

지능형 에이전트를 활용한 전자수표시스템

윤한성, 이재규

한국과학기술원 테크노경영대학원
yhs@msd.kaist.ac.kr

요약

기존의 수표체계(paper based check system)와는 달리, 전자수표시스템(electronic check system)에서는 지능형 에이전트의 기능을 활용하여 전자수표책(electronic checkbook)이 스스로 수표구좌(checking accounts)를 관리할 뿐만 아니라 부도수표의 발행을 미연에 방지할 수 있다. 수표책 에이전트(checkbook agent) 혼자서 부도수표의 발행(issuance)에 대한 판단이 어려운 경우, 은행의 중앙컴퓨터와 접속이 가능한 발행자은행의 통제에이전트(bank control agent)와 협조하게(cooperation) 된다. 이러한 두 단계의 여과(two levels of screening)를 통해, 수표구좌를 통제할 책임이 있는 발행자의 은행과 과도한 통신부담없이 악성수표(bad checks)의 발행을 막을 수 있다. IC 카드와 같이 인터넷상에 이러한 수표체계를 구현하기 위하여, 전문가시스템기능을 갖춘 지능형 에이전트의 구조와 에이전트간 메세지 구성을 보안을 고려하여 설계하였다.

1. 서론

인터넷을 통한 전자상거래(electronic commerce)의 급격한 확산과 함께[14][30][44], 안전하고 효율적인 전자지불시스템의 개발에 대해 많은 시도가 이루어지고 있다[31][6][21]. 현재 인터넷상에서 흔히 채택되는 지불방법은 신용카드, 전자이체, 전자수표 등이며, 보안(security)이 인터넷 지불의 주요 관심사가 됨과 더불어 SET(Secure Electronic Transaction)이 호응을 얻고 있다. 한편, 기존의 수표시스템(paper check system)은 긴 역사와 함께 아직도 미국의 경우에 가장 많은 지불이 수표에 의해 처리되고 있다[18].

수표지불을 전자환경상에 그대로 구현한 시스템(mere electronic version of the check payment)은 전자이체지불(electronic fund transfer, EFT) 또는 신용카드지불과 유사한 경우가

많다. 피지불자(payee)의 수표지불청구와 정산요구가 전자적으로(electronically), 그리고 지불(payment)과 거의 동시에(simultaneously) 진행되므로 피지불자에 대한 신용(외상)지불(credit-based payment)에 의한 자금활용의 유연성(flexibility in cash flow)이라는 장점이 더이상 쉽지 않게 된 점에서 전자이체지불과 유사해졌다. 그리고 신용기반의 수표지불이라는 장점을 살리기 위해 정산일자를 제도적으로 고정한다면, 지불자의 입장에서 신용카드지불과 유사해진다. 그런데, 신용카드와 수표체계의 기본적인 차이점의 하나는 지불승인(payment authorization)의 빈도(frequency)인데, 신용카드지불은 매지불시 승인이 필요하지만, 수표체계에서는 수표책(checkbook)단위로 승인을 받으므로 부도위험(default risk)의 방지를 위한 승인의 필요성이 적다.

기존의 수표체계(paper check system)에서는, 피지불자가 부도위험을 추정하기 위해 지불자 수표구좌의 잔고(balance)를 확인할 수 없으며, 지불자의 은행도 수표의 정산요구가 있을 때까지 불온한 의도의 수표발행(check issuance)을 통제할 수 없다. 피지불자가 부도위험을 제거할 수 있는 유일한 방법은 보증수표(certified check)를 받는 방법이지만, 이는 일상 수표지불상에서는 유지하기 어렵다.

한편, 동적인 자기 통제기능(dynamic self-control capability)과 은행에이전트(또는 사이버공간에서의 일반적인 신용정보관리자)에 대해 필요한 시점에 통신상의 질의(timely electronic inquiry)기능을 갖춘 전자수표책 에이전트(electronic checkbook agent)를 도입함으로써 엄청난 양의 지불승인노력없이 사전에 부도위험을 줄일 수 있다. 만약 부도위험이 이러한 시스템에 의해 상당부분 줄어든다면, 피지불자의 관점에서 부도의 위험을 제도적으로 제거할 수 있다. 즉, 심각한 부도위험이 사전에 제거된다면 이러한 위험은 지불자의 벌과금(penalty)으로 보상할 수 있거나, 또는 지불자의 은행(payer bank)이 마치 기존의 신용카드사처럼 매출증가에 의해

부도손실을 감당하거나, 만약 지불자나 피지불자의 서비스사용료(fee)가 적다면 부도위험에 대해 재무보험 등으로 처리할 수도 있다.

본 연구에서는, 기존수표(paper check)의 장점인 “지불자의 관점에서 신용기반의 수표발행”을 추구하고, 단점으로 지적되는 “피지불자의 관점에서 부도위험을 제거”할 수 있는 전자수표시스템을 모색하고자 한다. 이것은 기존의 신용카드체계보다 훨씬 경제적이며 기존의 수표체계보다 부도위험으로부터도 자유롭다. 이러한 연구의 목적을 수행하기 위해 분산된 에이전트기반 시스템(distributed agent-based system)을 제안하고자 한다. 본 연구에서 제안한 시스템을 SafeCheck이라고 부르기로 하며, SafeCheck은 세 종류의 에이전트, 즉, 지불자 측면에서의 checkbook 에이전트, 피지불자 측면에서의 check-receipt 에이전트, 그리고 지불자나 피지불자의 은행 측면에서의 bank's control 에이전트를 갖는다. 이러한 에이전트의 구조, 에이전트간의 메시지, 그리고 최소한의 통신량으로 에이전트간의 일관성을 유지할 수 있는 프로토콜 등을 설계하기로 한다. 특히, SafeCheck의 구조(architecture)를 결정하기 위해 여러 모델들을 구성하고 전자수표시스템의 필요사항(requirements)에 대해 평가하였다. 또한, 암호화(encryption), 부인방지(non-repudiation), IC카드응용 등에 대해서도 고려하였다.

2. 전자지불시스템 형태(Types)

2.1. 전자지불시스템의 분류

인터넷상에서 확인할 수 있는 4가지의 전자지불시스템을 <표-1>에서 이러한 시스템들을 구분할 수 있는 전형적인 특징으로써 분류하였다.

(1) 전자현금 (electronic cash)

전자현금형태에서는 지불이후에 별도의 정산처리가 필요없으며, 모든 지불절차는 지불자와 피지불자 사이에 지불정보의 교환으로 완료된다. CyberCoin[8]의 경우, 지불자의 수표구좌나 신용카드로부터 전자현금화된 가치가 전자지갑으로 이전하게 된다. 그래서 CyberCoin의 전자현금은 실제 현금과 똑 같은 가치를 갖게 되는데, Mondex[26]나 이와 유사한 IC카드형태의 지불시스템은[43] 모두 이 형태의 전자지불시스템에 속한다.

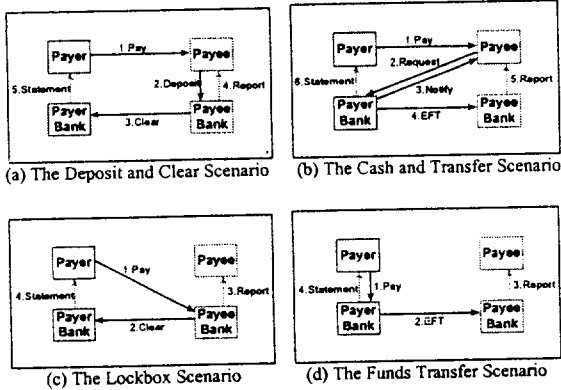
(2) 전자수표 (electronic check)

수표형태로 분류된 전자지불시스템은 다양한 형태의 모델을 갖는다. FSTC의 전자수표 프로젝트의 경우[16] 지불참가자간에 여러 지불시나리오가 <그림-1>과 같이 제시되었는데, 'Lockbox Scenario'나 'Funds Transfer Scenario'는 전자이체에 오히려 가까운 특성을 지닌다. 이는 앞서 언급한

<표-1> 전자지불시스템의 형태

Attributes	Electronic Cash	Electronic Check	Electronic Fund Transfer	Credit Card	Defaultless Check
anonymity of payer and payee	anonymous	identified	identified	identified	identified
default risk to payee	risk free	risky (unless certified check)	risk free	risk free	risk free with the complementary administrative treatment
permission of credit	not allowed	allowed	not allowed	allowed	allowed
issuance authorization frequency	availability of cash in the wallet	in principle, once for every checkbook (A variation may be checked for every issuance.)	once for every payment	once for every payment	once for every checkbook if credible (The level of credibility can be dynamically adjusted.)
available systems	Ecash[11], NetCash[25], CyberCoin[8], Modex[27], VisaCash[43]	FSTC's Electronic Check[16], NetCheque[30], VirtualPin[13], NetBill[5], PayNow[9], NetChex[28]	SFNB's QuickPay[36]	CyberCash[7], SET protocol[24]	SafeCheck

전자이체와 전자수표의 결합(merging)현상을 반영한 것으로 볼 수 있다. First Virtual의 VirtualPin 시스템[5]은 지불자의 지불후 별도의 정산기관의 서비스없이 직접 지불자의 계좌로부터 출금하여 정산처리를 수행한다.



<그림-1> 전자수표체계의 가능한 시나리오[16]

(3) 전자이체 (electronic fund transfer)

SFNB(Security First Network Bank)의 QuickPay[36]는 전자이체형태로 분류되는데, SFNB가 지불자의 인터넷상에서 입력한 지불지시에 따라 지불자의 계좌로부터 피지불자의 계좌로 이체지불한다. 피지불자가 이체지불을 원하지 않는 경우, 종이수표를 SFNB가 우송한다는 점에서 수표지불형태처럼 보이기도 하지만, 수표지불전에 지불자의 계좌에서 지불금액이 차감된다는 점에서 전자이체지불형태로 분류된다.

(4) 신용카드 (credit card)

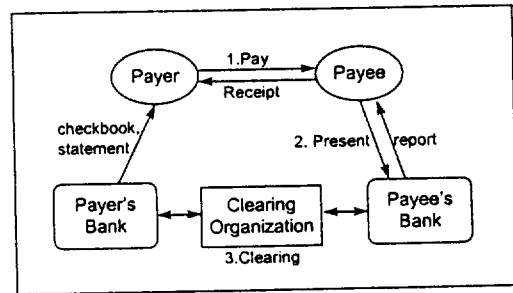
인터넷 쇼핑몰(shopping mall)에서 아직도 많은 지불이 사용자의 ID나 신용카드의 번호를 SSL(Secure Socket Layer) 형태의 암호화를 통해 피지불자의 웹페이지에 입력하는 형태로 이루어지고 있는데, 이와 같이 안전하지 못한 방식은 대다수의 고객(지불자)가 인터넷을 통해 구매/지불을 꺼려 하는 이유중의 하나이다. 이러한 문제를 극복하기 위해 SET(Secure Electronic Transaction) 프로토콜이 최근 개발되었다[24].

(5) SafeCheck

<표-1>에서 분류한 바처럼, 피지불자의 입장에서 부도위험을 제거하거나 최소한 줄이고, 경제적인 지불승인과정을 거치며, 신용기반(credity-based) 지불을 허용하기 위한 새로운 형태의 전자지불 시스템으로, 지능형 에이전트 기반 시스템으로 본고에서 제안하고자 한다.

2.2. 수표의 종류 및 처리

4 가지의 전형적인 지불시스템으로부터 변형된 형태로 발전할 수 있는데, 보통수표(regular check)로부터는 보증수표(certified check)이나 횡선수표(crossed check) 등을 그 예로 들 수 있다. 담보나 높은 신용등급을 근거로 한 보증수표는 보통수표와 유사하지만, 지불자의 은행이 보증한 한도내에서 수표지불이 가능하다. 그리고 횡선수표(crossed check)이나 매김수표(quoted check) 등은 구매상품이나 처리은행에 제한이 있다. 이러한 수표의 공통적인 처리과정은 <그림-2>과 같으며, 여러 은행간 수표의 교환 및 정산을 효율적으로 처리하기 위한 과정으로 중앙 정산기관이 필수적이다. 한편, 중앙집중적인 정산서비스는 인터넷과 같은 전자환경에서 은행간 직접적인 교환과 경쟁적인 관계에 있을 수 있다. 그러나, 본 연구에서는 현시점에서 일반적인 서비스인 중앙집중적인 정산서비스가 존재하는 것을 가정으로 하기로 한다.



<그림-2> 수표의 일반적인 처리과정

3. 전자수표시스템의 구조

SafeCheck의 위치를 다른 수표지불 시스템과 비교하기 위하여 기존의 전자수표 시스템의 구조적 모델(architectural models)을 분류하였다. 구조적 특징을 구분하는 기본적인 요인(factors)은 게이트웨이(gateway), 정산, 계좌보유(account storage) 서비스의 주체에 의한다.

3.1. 전자수표시스템의 4 가지 구조적 모델

(1) 지불 게이트웨이형 모델

이 모델에서는, 지불서비스 시스템이 인터넷상의 사용자(지불자 또는 피지불자)와 전용 금융망간의 지불 게이트웨이 역할을 한다. 모든 수표지불정보는 이 중앙집중적인 서버를 거쳐 은행의 주시스템(mainframe)으로 전달된다. 지불자의 자격확인(identification)은 모든 지불마다 지불 게이트웨이 서버에 의해 수

행된다. 하나의 중앙집중형 정산기관 (clearing house)은 인터넷외부에 존재한다. PayNow[9]나 NetChex[28]가 이 모델에 속한다. 이 모델의 장점은 다른 게이트웨이를 사용하는 사용자일지라도 동일한 정산기관에 의해 정산처리되므로 사용자그룹을 분리 (segregate)하지 못한다.

(2) 은행 게이트웨이형 모델

각 은행이 지불 게이트웨이 서버를 보유하는 지불 게이트웨이 모델의 특별한 경우이다. 한편, 은행은 지불 게이트웨이 서버를 외부 아웃소싱(outsourcing)할 수도 있을 것이다. FSTC의 전자수표[16] 또는 NetCheque[31]이 이 모델에 속한다.

(3) 게이트웨이-정산형 모델

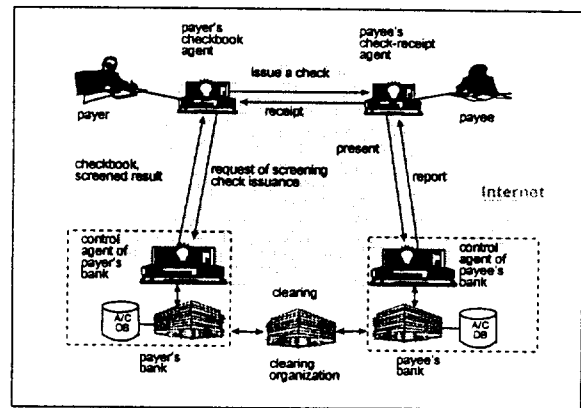
이 모델에서는, 지불 게이트웨이 서버가 지불 게이트웨이의 역할 뿐만 아니라 정산서비스도 제공한다. 지불 서비스 서버는 정산처리를 위한 수표정보를 갖는다. 이 모델의 장점은 이 서버에 등록된 고객과 은행간의 효율성 (efficiency)을 들 수 있다. 반면, 다수의 경쟁적인 정산기관이 있는 경우 정산상의 혼란이 있을 수가 있다. 정산기관간의 분리는 결국 사용자그룹을 분리하게 되는 결과를 초래한다. First Virtual의 VirtualPin[13]이 이에 속한다.

(4) 가상은행형 모델

지불 게이트웨이 서버가 완전한 은행의 역할을 하는 경우이다. 이 가상은행에 구좌를 가지고 있는 사용자간에는 정산을 포함한 전 지불처리 과정을 이 서버가 커버(cover)한다. 지불자와 피지불자가 같은 가상은행의 고객이라면, 가장 경제적인 구조이다. 그러나, 다수의 가상은행이 정산체계의 공유없이 서로 경쟁하는 관계인 경우에는, 사용자는 심각하게 분리되는 한계를 가진다. 카네기멜론대학의 NetBill[5]이 이 경우에 속한다.

3.2. SafeCheck의 구조

SafeCheck이 어떤 은행의 구좌를 가지는 사용자에 대해서도 서비스를 제공하기 위해서는, 사용자그룹을 분리하는 구조는 적당하지 않다. 더우기, 각 은행이 자신의 전자 수표책 (electronic checkbook)을 발급하도록 하기 위해서는 가장 적절한 구조가 은행 게이트웨이형 모델이다. 따라서, SafeCheck의 구조를 <그림-3>와 같이 설계하였다.

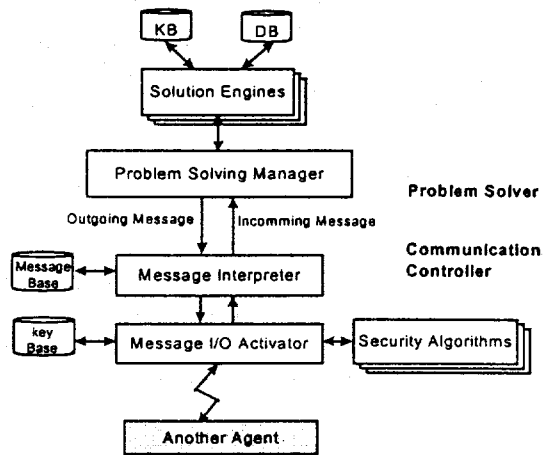


<그림-3> SafeCheck의 구조

4. SafeCheck에서의 에이전트 구조

4.1. 지능형 에이전트(Intelligent Agents)의 구조와 역할(roles)

지능형 에이전트에 대한 다양한 정의가 있지만[15][17][42], 공통의 속성으로 받아들여지는 것들은 자율성(autonomy), 통신기능(communication ability), 추론기능(reasoning capability), 학습기능(learning capability) 등이다[15][32]. 또한, 지능형 에이전트의 재무금융분야(financial area)에서 활용할 수 있는 분야로 개인은행업무 에이전트(personal banking agent), 전자지불 에이전트(electronic payment agent), 예산관련 에이전트(budgeting agent) 등이 제안되었다[34]. SafeCheck에서의 지능형 에이전트("SafeCheck-에이전트"로 부르기로 함)는 크게 문제해결기(problem solver)와 통신제어기(communication controller)의 두 부분으로 구성되어 있다. 추론기능(inference engine 혹은 solution engine)을 갖는 기존의 전문가시스템과 비교한다면, SafeCheck-에이전트는 <그림-4>와 같이 문제해결관리기(problem solving manager)와 통신제어기(communication controller)를 추가적으로 갖는다고 할 수 있다. 이 SafeCheck-에이전트는 UNIK-에이전트[23]의 개념으로부터 설계되었다. 지불거래참여자의 SafeCheck-에이전트는 동일한 구조를 갖으나, bank control 에이전트는 다른 것보다 한층 복잡하고 대용량의 지식베이스나 데이터베이스를 갖는다.



<그림-4> SafeCheck 에서의 지능형 Agent 구조

4.1.1. 문제해결기(Problem Solver)

문제해결관리기(Problem solving manager)와 해결엔진(solution engines)이 문제해결기의 주요 구성요소이다. 문제해결관리기는 에이전트에 대한 모든 처리과정을 통제하며, 외부로부터 전송된 메시지에 대해 적절한 해결엔진이 문제해결관리기에 의해 선택되고 운영된다. 해결엔진(solution engines)은 정방향추론(forward chaining), 신경망에 의한 추정이나 분류(neural network based estimation or classification), 지식기반형 추론(knowledge-based reasoning), 단순함수(simple function) 또는 메시지 생성(message generation)과 같은 문제해결방법(problem solving methods)의 집합체이다. 각각의 SafeCheck-에이전트는 역할에 맞게 서로 다른 해결엔진들을 갖는다.

그리고, SafeCheck-에이전트는 혼자서 또는 협조적으로(individually or cooperatively) 전자수표지불과 SafeCheck 서비스에 등록된 수표구좌의 관리를 한다. 여기서 우리는 이전에 수행된 많은 지능형 해결방안에 관한 연구들로부터 아이디어를 얻을 수가 있다. 예를 들면, 채권등급결정(bond rating), 신용등급결정(credit rating), 신용한도결정(credit limit deciding) 등과 같은 금융상의 목적(financial purpose)으로 인공지능망이 활발히 연구되었고 또 좋은 성능을 보였다[1][33][38][41]. 규칙기반형이나 또는 혼합형 접근방법을 통해 신용금액산정이나 대출 의사결정지원 등을 해결하기도 하였는데 [4][35][37], 이는 신용금액산정을 가지고 수표지불에서 신용금액산정을 통한 당좌대일한도를 결정하는데 활용할 수 있다.

자체적으로 갖는 적절한 해결엔진들을 통해, 각 에이전트는 다음과 같은 필요한

처리과정(proceesing)을 수행한다. 지불자의 checkbook 에이전트와 피지불자의 check-receipt 에이전트는 은행으로부터 수표처리기능중 상당한 부분의 고유기능을 위임받아(delegated) 처리한다.

(1) checkbook 에이전트

- 지불자의 수표구좌개설요청 판단 및 bank control 에이전트에 요구 : rule-base
- 백지수표요구시점 결정 및 bank control 에이전트에 요구할 백지수표량 산정 : rule-base
- 수표당 발행상한액 및 미정산 발행수표의 총금액 상한 결정 : rule-base
- 부도가능수표(suspicious) 발행의 스크리닝(screening)
 - 수표가 한도내에서 발행되는지 확인
 - 한도밖의 수표발행에 대해 bank control 에이전트에 대해 자문

(2) check-receipt 에이전트

- 받은 전자수표가 선호하지 않거나 (unpreferred) 부적절한(illegitimate) 경우 환송: rule-base
- 받은 전자수표에 대해 bank control 에이전트에 대해 지불요구 : rule-base
 - rule-base parameter : 받은수표의 유효일자, 피지불자의 선호구좌 등

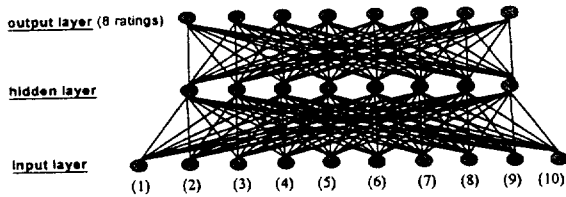
(3) bank control 에이전트

- 수표구좌개설 결정 : rule-base
- 수표구좌의 신용등급 결정이나 변경 : neural network
- 수표구좌형식(checking account modality)의 변경이나 정지 : rule-base
- checkbook agent로부터 요청받은 부도가능수표의 스크리닝(screening) : rule-base

지식베이스나 데이터베이스를 사용하여, SafeCheck-에이전트는 해결엔진(solution engine)을 수행할 모델이나 데이터를 보관한다. 모델을 지식베이스에 의미적 형식(semantic form)으로 보관하는 것은 다른 모델과 지식의 공유(share)가 용이하고, SafeCheck-에이전트의 내부언어(inner language)[40]인 UNIK-Object[20]로써 모든 모델을 관리하기가 용이하다. 예를 들면, 한 은행의 수표구좌에 대한 신용등급평가기능(credit rating)은 bank control 에이전트의 지식베이스에 의미적 표현으로 저장된 정방향 인공지능망(feedforward neural network)으로 [그림-5]과 같이 구성할 수 있는데, 10개의 입력노드와 8개의 노드를 갖는 은닉층, 그리고 8개의 출력노드를

갖는 인공지능경망이다.

각 SafeCheck-에이전트의 지식베이스나 데이터베이스는 변경권한(modification authority)에 따라 구분된다. 즉, 사용자나, 다른 에이전트 또는 자신에 의해서 변경되거나 갱신된다. 더우기, checkbook 에이전트나 check-receipt 에이전트의 경우에는 지식베이스나 규칙베이스 등이 bank control 에이전트에 의해 교환되거나 갱신된다.



- (1) average balance of saving accounts for recent 3 months
- (2) holding period of saving account
- (3) kind of possessing credit card
- (4) period of wage or pension transfer to the saving account
- (5) yearly amount of public charges from saving account
- (6) yearly amount of property tax in the recent year
- (7) working period of the recent place
- (8) monthly amount of wage or pension for the recent year
- (9) age
- (10) marriage or family members

<그림-5> 신용등급결정을 위한 인공지능망

4.1.2. 통신제어기

통신제어기는 메시지 해석기(message interpreter), 메시지 입출력기(message I/O activator) 그리고 보안알고리즘(security algorithms)으로 구성된다. 메시지해석기는 입출력하는 메시지를 해석하고 검증하는 것이외에 문제해결과정을 시작하게 한다. 메시지입출력기는 입출력 메시지의 흐름을 다루는데, 적절한 보안알고리즘을 가지고 보안프로토콜(security protocol)을 관리하고 TCP/IP 나 X.25 등의 통신프로토콜에 통해 암호화된 메시지를 전송하거나 전송받는다.

4.2. 부도방지형 전자수표(Defaultless Electronic Check)

4.2.1. 부도전자수표방지를 위한 방안(approaches)

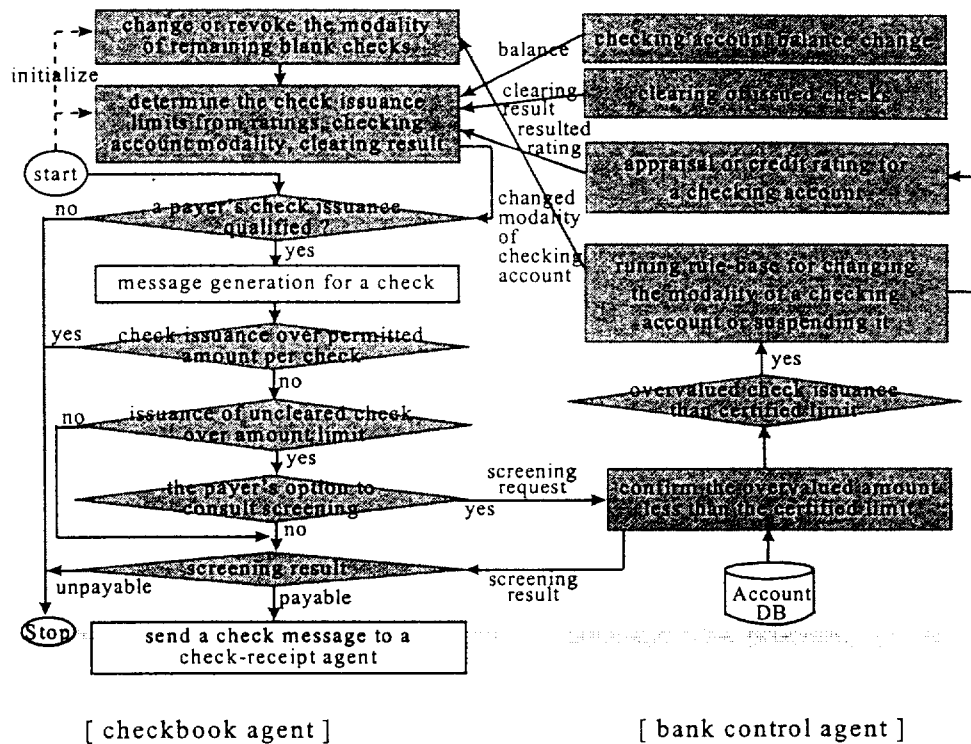
SafeCheck에서는, 두 단계(two-level)의 스크리닝(screening)으로 <그림-6>에 나타난 바와 같이 전자수표의 부도지불을 방지하고자 한다. 첫단계 스크리닝(level-1 screening)에서, 지불자의 checkbook 에이전트는 전자수표당 한도금액을 초과하거나 미정산 수표를

한도이상 발행하는 경우를 감시(monitor)하는데, 이는 checkbook 에이전트의 수표발행기록(issuance record), bank control agent로부터 전송받는 정산결과나 수표구좌의 잔고(balance) 등을 평가하는 규칙베이스(rule-base)에 의해 수행된다. Bank control 에이전트로부터의 정보는, 만약 checkbook 에이전트가 얼마동안 꺼져(shutdown) 있었을 경우에는 새로이 통신에 의해 갱신된다.

만약 수표발행허용에 대한 결정이 checkbook 에이전트 혼자서 불확실한 경우에는, bank control 에이전트는 지불자의 선택(payer's option)이 있는 경우 bank control 에이전트에게 자문을 요청한다. 발행수표가 보증한도를 초과 발행하는 시점을 bank control 에이전트가 확인하였을 때는, 지불자은행의 bank control 에이전트는 수표구좌의 형식(modality)을 변경하거나 지불정지(suspension)를 결정할 규칙베이스(rule-base)를 수행한다. <그림-7>에서의 AND/OR 그래프의 규칙베이스는, 수표구좌의 형식을 지불자의 지불기록(issuance record)에 따라 '보통수표의 구좌'나 '보증수표의 구좌' 또는 '지불정지'의 결정을 자동으로 처리한다. 변경된 수표구좌의 형식에 따라, 수표구좌의 신용등급은 새로이 결정된다. 이러한 변화나 발행수표의 정산(clearing)이 발생할 때마다 checkbook 에이전트의 수표발행한도는 수정된다. 대부분의 의심스러운 수표발행의 스크리닝은 checkbook 에이전트에 의해 수행되므로, <그림-6>의 에이전트간 통신요구 빈도는 매우 적다.

4.2.2. 고안된 방안에 대한 유효성 검증

부도방지형 전자수표시스템을 위해 제안된 방안의 유효성(effectiveness)을 검증하기 위하여, 기존의 수표시스템(conventional paper based check system)에서의 부도요인을 SafeCheck에 적용하여 보았다. 부도의 가장 큰 두가지 요인은 지불정지된 수표구좌로부터 이미 교부된 백지수표를 가지고 수표를 발행하는 경우와 발행된 수표를 정산할 수표구좌의 잔고가 충분하지 않을 경우이다. 이러한 사유를 포함한 부도사유가 <표-2>와 같이 SafeCheck-에이전트에 의해 제거될 수 있다.



<그림-6> 전자수표의 부도방지를 위한 2 단계 스크리닝(two level screenings)

에이전트간 SafeCheck의 문제해결의 효율성(efficiency)을 위해, 기존의 수표체계(paper based check system)에서는 은행에 의해 수행되었던 처리과정(processes)을 checkbook 에이전트가 상당부분 책임있게 처리하게 하였다. Checkbook 에이전트는 혼자서 해결할 수 없는 부분을 bank control agent와 협조적으로(cooperatively) 문제를 해결할 수 있다. 따라서, bank control agent에 대한 통신요구량은 대폭 감소되고, 전체의 문제해결 부담을 에이전트간에 분담함(sharing)으로써 효율적으로 수행된다.

심각한 부도위험이 두단계의 스크리닝을 통해 제거될 수 있으므로, 수표발행자의 은행이 피지불자에 대한 추가부담(additional fee)없이 지불을 보장할 수 있다. 반대로 악성 수표발행자(bad issuer)는 은행에

벌과금(penalty)을 지불해야 하고, 이러한 기록은 개인의 전자 checkbook 에이전트나 bank control 에이전트에게 보고된다. 이러한 기록은 checkbook 에이전트나 bank control 에이전트에 있는 규칙베이스(rule-base)에 따라 수표발행의 발행한도를 조정하게 된다.

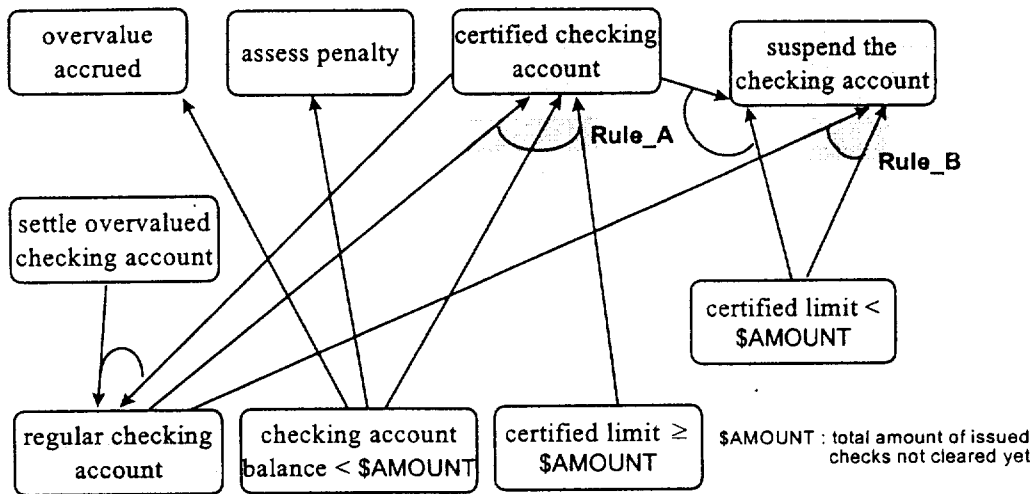
5. 에이전트간의 메시지

5.1. 메시지 구성

SafeCheck-에이전트의 외부언어(outer language)로 KQML(Knowledge Query and Manipulation Language)을 활용하여, <그림-8>과 도시한 바와 같이 TCP/IP 통신계층(layer)의 상위 3계층으로 메시지 구조를 설계하였다. 그중 ACL(Agent Communication Language)계층은

<표-2> SafeCheck 에서의 부도가능수표 (suspicious check)의 제거

causes of default in paper checks	screening agent	default risk of a legal payee
check issuance from a suspended checking account	bank's control bank	eliminated
insufficient balance of a checking account	bank's control bank	eliminated
check issuance over the amount limit	checkbook agent	eliminated
defect of check form	checkbook agent	eliminated
false signature	all agents	eliminated



(a) AND/OR 그래프

```

[[ RULE_A
  IF [checking_A/C checking_A/C_of_receiving_message] ;; local binding
      (equal checking_A/C 'regular_checking_A/C)
  AND (more_than issued_checks_amount balance_of_checking_A/C)
  AND (not_more_than issued_checks_amount certified_limit_of_checking_A/C)
  THEN (change_modality checking_A/C 'certified_check) ]]
```

```

[[ RULE_B
  IF [checking_A/C checking_A/C_of_receiving_message] ;; local binding
      (equal checking_A/C 'regular_checking_A/C)
  AND (more_than issued_checks_amount certified_limit_of_checking_A/C)
  THEN (suspend_checking_account checking_A/C) ]]
```

(b) 규칙 예(역방향 추론)

<그림-7> 수표구조형식 변경을 위한 AND/OR 그래프와 규칙

응용영역(domain)과는 무관한 KQML[40]의 performative와 그것의 파라메타(parameter)로 구성된다.

다음으로, Security계층은 메시지교환의 보안처리(security processing)를 위해 “:content” 파라메타(parameter)에서의 구성요소(components)를 보유하기 위해 고안되었다. 새로운 보안 파라메타(Security parameter)를 도입[39]하기 보다, SafeCheck에서는 내부언어(inner language)로 구성과 조작이 가능하도록 보안요소(security components)를 구성하였다. Check계층의 모든 메시지 구성요소는 “message”항목의 <encrypted-message-content>에 암호화되어 포함된다. 다른 구성요소와 함께, Security계층은 다음과 같이 구성된다.

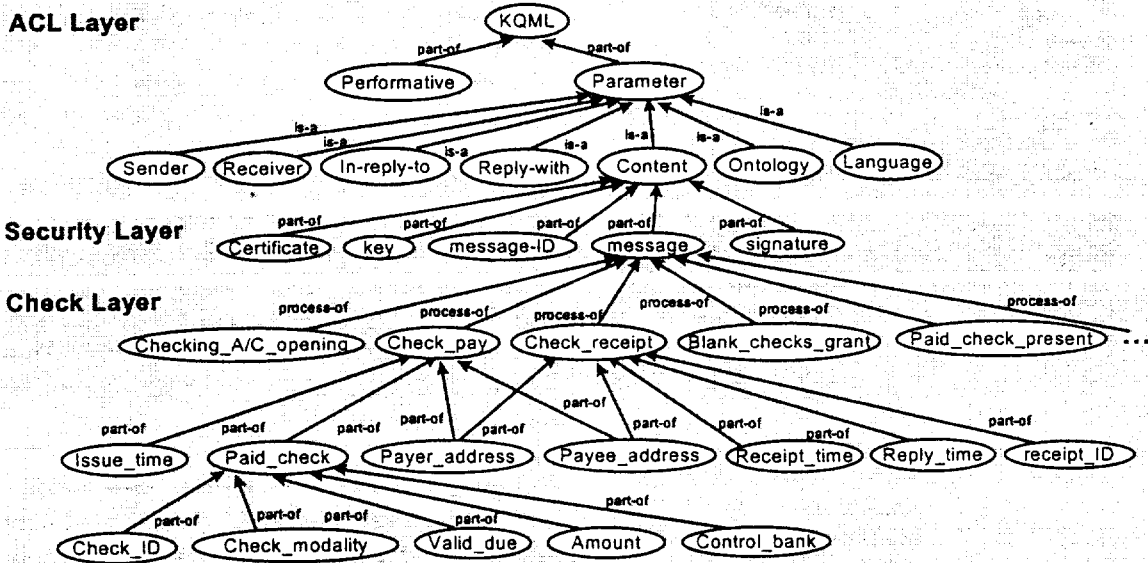
```

(message <encrypted?> <enc-type>
  <encrypted-message-content>)
(key <enc-type> <encrypted-key>)
```

```

(message-ID <encrypted-message-ID>)
(certificate <own-certificate> <CA-certificate>)
(signature <digest-type> <signature>)
```

“message”항목에서의 <enc-type>는 “key”항목의 대칭형키(symmetric key)를 암호화하기 위한 비대칭 알고리즘[3]을 나타낸다. “key”항목은 “message”의 <encrypted-message-content>를 생성하기 위한 대칭형 암호화의 암호화 방법과 피전송자의 공동키(public key)로 암호화된 대칭형키로 구성된다. 전송되는 각 메시지는 암호화된 “message-ID”항목을 갖는데, 이것은 메시지의 이중사용방지(replay)를 위한 것이다. “certificate”항은 전송자(sender) 에이전트와 인증기관(certificate authority)의 전자인증서(electronic certificate)를 전송하기 위한 것이다. 그리고 <signature>는 전송자 에이전트의 개인키(private key)로 암호화된 check계층 내용의 해쉬(hash)이다. 본 논문에서 자세히 설명되지는 않았지만, 메시지



<그림-8> SafeCheck에서의 메시지게층

교환프로토콜에 의해 각 메시지를 전송할 때에 모든 부분은 아니지만 필요한 부분이 Security계층에 포함된다.

check계층은 [그림-8]에서와 같이 수표구좌의 개설요구(checking account opening request), 수표지불(check payment) 등과 같은 여러 기본적인 처리(elementary transactions)와 정보부분(information parts)를 정의한다. 전자수표와 그것의 영수확인(receipt)에 관해 메시지 구성요소가 [그림-8]에 도시되었다.

5.2. 메시지 생성(Message Generation)

Security계층의 “message”항목에 암호화되어 포함된 여러 내부 메시지는 에이전트간의 자율적 또는 협조적으로 (autonomously or cooperatively) 수행된 문제해결절차(solution procedure)의 결과에 따라 생성된다. 본 섹션에서는 전자수표의 발행의 예제를 통해 메시지생성을 설명하기로 한다. 메시지의 생성은 에이전트나 사용자에 의해 개시(initiate)된다. 수표메세지는 사용자인 지불자(human payer)의 주도(trigger)로 생성된다. 다음으로, 지불자의 최종확인으로 발행함에 앞서, checkbook 에이전트는 부도수표의 방지를 포함한 필요한 절차를 자율적 또는 협조적으로 처리함으로써 메시지 생성작업을 수행한다. 다음과 같은 단계를 거쳐 전자수표는 발행되고 check-receipt 에이전트에게 전송된다.

(1) checkbook 에이전트는 지불거래 대상인 지불자의 check-receipt 에이전트로부터 보내온

MIME형태의 지불정보와 보유 수표구좌를 비교한 후, 지불가능한 수표구좌를 선택한다.

(2) 사용자(payer)의 최종확인을 거쳐, checkbook 에이전트는 [그림-9]의 스크리닝 처리과정을 거쳐 전자수표를 발행한다. 생성된 수표메세지는 checkbook 에이전트의 통신제어기에 의해 필요한 암호화과정과 ACL형태로 변환되어 지불거래 상대자인 check-receipt 에이전트에게 전송된다. 예시적인 메시지의 내부 형태(inner form)는 다음과 같다.

```
<Check
  <Payer_address          **** *
  <Payee_address          **** *
  <Issue_time              961201/093455>
  <Paid_check
    <Check_ID              encrypted_value >
    <Check_modality        Regular>
    <Valid_due              961216/093455>
    <Amount                 70000>
    <Control_bank           Hanil_bank>>>>
```

(3) 피지불자의 check-receipt 에이전트는 다음 섹션에서 설명할 “Reply” performative를 통해 다음의 내부 형태(inner form)의 영수증(receipt)을 checkbook 에이전트에게 전송한다.

```
<Check_receipt
  <Payer_address          **** *
  <Payee_address          **** *
  <Receipt_time           961201/093515>
  <Reply_Time             961202/131556>
  <Receipt_ID             76587098798>
  <Paid_check>
    <Check_ID              encrypted_value >
    <Check_modality        Regular>
```

<Valid_due 961216/093455>
 <Amount 70000>
 <Control_bank Hanil_bank>>>>

5.3. 메시지 교환(Message Exchange)

KQML[40]의 performative를 활용하여, SafeCheck에서의 기본적인 메시지 교환규칙에 따라 메시지가 교환된다. 이러한 규칙에 따라 다음과 같이 주메세지(main message)를 전송하는 performative의 교환순서를 다음과 같이 정하였다. 여기서 “A”와 “B”는 각각 전송자와 수신자를 뜻한다.

- (1) (Standby ... (performative_of_main_message ...)) ; A sends to B.
- (2) (Ready ...) ; B sends to A.
- (3) (Next ...) ; A sends to B. [B evaluates “(performative_of_main_message ...)”.]
- (4) (Reply ...) ; B sends to A the result of evaluating “(performative_of_main_message ...)”.
- (5) (Achieve ...) ; A and B confirm the main message transmission finally.

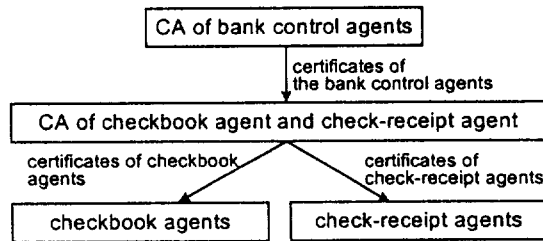
6. 보안사항의 고려

공통키 암호화방법(public key cryptography)에 따른 메시지교환의 보안을 위해, 인증기관(certificate authority, CA)은 자신의 개인키(private key)로 전자서명(electronic signature)한 거래참여자의 공유키를 포함하는 전자인증서(certificate)를 통해 각 거래참여자(participant)의 자격(qualification)을 인증한다. SafeCheck에서는, bank control 에이전트가 checkbook 에이전트나 check-receipt 에이전트를 위한 CA의 기능을 갖는다. 만일에 지불자나 피지불자가 자신의 은행에 등록된다면, 각각의 은행으로부터 인증서를 갖는다. 인증서는 개인별로 각 은행마다 거래하는 모든 구좌의 정보를 담을 수 있다. 그리고 각 등록된 은행의 CA는 인증서의 발급이나 취소를 책임지고 신뢰할 만한 제 3의 기관이 수행한다. 이러한 CA를 위한 구조는 <그림-9>와 같다.

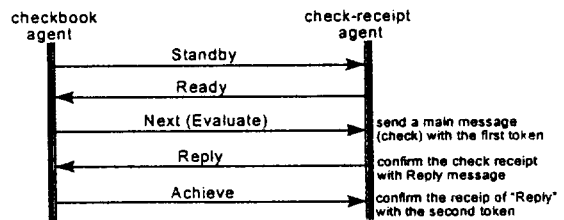
메시지교환의 무결성(Integrity), 비밀성(privacy) 그리고 인증(authentication) 등은 KQML메시지의 전자서명에 의해 보장된다. 필요한 메시지교환의 부인방지(non-repudiation)를 위해, 부인방지용 토큰(token)[19]를 활용하여 2-토큰 프로토콜을 고안하였다. 이것을 통해 쌍방향의 메시지 전달자가 제 3의 공증역할자(notarial)와 함께 서로의 부인방지를 이룰 수 있다.

2-토큰 프로토콜을 <그림-10>에서 KQML

performative를 통해 전자수표지불의 예로써 설명하였다. Check-receipt 에이전트는 두번째 토큰(second token)없이 bank control 에이전트에게 받은 전자수표에 대해 지불요구를 할 수 없다. Checkbook 에이전트는 “Reply”와 함께 전해진 수표영수증(check receipt)을 가지고 check-receipt 에이전트의 부인방지에 대처할 수 있다. 그리고, check-receipt 에이전트는 bank control 에이전트에게 받은수표의 결제(clearing)를 요구하기 위해서는 반드시 checkbook 에이전트로부터 두개의 토큰을 받아야 한다. 또한, 피지불자의 bank control 에이전트는 check-receipt 에이전트로부터 지불요청받은 수표에 대해 공증(notary)의 역할을 수행한다. SafeCheck에서 토큰은 check-ID를 포함하는데, 그것은 지불자은행의 control 에이전트의 공유키(public key)로 암호화된 것으로 bank control 에이전트로부터 교부된 전자백지수표(electronic blank check)으로 사용된다.



<그림-9> SafesCheck의 CA 구조



<그림-10> 토큰을 통한 전자수표 교환

7. 결론

본 논문에서는 세 종류의 지능형 에이전트를 활용하여 부도방지형 전자수표시스템을 제안하였다. 발행수표(issued check)의 금액과 수표구좌의 잔고를 단순비교한 대신에, checkbook 에이전트는 지능형 에이전트의 기능을 통해 수표구좌의 평가와 항상 일치하는 수표발행한도를 조정한다. 또한, checkbook 에이전트나 check-receipt 에이전트는 기존의

수표체계(conventional check system)에서 사용자나 은행에서 수행되었던 많은 부분을 직접 수행한다. 이러한 특성은 시스템간 통신부담을 줄여주고, 적은 통신부담으로써 부도방지형 수표를 구현할 수 있다.

IC카드를 통해 전자인증서(certificate)나 백지수표 또는 받은수표의 보관을 통한 보안(security)이나 전자지갑(electronic wallet)의 일반적인 응용이외에, 지능형 에이전트의 개인적인 부분(personal portion)이 IC카드으로써 휴대할 수 있는 방안도 설계가능하다. 이러한 특성은 C-SET[12]과 같은 표준과도 보조를 맞추어야 할 것이며, 전자수표처리과정이 더욱더 분산화될 것이다.

SafeCheck 은 부도위험(default risk)없이 보다 경제적이므로, 피지불자에게는 신용카드보다 매력적일 수 있다. 그리고 지불자의 신용에 기반한 신용(외상)지불이 은행의 동의하에 허용되므로 신용할 만한(credible) 지불자에게도 보다 선호될 수 있다. 신용이 나쁜(discreditable) 지불자에 대한 서비스는 모든 지불처리에 대해 bank control 에이전트에게 확인하는 신용시스템(credit system)으로 변하게 되고, 결국은 전자이체(EFT)지불과 유사하게 될 것이다. 공통적으로 부도없는 지불을 보장함으로써, 신용카드형태/ 수표형태/전자이체형태의 전자지불은 피지불자에 대한 신용(외상)지불수준(credit level)에 의해 분류할 수 있을 것이다.

참고문헌

- [1] Benachenhou, D., M. Cader, and G. Deboeck, "Implementation of a Neural Trading System", Proceedings of IJCNN '92, Vol. 1, Beijing, pp. 360-365, 1992.
- [2] C. Brown, D. E. O'Leary and A. Sangster, "AI on the WWW", IEEE Expert, pp.50-55, Aug., 1995.
- [3] Bruce Schneier, Applied Cryptography, John Wiley & Sons, Inc., 1996.
- [4] Carter C. and J. Catlett, Assessing Credit Card Applications Using Machine Learning", IEEE Expert, Fall, pp. 71-79, 1987.
- [5] C.M.U.'s I.N.I., "The NetBill Project", <http://www.ini.cmu.edu/netbill>, 1997.
- [6] A. Crede, "Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems Using the Internet", <http://jcmc.huji.ac.il/voll/issue3/crede.html>, 1997.
- [7] CyberCash, Inc., "CyberCash - Information", <http://www.cybercash.com/cybercash/news>, 1997.
- [8] CyberCash, Inc., "Introducing CyberCoin™", <http://www.cybercash.com/cybercash/shoppers/coingenpage.html>, 1997.
- [9] CyberCash, Inc., "PayNow™ Pilot Programs", <http://www.cybercash.com/cybercash/paynow>, 1997.
- [10] DigiCash, "DigiCash Products - the CAFE project", <http://www.digicash.com/products/projects/caf.html>, 1997.
- [11] DigiCash, "DigiCash - Publications", <http://www.digicash.com/publish/publish.html>, 1996.
- [12] Europay International, "Europay Profile", <http://www.europay.com/prof02.htm>, 1997.
- [13] FirstVirtual Holdings Inc., "The First Virtual Solution", <http://www.fv.com/demo>, 1997.
- [14] Forrester Research, <http://www.forrester.com>, 1997.
- [15] S. Franklin and A. Graesser, "Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents", <http://www.mscl.memphis.edu/~franklin/AgentProg.html>, 1996.
- [16] FSTC, "FSTC Electronic Check Project", <http://www.fstc.org/projects/echeck/index.html>, 1996.
- [17] D. M. Gilbert *et al.*, "The Role of Intelligent Agents in the Information Infrastructure", IBM Co. Research Triangle Park, USA, <http://activist.gpl.ibm.com:81/WhitePaper/ptc2.htm>, 1995.
- [18] The Green Sheet Online, "GreenSheet Annual Survey", <http://multiplex.com/Greensheet>, 1997.
- [19] ISO/IEC DIS 13888-3, "Information Technology - Security Technique - Non-repudiation - Part 3, 1997.
- [20] KAIST, UNIK User's Manual (in Korean), Intelligent Information System Lab., Graduate School of Management, Korea Advanced Institute of Science and Technology, 1994.
- [21] R. Kalakota and A. B. Whinston, "Frontiers of Electronic Commerce", Addison-Wesley Publishing Co., 1996.
- [22] Kukmin Bank, Procedures of Checking Account(in Korean), 1995
- [23] Lee, Jae K. and Lee, W., "Intelligent Agent Based Contract Process in Electronic Commerce: UNIK-AGENT Approach", *Proceedings of Hawaii International Conference on System Science*, USA, 1997a.
- [24] MasterCard/Visa, Secure Electronic transaction (SET) Specification(Version 1.0), May, 1997.
- [25] Medvinsky, G. and Neuman, B. C., "NetCash: A design for Practical Electronic Currency on the Internet", *Proc. Of 1'st ACM Conference on Computer and Communications Security*, 1993.
- [26] Mondex International, "Mondex Technology", <http://www.mondex.com>, 1996.
- [27] NetCash: The USC Anonymous network payment research prototype, <http://gost.isi.edu/info/NetCash>, 1996.
- [28] Net1 Inc., "NetChex homepage", <http://www.netchex.com/>, 1996.
- [29] Netscape, "SSL 3.0 Specification", <http://home.netscape.com/eng/ssl3/index.html>, 1996.
- [30] Network Wizard, "Internet Domain Survey", <http://www.nw.com/zone/WWW/top.html>, 1997.
- [31] B. Clifford Neuman and G. Medvinsky, "Requirement for Network Payment: The Netchque™ Perspective", *Proc. Of IEEE Comcon '95*, San Francisco, Mar., 1995.
- [32] Mark Nissen, "Intelligent Agents: A Technology and Business Application Analysis", <http://haas.berkeley.edu/~heilmann/agents/>, 1995.
- [33] Odom, M. D. and R. Sharda, "A Neural Network Model for Bankruptcy Prediction", *Proceedings of*

- IJCNN '90, Vol. 2, San Diego, pp. 163-168, 1990.
- [34] Personal Agents Inc., "The Future of Electronic Commerce", <http://www.yourcommand.com>, 1996.
 - [35] A. Sangster, The Bank of Scotland's Lending Adviser Expert System, COMPASS", Proc. of the 11'th Int'l Conf. on A.I. for Applications, pp. 24-30, 1995.
 - [36] Security First Network Bank, "Bank Demonstration", <http://www.sfnb.com/demos/bankdemos.html>, 1997.
 - [37] Srinivasan, V. and Y. H. Kim, "Designing Expert Financial Systems: A Case Study of Corporate Credit Management", Financial Management, pp. 23-31, Autumn 1988.
 - [38] Surkan, A.J. and J.C. Singleton, "Neural Networks for Bond Rating Improved by Multiple Hidden Layer," Proc. of IJCNN '90, Vol. 2, San Diago, pp. 157-162, 1990.
 - [39] C. Thirunavukkarasy, T. Finin and J. Mayfield, "Secret Agents - A Security Architecture for the KQML Agent Communication Language", CIKM'95 Intelligent Information Agents Workshop, Baltimore, Dec. 1995.
 - [40] Tim Finin, "Agent-Communication Language plus example agent policies and architectures", <http://www.cs.umbc.edu/kqml/kqmlspec/spec.html>, 1996.
 - [41] J. Utans and J. Moody, Selecting Neural Network Architecture via the Prediction Risk: Application to Corporate Bond Rating Prediction", Proc. of the 1'st Int'l Conf. on A.I. Applications on Wall Street, pp. 35-41, 1991.
 - [42] Sankar Virdhagriswaran, "Mobile Unstructured Business Object (MuBot)[TM] Technology", <http://www.crystaliz.com/logicware/mubot.html>, 1996.
 - [43] Visa International, "Visa - Visa Cash", <http://www.visa.com/cgi-bin/vee/nt/cash/main.html?2+0>, 1997.
 - [44] "Conference Summary", <http://cism.bus.utexas.edu/ravi/ecom-flier>, International Conference on Electronic Commerce, Univ. of Texas Austin, Oct. 30-31, 1995.