データベースシステム 128－25
（２００２．７．１８）

電子商取引のための分割取引トランザクション

伊藤ちひろ　岩井原瑞穂　上林弥彦

京都大学大学院情報学研究科

インターネットの発展により、電子商取引の機会が増大している。電子商取引の特徴は、互いに会ったことのないような当事者間での金品の授受が行われることである。また、パーソナルコンピュータの高性能化やネットワーク技術の高度化に伴いサーバを経由せずに直接データ交換を行うPeer to Peer環境が普及しつつある。このような取引では、認証などの手段によってあらかじめ取引相手の身元が保証される訳ではない。従って、相手を完全に信頼した取引を行うことは困難となる。本稿では、取引相手に対する信頼に限度を設定し、その限度内で取引を分割することによって、起こりうる損害を一定限度に抑えるプロトコルを提案する。また、設定された限度による取引可能性についても論じる。

Installment Trade Transactions for Electronic Commerce

ITO Chihiro　Mizuho Iwaihara　Yahiko Kambayashi

Graduate School of Informatics, Kyoto University

The Internet technology encourages electronic commerce between people and/or organizations that are physically distributed in different location, which makes it difficult to trust each other. This paper proposes the degree of trust which limits the amount of money or goods that can be sent at one time according to the risk of the parties on trades. Then we discuss the feasibility of transactions within given credit and propose algorithms to judge the feasibility.

1　はじめに

インターネットの発展により、電子商取引の機会が増大している。電子商取引の特徴は、互いに会ったことのないような当事者間での金品の授受が行われることである。また、パーソナルコンピュータの高性能化やネットワーク技術の高度化に伴いサーバを経由せずに直接データ交換を行うPeer to Peer環境が普及しつつある。サーバ経由しないということは、認証などの手段によってあらかじめ取引相手の身元が保証されている訳ではない。このため、相手の信用性は大きな問題になる。

これまでの研究では、電子商取引を公正に行うためには信頼できる第三者機関(Trusted Third Party: TTP)を経由して商品と代金を交換するプロトコルや機構が提案されてきた[4][8][5][2]。

TTPを介した基本的な取引を図1に示す。客は金銭を、ベンダは品物をそれぞれTTPに託す。両方が預けられたことを確認した後、TTPは、金銭をベンダに、品物を客に渡すことで取引が完了する。

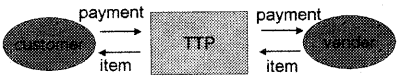

図 1: TTP を介した取引

これらの方法では、TTP は両方の取引主体から常に信用されていることを前提とし、正直であり事故も発生しない。しかし、インターネットのように様々な取引主体が多様な相手に対して行う取引にそのまま適用することは困難だと考えられる。

そこで本論文では、取引相手や仲介者に与える信頼に対し限度を設定することを提案する。取引相手や仲介者のリスクを考慮し、取引の各時点において一度に送付できる金品の最大額を規定する。この限度枠の範囲内で商品や代金を分割して送付することで、リスク分散を図る。

対象とする商品は、ある単位に分割してもそれぞれが商品として成立するような電子データである。例えば、ビデオ画像のようなデジタルコンテンツを分割配信する場合や、ソフトウェアのライセンスを使用毎 (pay-per-use) に、もしくは一定期間毎に更新する場合などに、本手法が利用できる。この場合、更新時にネットワークを経由して、サーバから新たなライセンスキーを発行してもらうことになる。

商品の発送は、仲介者やネットワークの負担を考え、暗号化したデータを購買者に送り、復号鍵を仲介者に送付する方法 [8] が適している。また、代金の支払いには Web banking 等より仲介者の銀行口座に振り込むことを想定している。

仲介者の選択は、手数料や信頼度などを判断材料に、動的に実施する。

本稿は以下のように構成される。第 2 節では、一般の電子商取引および本論文における用語『公正さ』と『リスク』について述べる。第 3 節では、本論文で用いる記法を定義する。第 4 節では、商品や代金を一定額以下にそれぞれ分割して交換することでリスク分散を図るプロトコルを提案し、設定された限度枠における取引可能性について議論する。関連研究については 5 節に挙げ、6 節では結論と今後の課題を述べる。

2 電子商取引における公正さとリスク

電子商取引に『公正な交換 (fair exchange)』は欠かせない。Franklin らは、公正な交換プロトコルとは、「二者間で秘密の交換を行う際、途中で処理を中断したり誤った行動をとったりした場合でも、どちらかの側が有利になることはない [2]」ようなプロトコルであるとしている。

また Gärtner らは、公正さの形式的定義を行った [3]。公正さにはレベルがあり、『強い公正さ』とは、不正が全く起こらないことが保証される。それに対し、『弱い公正さ』とは、取引の場では完全な公正が保証されなくとも、不利益を被った場合にそのことが証明でき、裁判所などの別の場所で公正な裁定を受けることが可能である状態を指す、というものである。

ただし強い公正さを保障する場合でも TTP が完全に公正であるという前提が必要であるという弱点があるとことを彼らも指摘しており [10]、紛争 (dispute) の事後処理、revoke、compensation などを含んださらに細かい fairness の分類を示している。本稿で実現されるのは、上でいう弱い公正さに該当する。取引を分割することによってリスク分散を図るが、

2.1 リスク

電子商取引においては、一般に商品と対価を同時に交換することは困難であるため、取引が中断されると参加者のいずれかが損害を被るような時点が存在する。

ある時点において取引参加者に発生し得る損害の量を**リスク**と呼ぶ。売り手と買い手が直接取引する場合、以下のようなリスクが考えられる。

- 商品を受け取ったのに対価を支払わない、または対価を支払ったのに商品が届かない
- 対価を支払ったが、届いた商品が契約とは異なる
- 期限が定められている場合、その期限内に商品が届かない、または期限内に支払いがなされない

これらは、取引参加者によって意図的に発生する場合と、ネットワークやサーバの事故によって発生する場合がある。

また、どれだけ信頼できる相手でも不慮の事故の可能性もある。信頼できる仲介者を利用することで、確かにリスクは軽減されるが以下のような場合が考えられる。

- 仲介者に金品を委託した状態で、仲介者が業務続行不可能になる
- 仲介者と取引相手の結託。こちらに金品が届くことなく取引相手には金品が届いてしまう

このように、参加者が多岐に渡る商取引においては危険性が大きいため、損失を一定限度に抑える機構が必要であると考える。

3 記法の定義

取引において、どれだけのリスクを許せるかということは取引相手の信頼度に依存する。また、取引参加者 A から B への信頼度と、B から A への信頼度は等しいとは限らない。そこで、リスクの限度枠を有向グラフの枝の重みとして表現することにする。

定義 1（リスク限度枠グラフ） M を仲介者の集合、S を売り手の集合、C を購買者の集合とする。

リスク限度額グラフ $G=(V,E)$ において、各枝 $(u,v)\in E$ が非負数の重みリスク限度額 $L(u,v)\geq 0$ を持つ。ここで、$V=M\cup S\cup C$ また $E=V\times V$ である。リスク限度額 $L(u,v)$ は、u が v に対して負えるリスクの最大額である。

$L(u,v)=0$ のとき、u から v の金品の移動は信用がないため行えないことを表わす。それぞれのリスク限度額は、信用機関等の情報や各参加者の判断などにより定められるものとする。

定義 2（分割） 分割 とは、関数 D によって商品 g が m 個の分割商品

$$D(g)=\langle g_1,g_2,...,g_m\rangle,$$

に写像されることである。ここで、g_i は分割して送付可能な商品の最小単位である。

商品 g の価格は、$P(g)$ と表す。なお一般に、分割後の商品価格の合計は分割前の商品価格よりも大きくなることが多い。この差額は分割手数料に相当するが、ここでは簡単のため考慮せず、両者は等しいと仮定する。

定義 3（取引操作） 各操作は、取引における最小単位である。

$u\rightarrow v:g$　参加者 u が商品 g を参加者 v に送付する

$u\rightarrow v:P(g)$　参加者 u が g の代金を参加者 v に送付する

各操作の実行は完了した時点で各参加者へ通知がなされ、次の操作が行われることとする。

定義 4（状態変数） 時刻 t に行われた操作直後の状態において、参加者 v が支払い不能になった場合に参加者 u に発生し得る損害の量をリスクとし、$r_t(u,v)$ と書く。また、u が v に対して支払わなければならない残高を債務額とし、$d_t(u,v)$ と書く。

このとき、各変数には

$$\begin{aligned} r_{t_i}(u,v) &= r_{t_{i-1}}(u,v)+p_{t_i} \\ r_{t_i}(v,u) &= r_{t_{i-1}}(v,u)-p_{t_i} \\ d_{t_i}(u,v) &= d_{t_{i-1}}(u,v)-p_{t_i} \\ d_{t_i}(v,u) &= d_{t_{i-1}}(v,u) \end{aligned} \qquad (1)$$

なる関係が成立する。ただし、p_t は u から v に送られた価値である。

定義 5（支払い可能額） また、参加者 u が時刻 t における操作の実行後に、v に送付可能である商品または対価の最大値を支払可能額と呼び、$a_t(u,v)$ と書く。ここで、

$$a_{t_i}(u,v) = L(u,v)-r_{t_i}(u,v) \qquad (2)$$

である。

これらの変数を用いて参加者の状態を記述する。操作の結果、ある参加者のリスクが負数になる時点が生じる。これは、その時点で取引が中断した場合、参加者に正当でない利益が生じる可能性があることを示している。

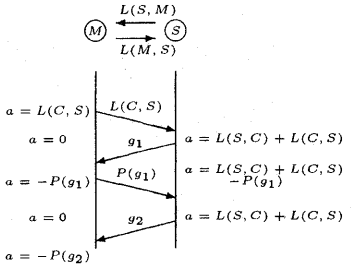

図 2: 直接取引の例

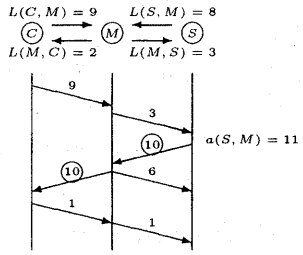

図 3: 仲介取引の例

取引開始前の時点 t_0 においては、リスクは 0 であり債務額は商品価格に等しい。一方取引が完了した時点 t_e においては、リスク及び債務額は 0 になる。従って、ある取引が可能であるということは、参加者の状態が

$r_{t_0}(u,v) = 0,\ d_{t_0}(u,v) = P(g)$ から $r_{t_e}(u,v) = 0,\ d_{t_e}(u,v) = 0$, へ至る取引系列 T が存在するということである。

4 交換プロトコルと実行可能性

4.1 直接取引

買い手 C が、売り手 S から商品 g を直接購入する場合を考える。仲介者は利用しない。商品 g は分割関数 f_p によって $\langle g_1, g_2, ..., g_m \rangle$. のように m 個の部分に分割可能である。

図 2 に取引の一例を示す。一般に、取引における最初の操作は、買い手 C が売り手 S に代金の一部を送付する方が、取引可能性は増大する。なぜならば、S が代金の一部 p_1 を受け取った分だけ S の支払い可能額 $a_1(S,C)$ が増加するからである。

送付する金額に限度枠を採用すると、まず C から S に $a_1(C,S) = L(C,S)$ が支払われる。S が C に g_1 を送ることができるのは、$P(g_1)$ が S の支払い可能額 $a_2(S,C)$ 以下であるときのみである。C が S に受け取った商品の対価を支払う度に、$a(S,C)$ は $L(C,S) + L(S,C)$ となる。したがって、以下のことがいえる。

買い手 C と売り手 S 間の直接取引では、取引可能となる必要十分条件は、分割された各商品の最大額を g_{max} として、$P(g_i) \leq L(C,S) + L(S,C)$ $(i = 1, 2, \cdots, m)$. である。

取引不能となった場合は、商品の分割を細かくする、あるいは、限度枠を大きくする交渉を行い、取引を可能にする作業を行うことが考えられる。

4.2 仲介者のある取引

ここでは、仲介者のある取引について考える。名前が知られており信頼度が高い仲介者を利用することで、リスク限度枠は大きく設定できる。仲介者は、買い手が支払い不能になった場合や商品提供者が商品送付不能になった場合、発生する損害を補填するものとする。仲介者が補填可能な最大額は、他の参加者に対し設定したリスク限度枠となる。仲介者にとってのリスクと債務額は、買い手と提供者に対してそれぞれ個別に設定することとする。例えば、買い手から代金を預かった場合に低減されるのは買い手に対するリスクであって、提供者に対するリスクではない。

まず、単一の仲介者を利用して商品の分割送付を行う場合について述べる。商品の送付方法は二通り考えられる。

1. 前に送付した商品についての決済が完了してから、次の商品を送付する
2. 前に送付した商品の決済の完了を待たずに、次の商品を送付する

2. の場合は、商品提供者にとって新たに送付できる商品の限度額は、前回の商品発送によって生じたリスクの分だけ 1. と比較して小さくなる。したがって、2. のもとで実行可能な取引は必ず 1. のもとでも可能であるので、取引可能性を考える上では 1. の場合のみを検証すればよいことになる。

売り手 S から購買者 C が 10 円の商品を一括購入する場合を考える。$L(C,S) = 1$、$L(S,C) = 3$ とする。この場合、$L(C,S) + L(S,C) = 4$ となり商品価格に満たないので、取引は不可能である。そこで仲介者 M を利用することを考える。$L(C,M)$ と $L(S,M)$ のいずれもが商品価格以上であれば、明らかに取引は可能である。ここでは、$L(C,M) = 9$ 円, $L(M,C) = 2$ 円, $L(S,M) = 8$ 円, $L(M,S) = 3$ 円とする。このような取引の様子を図 3 に示す。

仲介者 M を用いると、S は M から先払いされた代金 (の一部) を受け取ることにより、支払い可能額 $a(S,M)$ は

$$a(S,M) = min(L(C,M), L(M,S)) + L(S,M) = 11$$

となる。したがって、S は M に 10 円の商品を送付することが可能となる。また、M の C への支払い可能額 $a(M,C)$ は

$$a(M,C) = L(C,M) + L(M,C) = 11$$

であるため、S からの商品を受け取った M は、これを C へ送付可能である。商品を受け取った C は、残金 1 円を M に送付し、M は S に送付することで、取引は終了する。

このように、仲介者 M を利用した g の分割取引が可能となる条件は、$L(M,S)+L(S,M)$、$L(C,M)+L(S,M)$、$L(C,M)+L(M,C)$ のいずれもが $P(g_i)$ 以上であることである。ただし $i = 1,2,\cdots,m$ とする。

4.3 複数の仲介者を経由した取引

仲介者を利用する場合、取引相手が必ずしも自分と同じ仲介者を利用したいとは限らない。このようなとき、複数の仲介者を介する方法が考えられる。

4.3.1 限度額グラフがリスト構造の場合

まず、限度額グラフは、図 4 のように購買者 C から売り手 S までの双方向リスト構造を仮定する。仲介者が単数の場合と同様、一つの分割単位の取引が完了してから次の分割単位の取引を開始するものとする。C から S の間に、仲介者が $M_1, M_2, \cdots, M_n$ のように n だけ介在しているとする。

分割商品 g_1 についての交換は以下のように行われる。なお $\min(\ L(M_{j-1}, M_j\ ) \mid j = 1,2,\cdots,i)$ を $L^{min}(C,M_i)$ と記述している。

1. 時刻 t_1 に、最初の操作 $C \rightarrow M_1 : L(C,M_1)$ が行われる。時刻 $tn+1$ に S に届けられる金額は、C から S への経路上の各枝で設定されているリスク限度枠のうち、最小のものとなる。これを $L^{min}(C,S)$ とする

2. 時刻 t_{n+2} に S が M_n に発送できる商品の最大額は、$a_{t_{n+2}}(S,M_n) = L^{min}(C,S) + L(S,M_n)$ となる。同様に、S から発送された商品を受け取った M_n は M_{n-1} に商品を送るが、発送可能な商品の最大額は $a_{t_{n+3}}(M_n,M_{n-1}) = L^{min}(C,M_n) + L(S,M_n)$ となる。

3. C は時刻 t_{2n+1} に商品を受け取り、時刻 t_{2n+2} に C は M_1 に $a_{t_{2n+2}}(C,M_1) = P(g_1)$ を支払う

S から M_n へ商品を発送し、かつ M_i まで送付される条件は、C から M_i への経路上の各枝で設定されているリスク限度枠のうち、最小のもの $L^{min}(C,M_i)$ と $L(M_i,M_{i-1})$ との合計が発送したい商品の価格以上であることである。逆に、この合計が商品価格未満であるならば商品発送はできない。したがって、取引が可能となるのは、$P(g_{\max})$ を分割商品の最大額として、以下が満たされる場合である。

$$P(g_{\max}) \leq L^{min}(C,M_i) + L(M_i,M_{i-1}) \quad (i = 1,2,\cdots,n+1), \tag{3}$$

取引可能判定は、以下のアルゴリズムで行える。

Algorithm Find Trade 1 C を M_0、S を M_{n+1} とする。

1. $L^{min}(C,M_0)$ を無限大とする。
2. $i = 1$ から $n+1$ まで、*3-4* を繰り返す
3. $L^{min}(C,M_{i-1})$ と $L(M_{i-1},M_i)$ を比較し、小さい方を $L^{min}(C,M_i)$ に代入する

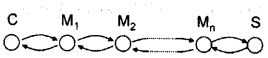

図 4: リスト構造の限度額グラフ

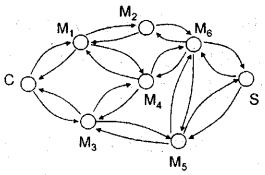

図 5: 一般の構造を持つ限度額グラフ

4. もし $L^{min}(C, M_i) + L(M_i, M_{i-1}) \geq P(g)$ ならば以下を実行する

   - $i = n$ ならば、取引可能
   - $i \neq n$ ならば、i に 1 を加え 2. を実行する

   もし $L^{min}(C, M_i) + L(M_i, M_{i-1}) < P(g)$ ならば、取引は実行不可能である。

このアルゴリズムの実行時間は、$O(n)$ となる。n は商取引の仲介者の数であることから、実用上問題ないと考えられる。

4.3.2 一般の構造を持つ限度額グラフの場合

次に、図 5 のような一般的な限度額グラフについて考える。リスト構造の場合とは異なり、代金の支払いと商品の送付では同じ経路や仲介者を経由するとは限らないが、ここでは送金と商品送付を同じ仲介者による逆順の経路で実施する場合を考える。この場合は、グラフが双方向リストのときとほぼ同様に考えることができる。つまり、取引が可能となる必要十分条件は、限度額グラフにおける C から S に至る各経路を双方向リストとみなしたとき、(3) 式が成立する経路が存在することである。

以下に、与えられた限度額グラフ G において、送付できる商品の最大額 $P_G^{\max}$ を求めるアルゴリズムを示す。

Algorithm Find Trade 2

1. 限度額グラフ $G = (V, E)$ において、$V^a = \{C\}$ とし、$L^{\min}(C, C)$、$P^{\max}(C)$ を無限大とする。

2. V^a に含まれないノードの中から v を選択する。ただし、S は最後に選択するとする。

   $V^a (i = 0, 1, \cdots, m)$ の各ノードについて、以下を計算する。

   $L^{\min}(C, v) = \max(\min(L^{\min}(C, v_i^a), L(v_i^a, v)))$

   $P^{\max}(v) = \min(P^{\max}(v_i^a), L^{\min}(C, v) + L(v, v_i^a))$

3. $P_v^{\max} > 0$ ならば、v を V^a に追加する。

4. $v \neq S$ ならば *(2)* に戻る。

5. $v = S$ ならば、$P_G^{\max} = P_S^{\max}$ である。

このアルゴリズムで得られた $P_G^{\max}$ が送付したい商品の最大額以上であれば、取引が可能である。また、このアルゴリズムは greedy algorithm の変形であり、実行時間は、ノード数を n とすれば $O(n^2)$ となる。

5 関連研究

電子商取引における信頼性について扱った研究では、仲介者を用いたプロトコルがいくつか提案されている。Ketchpel と Garcia-Molina らは電子商取引における信頼の問題について言及した [4]. Su や Manchala らは、図 1 に示したような基本的な取引において、品物が巨大な電子データであるような場合に発生する問題を指摘した [8]。彼らが指摘したのは、TTP やネットワークのコストの問題と商品の品質保障の問題であり、これらには暗号化技術を用いた対処方法を示した。これらの研究では、TTP は完全に信頼できるとしている。

Pagnia らは、モバイルエージェント同士の取引機構を提案している [6]。二つのモバイルエージェントが鍵のかかる一つの部屋に入り、交渉・取引を行うというものである。この基礎となるのは、信頼できる処理環境 (TPE) と呼ばれる改竄できないハードウェアデバイス [12] であるとしている。

これらのプロトコルでは TTP やそれに相当するものに無限の信頼を与えているため、事故のときの損害が莫大になる可能性がある。これに対し、本稿のアプローチでは損害を抑えることができる。

通常、交換を仲介する第三者機関は完全に信頼できるという仮定を置くが、一方、Franklin らは暗号技術を用いて、必ずしも信頼できるとは限らない第三者に仲介を依頼できるデータ交換プロトコルを提案した [2]。このプロトコルでは、取引を行う二者と

仲介者のうち任意の一人が裏切った場合、取引は不成立となるが誰も不利益を被らない。ただし、このうち二者が結託した場合には対処できない。

商品を分割して損害を抑えるという考え方は、Sandholm らが *gradual exchange* protocols[7] という形で提示している。この protocols では、ベンダと客との直接取引を前提としているので、商品の形態は、取引が途中で中断されても大きな損害にならない程度に分割できるものに限られる。本稿で提案する手法は、仲介者を利用することで、細分割が原因で発生する問題に対応する。信頼度が高い仲介者を利用すると、分割単位を大きくすることができ、またあるいは分割せずに取引できる商品が多くなる。

一つの TTP では、売り手と買い手双方が信用できる TTP が存在しなければならない。売り手と買い手を柔軟に結びつけて取引を行うには、共通の TTP が存在することは困難であり、複数の TTP を介在して動的に交換経路を定めることが必要である。TTP の動的ネットワークに関しては Manchala[5] らが議論を行っているが、ここでも TTP 間のリスク回避が必要である。商品や支払いを分割することで、リスクの分散が図れるだけではなく、複数の仲介者を経由したり、分割した商品をそれぞれ別々の仲介者に委託することで売り手と買い手のプライバシの保護も可能となる。

6 おわりに

本稿では、電子商取引において相手や仲介者に与える信頼に限度を設け、分割取引を行うことによりリスクの分散を図るプロトコルを提案した。信頼の限度枠をグラフ構造で表現し、分割された商品の価格との関係から取引可能性を判定するアルゴリズムについて述べた。仲介者を利用することで信頼の限度をより高く設定でき、また、複数の仲介者を利用することで多様な相手と様々な取引が可能となる。今後の課題として、商品の分割方法の検討や、さらに詳細なプロトコルの設計が挙げられる。トランザクションが中断した場合の回復方法や、責任の分担などを明確にしなければならない。また、リスク限度枠情報は、プライバシにかかわることであるため取引可能かどうか判断するプロトコルでは慎重に扱うべきである。

謝辞

本稿の執筆にあたり、有用な助言、議論をしていただきました上林研究室の皆様に感謝いたします。

参考文献

[1] N. Asokan, M. Schunter, and M. Waidner, "Optimistic Protocols for Fair Exchange", *Proc. 4th ACM Conf. on Computer and Communications Security*, pp. 6–17, Zürich, Switzerland, April 1997.

[2] M. K. Franklin, M. K. Reiter, "Fair Exchange with a Semi-Trusted Third Party", *Proc. 4th ACM Conf. on Computer and Communication Security*, April 1997.

[3] F. C. Gärtner, H. Pagnia, and H. Vogt, "Approaching a Formal Definition of Fairness in Electronic Commerce", *Proc. International Workshop on Electronic Commerce (WELCOM'99)*, pp. 354–359, Lausanne, Switzerland, Oct, 1999.

[4] S. P. Ketchpel, H. Garcia-Monia, "Making Trust Explicit in Distributed Commerce Transactions", *Proc. 16th ICDCS*, pp. 270–281, Hong Kong, May 1996.

[5] D. W Manchala, "Trust Metrics, Models and Protocols for Electronic Commerce Transactions" *Proc. 18th ICDCS*, pp. 312–321, Amsterdam, May 1998.

[6] H. Pagnia, H. Vogt, F. C. Gärtner, and U. G. Wilhelm, "Solving Fair Exchange with Mobile Agents", *Proc. 2nd ASA/MA*, pp. 57–72, 2000.

[7] T. W. Sandholm and V. R. Lesser, "Equilibrium analysis of the possibilities of unenforced exchange in multiagent systems", *Proc. 14th International Joint Conf. on Artificial Intelligence*, pp. 694–703, San Mateo, August 1995.

[8] J. Su, D. Manchala, "Building Trust for Distributed Commerce Transactions", *Proc. 17th ICDCS*, pp. 322–329, Baltimore, May 1997.

[9] J. Su, D. Manchala, "Trust Vs. Threats: Recovery and Survival in Electronic Commerce", *Proc. 19th ICDCS*, pp. 126–133, 1999.

[10] H. Vogt, H. Pagnia, and F. C. Gärtner "Modular Fair Exchange Protocols for Electronic Commerce", *Proc. 15th Annual Computer Security Applications Conf.*, pp. 3–11, Phoenix, December 1999.

[11] H. Vogt, H. Pagnia, and F. C. Gärtner, "Using Smart Cards for Fair Exchange", *Proc. International Workshop on Electronic Commerce (WELCOM 2001)*, pp. 101–113, Heidelberg, Germany, November 2001.

[12] U. G. Wilhelm, L. Buttyán, and S. Staamann, "On the Problem of Trust in Mobile Agent Systems", *Symp. on Network and Distributed System Security*, pp. 114–124, March 1998.