej ilości pojawiających się cały czas nowych danych nie byłby w stanie skutecznie funkcjonować w warunkach ogólnopolskich.

J. Major i D. Riedinger (zob. [Major, Riedinger 2002]) zaprojektowali w 2002 r. kilkuwarstwowy system ekspercki oparty na regułach, w którym wiedza specjalistów jest zintegrowana z modelami statystycznymi. Pierwszy filtr stanowi 27 statystyk behawioralnych, filtrujących podejrzane operacje. Następnie aplikowane są reguły logiczne, a na końcu przeprowadzane jest wnioskowanie z użyciem metod sztucznej inteligencji.

Ciekawe wnioski sformułowano również w pracy J. Pathaka (zob. [Pathak i in. 2003]),gdzie zaprezentowano badania nad wykorzystaniem logiki rozmytej do wykrywania nadużyć medycznych. Systemy rozmyte (*fuzzy logic systems*) wydają się być szczególnie korzystną reprezentacją wiedzy dla potrzeb identyfikacji oszustw. Zachowują regułowy proces wnioskowania (Jeżeli..., to...), a jednocześnie płynnie odwzorowują rzeczywiste zależności i są w stanie podać stopień pewności swojej decyzji (tutaj: prawdopodobieństwo oszustwa). Systemy rozmyte poddają się automatycznemu uczeniu za pomocą wielu metod, m.in. gradientowych, clusteringowych, z wykorzystaniem algorytmów genetycznych, wykazując wysoką trafność klasyfikacji. Ich dużą zaletą jest (przy zachowaniu odpowiedniego reżimu w trakcie automatycznego uczenia) zrozumiały proces wnioskowania i możliwość wytłumaczenia swojej decyzji.

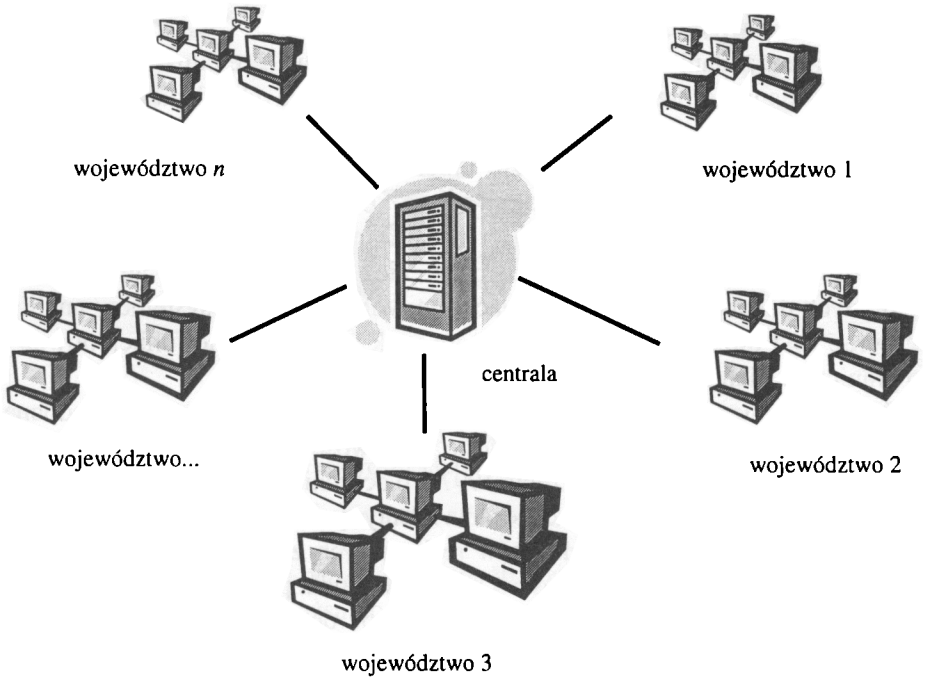
Modele zachowań przestępczych podlegają nieustannym modyfikacjom. Rodzi to konieczność projektowania systemów z założenia adaptacyjnych, wykorzystujących dynamiczne modele wiedzy, uwzględniające temporalne i behawioralne aspekty oszustw i nadużyć.

5. Zastosowanie agentów w rozproszonym systemie e-RUM

Przeglądając możliwości krajowych systemów detekcji nadużyć w zakresie usług dostarczanych masowym klientom, np. telekomunikacji, energetyki, czy telewizji kablowych, można zauważyć, że wykorzystują one dość podstawowe technologie analityczne – korelacje danych czy względnie proste analizy odchyleń. Zwłaszcza prace w zakresie detekcji nadużyć w systemie służby zdrowia są wyjąt-

kowo ograniczone, przede wszystkim przez brak systemu, na którym można by testować koncepcje i technologie. Badania nad wykorzystaniem sztucznej inteligencji w tym sektorze zaczynają dopiero być prowadzone.

Analizy korelacyjne, wykorzystanie dorobku OLAP i *Data Mining* są naturalną drogą do wykrywania nadużyć w elektronicznym RUM-ie. Jednakże architektura rozproszona przyszłego systemu – o ile taka zostanie wybrana, może wiele z dostępnych technologii analiz znacznie ograniczyć. Poniżej opisano niektóre możliwości zastosowania **technologii agentowej**, przy założeniu, że wdrożony zostanie model rozproszony, tzn. teren kraju zostanie podzielony na regiony (najprawdopodobniej województwa), które będą miały własne centra gromadzenia danych medycznych. Do centrali będą przesyłane zbiorcze dane finansowe i medyczne placówek służby zdrowia oraz raporty bez szczegółowych danych pacjentów. Typowy szkic tej architektury przedstawiono na rys. 1.



Rys. 1. Ogólny model rozproszonej struktury e-RUM-u

Źródło: opracowanie własne.

Dla celów niniejszego artykułu przyjęto, że „agent" to program komputerowy wyposażony w umiejętność samodzielnego przeglądania danych oraz wnioskowania. Wnioskowanie dotyczy zarówno wykrywania podejrzanych operacji, jak i

kierunków dalszych poszukiwań. Program ten może przenosić się między serwerami sieci e-RUM, zabierając potrzebne dane ze sobą, o ile dane te nie naruszają ograniczeń związanych z bezpieczeństwem. Agent nie musi mieć możliwości samodzielnego uczenia się, gdyż proces ten może odbywać się w wyspecjalizowanym laboratorium pod kontrolą specjalistów. Programy agentowe mogą komunikować się ze sobą oraz z systemem centralnym.

Wykorzystując do wyszukiwania nadużyć model klasyfikujący, często należy sięgać do danych z innych województw. Przykładem może być kontrola recept zrealizowanych w jednym województwie, a wypisanych w innym. Podobnie dzieje się ze skierowaniami z placówek położonych w innych województwach, czy chorymi, którzy wręcz podróżują po terenie całego kraju. W takich wypadkach kontrola na poziomie lokalnym nie jest wystarczająca.

Dwa najistotniejsze ograniczenia dla tradycyjnych metod analitycznych, jakie mogą się pojawić w przypadku utworzenia rozproszonego e-RUM-u, stanowią dwa aspekty, a mianowicie:

– charakter zadania analitycznego będzie powodował, że odnajdywanie związków między danymi, przeszukując zdalnie serwery w innych oddziałach, może być nieefektywne,

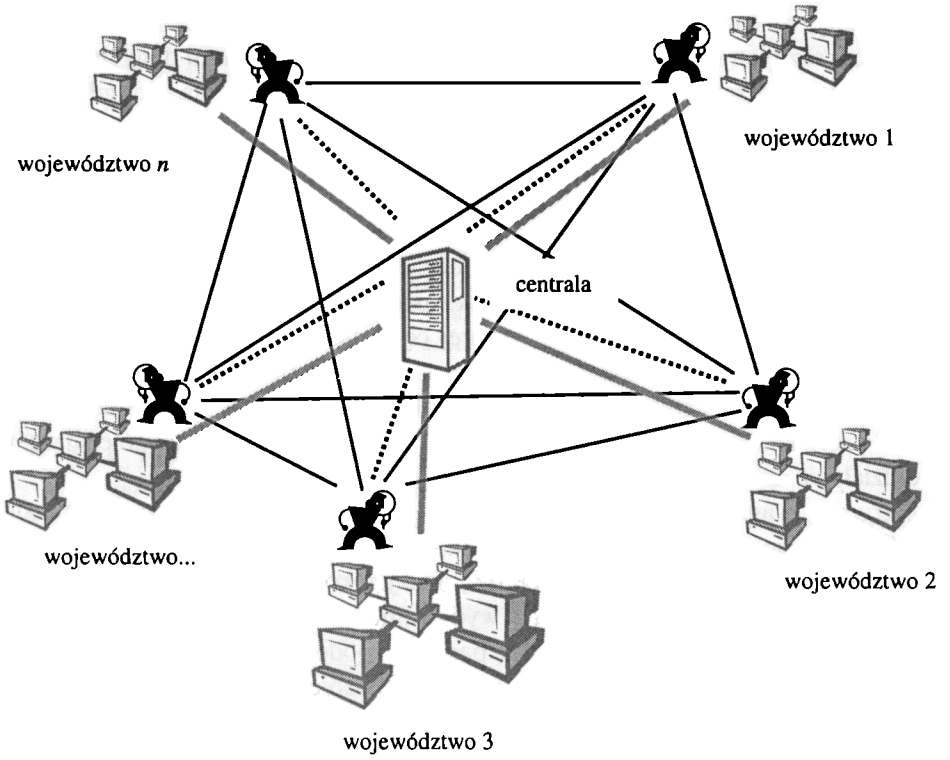
– projekt systemu e-RUM będzie uniemożliwiał przesyłanie szczegółowych danych medycznych między serwerami.

Pierwsze ograniczenie ma charakter wyłącznie ekonomiczny. Nawet w obliczu możliwości zdalnego dostępu do danych z całego kraju, w wielu analizach ilość potrzebnych danych może spowodować zbyt wolne działanie systemów analitycznych oraz zbyt duże obciążenia sieci, które i tak będą zapewne funkcjonować blisko granicy swoich możliwości.

Drugie ograniczenie ma charakter fundamentalny i jest bardzo prawdopodobne ze względu na niebezpieczeństwa, jakie niesie możliwość zdalnego dostępu do danych medycznych. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i dentysty, Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, rozporządzenia wydane na podstawie tych ustaw oraz inne źródła prawa poważnie ograniczają dostęp do danych medycznych. Możliwość dostępu do danych spoza lokalnego oddziału e-RUM-u może zostać celowo zablokowana albo udostępniona dla wąskiej grupy osób i zabezpieczona w bardzo wyrafinowany sposób. Trudno sobie wyobrazić, żeby umożliwiono taki dostęp programom komputerowym, które same dokonywałyby wyboru, czyje dane z innych oddziałów chcą zweryfikować i jak dokładnie.

W rozważanej architekturze, z uwzględnieniem przedstawionych ograniczeń systemu, możliwe jest zastosowanie podejścia odmiennego od metod tradycyjnych, a mianowicie wykorzystanie mobilnych i współdziałających ze sobą agentów – zob. rys. 2. Serwery należące do e-RUM-u byłyby przygotowane do przyjmowania i obsługi agentów, które wykonywałyby potrzebne analizy na danych dostępnych

lokalnie, mogąc w każdej chwili przenieść się do serwera położonego w innym województwie w celu skonfrontowania danych czy prześledzenia nowych śladów.



Rys. 2. Ilustracja funkcjonowania mobilnych agentów programowych w rozproszonej strukturze e-RUM-u

Źródło: opracowanie własne.

Prześledźmy na dwóch przykładach możliwości działania agenta.

Przykład 1. Kradzież tożsamości

Jednym ze sposobów dokonania nadużycia w systemie e-RUM jest wykorzystanie czyjejś tożsamości do rejestrowania fikcyjnych badań i zabiegów. Jest to możliwe np. poprzez podrobienie karty identyfikacyjnej pacjenta lub udostępnienie jej przez osobę będącą w zmowie z lekarzami. Agent programowy mógłby zidentyfikować potencjalne nadużycia, np. zauważając dużą częstotliwość zabiegów wykonywanych na danej osobie oraz obserwując profil wykonywanych badań i zabiegów.

W pewnych granicach duża liczba badań nie musi powodować alarmu, ale warto sprawdzić, czy ta sama osoba nie jest badana w innych województwach oraz jaki jest profil wykonywanych tam badań i zabiegów. Agent programowy może swo-

bodnie przenieść się do odległych serwerów, zabierając ze sobą zgromadzone do tej pory statystyki i niektóre dane o analizowanym pacjencie. Znajdując się na nowym serwerze, może szybko, efektywnie i bezpiecznie przeszukać bazę danych, uaktualniając posiadane informacje. Po szczegółowym przeanalizowaniu historii pacjenta na różnych serwerach możliwa jest decyzja o przekazaniu danych pacjenta do sprawdzenia przez analityka lub też o zignorowaniu zagrożenia (np. gdy dane z innych województw nie dają powodów do niepokoju).

Przykład 2. Wyłudzenia refundacji leków

Innym typowym nadużyciem jest wypisywanie fikcyjnych recept na niektóre lekarstwa. Proceder ten ma to do siebie, że pojawia się nagle i dotyczy jednego lub kilku specyfików. W sobie tylko znany sposób nieuczciwe zakłady na terenie całego kraju dowiadują się o pojawiającej się okazji i przez podstawione osoby wykupują medykamenty, by później sprzedawać je po wyższej cenie podmiotom nieuprawnionym do refundacji. Ponieważ dysponują ogólnokrajową statystyką dotyczącą lekarstw, wzrost sprzedaży danego lekarstwa spowodowany wyłudzeniami może być niezauważalny. W tym przypadku można wykorzystać zaletę technologii agentowej polegającą na współdziałaniu agentów umiejscowionych na różnych serwerach e-RUM.

Pierwszy z agentów, który zauważy zwiększone wydawanie recept na jeden specyfik lub więcej specyfików przez niektóre zakłady w swoim województwie, może poinformować pozostałych agentów, podając kod lekarstwa. W krótkim czasie agenci mogą skontrolować historię wydawania recept na dane lekarstwo. Wiedząc, czego szukają, mogą być znacznie bardziej „podejrzliwi". Nawet stosunkowo niewielki wzrost liczby wypisywanych recept w pojedynczych zakładach może rodzić konieczność dalszej obserwacji i dokładnej analizy historii zakładów. Nagły wzrost liczby recept wydawanych na niektóre lekarstwa może być skorelowany z danymi z innych województw, ponownie, dzięki przesłaniu informacji do pozostałych agentów. Zebrane dane dotyczące podejrzanych operacji mogą być skierowane do centralnego systemu analiz, który będzie dalej automatycznie zarządzać analizami lub uruchomi alarm, przesyłając raport do analityka.

6. Podsumowanie

Jednym z głównych celów informatyzacji służby zdrowia jest zapobieżenie ogromnej skali oszustw i nadużyć, jakie są dokonywane przez nieuczciwe zakłady zarówno publiczne, jak i prywatne. Już sama elektronizacja procesów w znacznym stopniu ograniczy możliwość wyłudzeń, ale – jak pokazuje praktyka z innych dziedzin – nie powstrzyma ich całkowicie. W koncepcji rozproszonego sytemu Rejestru Usług Medycznych podstawowe techniki analityczne, jak OLAP czy *Data Mining*, mogą okazać się mało przydatne ze względu na znaczne rozproszenie danych. Wydaje się, że w takiej sytuacji obiecującą technologią może być wykorzystanie mobilnych i współdziałających ze sobą agentów programowych.

Literatura

Bielewicz A., *Znów mamy szansę być liderem*, „Computerworld" 31.01.2005.

Brycki G., *Informatyzacja to miliardy oszczędności*, „Rzeczpospolita" 13.09.2005.

Chan P.K., Fan F., Prodromidis A., Stoflo S., *Distributed Data Mining in Credit Card Fraud Detection*, IEEE Intelligent Systems Nov/Dec 1999.

Graco He, H., W. & Yao, X., *Application of Genetic Algorithms and k-Nearest Neighbour Method in Medical Fraud Detection*, Proc. of SEAL, 1998.

Hongxing H., Warwick G., Xin Y., *Application of Genetic Algorithm and k-Nearest Neighbour Method in Medical Fraud Detection*, "Lecture Notes in Computer Science" 1998, vol. 1585.

Jadczak A., *Miejsce, w którym chora jest informatyka*, „Computerworld" 02.11.2004.

Krupa T., *Bimber zamiast RUM-u*, „Computerworld" 29.09.2003.

Major J., Riedinger D., *EFD: A Hybrid Knowledge/Statistical-based System for the Detection of Fraud*, "Journal of Risk and Insurance" 2002 nr 69(3).

Pathak J., Vidyarthi N., Summers L., *A Fuzzy-based Algorithm for Auditors to Detect Element of Fraud in Settled Insurance Claims*, Odette School of Business Administration, Working Paper 2003 nr 03-9.

Piński J., Trębski K., *RUMowisko Balickiego*, „Wprost" 2005 nr 1165.

Prodromidis A., Stoflo A., *Agent-Based Distributed Learning Applied to Fraud Detection*, CUCS- -014-99.

Przybyłka A., *Rola informatyzacji jako narzędzia wspomagającego procesy leczenia i zarządzania w opiece zdrowotnej*, „Antidotum" 2002 nr 6.

Raport NIK „Informacja o wynikach kontroli utworzenia i funkcjonowania Narodowego Funduszu Zdrowia", lipiec 2005.

Samcik M., *RUM – system informatyczny w służbie zdrowia*, „Gazeta Wyborcza" 13.04.2004.

Strug A., *Tworzenie idealnego systemu ochrony zdrowia: Rejestr Usług Medycznych – stary czy nowy*, „Służba Zdrowia" 2002 nr 48-50.

Wang H., Mylopoulos J., Liao S., *Intelligent Agents and Financial Risk Monitoring Systems*, "Communication of the ACM", March 2002, vol. 45, nr 3.

Wang J., He H., Graco W., Hawkins S., *Application of Neural Networks to Detection of Medical Fraud*, "Expert Systems with Applications" 1997 nr 13.

Wu J., Park J., *Intelligent Agents and Fraud Detection*, www.glennshafer.com/courses/downloads/wupart.pdf, 2001.

MOBILE AGENTS IN POLISH HEALTH CARE SYSTEM

Summary

The main aim of introducing complex information systems into public health care system is to reduce number of frauds. The most popular conception considers distributed architecture with many servers collecting necessary data. In such architecture, methods like OLAP or even data mining can turn out to be useless or, at least, not efficient enough. In the paper, typical methods of medical fraud detection are presented and a mobile agents technology is proposed, as the promising tool for this purpose.