Virtual Card Payment Protocol and Risk Analysis Using Performance Scoring

Xu Xianhua
Lotus (IBM) Asia Pacific
750E, Chai Chee Industrial Park, Singapore, 460426
xian_hua_xu@lotus.com

Sung Sam Yuan, Ge Ling, Tan Chew Lim
Department of Computer Science
National University of Singapore Singapore119260
{ssung, geling, tancl}@comp.nus.edu.sg

Abstract

There are several payment protocols mediated by trusted third party functioning as bank (or credit card) agents. But these protocols do not integrate all parts of the protocol together. These agents only establish payment intention but not handle settlement. These protocols rely on traditional payment systems and logistics pathways to complete transactions, thus the efficiency is low. In addition, though the agents in these protocols took up some services of the traditional financial conglomerates, risk analysis of the agents is unintentionally neglected.

Here we developed an integrative and instantaneous payment protocol--virtual card payment protocol. Broker in our protocol is a bank agent, a financial conglomerate, a logistics assistant, a creditor to score participants' performance and an arbitrator to solve dispute between customers and merchants. In this protocol, one transaction is divided into 3 parts and different parts of the transaction apply different security level. Settlement can be instantaneously handled totally online, without direct involvement of traditional payment systems. Logistics is integrated to process through Internet. We define this technique "pay-on-delivery-online". Since inconsistency in transactions causes customer to complain, we introduce complaint-processing to build trust among involved participants. To dissipate risk concentration in Broker, we propose an algorithm to quantify participants' trustworthi-ness by estimating participants' transaction history with statistic analysis. Since it assumes that the participants' performance can only be evaluated by those that have established business with them, the model is more objective than poll online and is like the credit scoring or behavioral scoring in real world banking systems.

1 Introduction

With dramatic expansion of Internet, there is a great deal of significance in development of Ecommerce since it can extend the business beyond national borders quickly. Thus it is crucial for effective researchers to deal with the roles of participants involved in Ecommerce, like merchant, supplier, customer, partner, credit company, financial conglomerate, in global distribution. In addition, equality among participants, which is key in traditional business, should be ensured definitely. Every participant in Ecommerce should make profits but protect its interest.

Every transaction in Ecommerce is composed of three parts: data communication, logistics and payment Data communication is online procedure to establish business, including request confirmation and order verification. Logistics is to deliver products. Internet is a good pathway for digital products. To payment and settlement, a plethora of payment protocols have been brought about to solve this problem. The issues for every payment protocol are security, atomicity, integrity and non-repudiation. Most protocols apply mathematical encryption algorithms to protect the confidentiality of transactions. [10,11,12] Other payment protocols introduce the trusted third party to mediate the settlement so as to protect the customers' privacy. [13]

However, most existing payment protocols are very complicated, expensive and tedious. Those payment protocols applying cryptography are even more expensive and cumbersome. They handle settlement of transactions depending on traditional banking systems or credit card companies thus payment is always delayed. On the other hand, some payment protocols neglect problems in logistics and delivery. But some customers may refuse traditional delivery with slow speed. So the efficiency is counteracted by the delay of payment, and the speed of logistics. Those existing business models in fact combine slow traditional business modules with fast Internet, thus the overall efficiency is not satisfactory. Thereafter, it is necessary to bring about a competitive Internet payment protocol integrating three parts together.

Not only those existing protocols cannot process transactions instantaneously and the procedure is very complicated, but also they neglect the evaluation of the past performance for each participant to reduce risk and prevent abuse. No credit scoring systems are integrated into Internet payment systems. Those protocols cannot treat the participants fairly, especially customers. They require customers to pay for the loss in the abortion of transactions. Even if some can ensure certified delivery, they cannot offer any opportunity to complain if the goods are not satisfactory. Pay-on-delivery is the technique that the customer only pays after delivery is certified and can treat each equally[7]. Complaint processing and performance scoring system can offer an opportunity for customers to require second delivery or make comments on the goods from the merchants.

A promising Internet payment protocol should be simple, secure, fair, instantaneous and atomic, taking low

0-7695-0990-8/01/$10.00 (C) 2001 IEEE

risk, integrating payment with online delivery and ensuring message integrity and no-repudiation. Pay-on-delivery-online is a technique derived from pay-on-delivery to integrate transaction's three parts together. With pay-on-delivery-online, virtual bank can present anonymous, traceable, redeemable and atomic electronic money, or manage the stored-value accounts to transfer or handle settlement online, and evaluate each account's credit performance score. Such is virtual card payment protocol to be described in the next part.

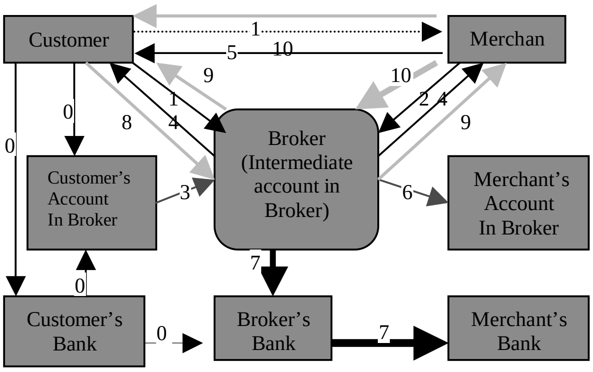
2 Virtual Card Payment Protocol

Virtual Card Payment Protocol is such a simple fair and instantaneous protocol that the trusted third party is a virtual financial conglomerate to apply the technique pay-on-delivery-online. This protocol can process transaction instantaneously with conventional parties: Broker(B), Merchant(M) and Customer(C), ensure anonymity and prevent tampering, eavesdropping and impersonation.

This protocol divides one transaction into three parts: public C2M, secure C2B and highly secure B2M. It uses temporal disposable single-use password (*Ecode*) created randomly by Broker specifying each transaction. Delivery is also performed through this third-partied Broker with temporal single-use key (*PickID*) for picking up. Even attackers deceive to order, *PickID* is merely sent to the customer's mailbox. Thus, here the high expense of key management in other payment protocols is avoided and replaced with the management of temporal *Ecode* and *PickID* at much lower cost. Risk in payment protocols concentrates in those abusers. Using statistics, we develop a method to compute the performance scores of each participant in our protocol. Each participant in transaction is evaluated and risk can be dissipated through comparing the each participant's performance score and selectively processing the payments requested by the customers with good historical performances. This protocol is promising for digital products since it integrates data communication, payment and logistics together and can process transaction real-time.

2.1 Transaction Procedure

There are 3 layers, namely users, Broker and bank' layer (see Figure 1), respectively to establish business, mediate online processing and complete settlement. There are four steps in one transaction: open an account in Broker, business establishment, *Ecode* verification and *PickID* delivery, and payment transfer from customer to merchant through the intermediate account. *Ecode* plays a key role as temporal "password" but used only once. Intermediate account is like a buffer to achieve money atomicity. It is assumed Broker can produce enough random temporal passwords and picking-up keys. Product delivery is completed by email and *PickID* can preserve product atomicity. Broker also can evaluate how trustworthy the participants are, to help make business decision. The customer need not provide any address to merchant in business establishment, and Broker only provides customer's reliability to merchant. Merchant doesn't know who is the customer but know how reliable the customer is. Thus our protocol supports anonymity but avoids establishing business blindly.



Customer
Merchan
1
5
10
9
10
1
4
2
4
0
8
0
9
Broker (Intermediate account in Broker)
Customer's Account In Broker
3
6
Merchant's Account In Broker
7
0
Customer's Bank
0
Broker's Bank
7
Merchant's Bank

Figure1 illustration of Transaction in Virtual Card Payment Protocol

M: merchant, C: customer, B: Broker

0. C: open an account in Broker and add cash to the account
1. C M: ordering goods
   C B: link to B's website from the M's order form, then login C's account in B and activate the random function in B to create *Ecode*. The customer can cut and paste the *Ecode* to the order form and complete the order request.
2. M B: ask for verification of *Ecode* and AccountID
3. B: Broker compares the *Ecode*, account ID, and business information. If not identical, transaction is abortive. If yes, Broker creates *PickID*, transfers the payment from the customer's account to the intermediate account.
4. B C: *PickID* by email, wait for repudiation from C. If no response, B assumes C accepts.
   B M: *PickID*, payment status
5. M: process the payment status. C download products by *PickID*
6. B: waiting for complaint from C. If no complaints, B transfers from intermediate account in Broker to merchant's in Broker.
7. B M: Broker's bank transfers to merchant's in batch

Complaint processing if goods is not delivered or satisfactory

8. C B: Request to deliver the product again with *PickID*
9. B: another *PickID* created, compute participants' reliability
   B M: the *PickID*; B C: the *PickID* by email
10. M: complaint processing (make *PickID* valid and tell Broker that the complaint has been processed)
   C: download the products.

2.2 Complaint Processing &Abuse Management

If transaction is valid, the customer's account has been debited though the merchant still has not received the pay. If products are not satisfactory, or if there are some problems in delivery, customers should have opportunity to complain and Broker deters the transfer from intermediate account to merchant. To punish the dishonest, it is necessary to evaluate the participants' trustworthiness. If a merchant always provides unsatisfactory products, it should be warned in the blacklist. Merchant can require Broker to make a decision whether the customer is to be trusted and selectively process the request from only those not always complaining. Thereafter, abuse includes customer and merchant abuse. A customer receiving the satisfactory goods still complains, so that the merchant has to process complaints all the time, which creates customer abuse. On the other hand, a merchant creates merchant abuse if he always receives different customers' complaints and/or not processing complaints for long. Following we introduce performance scoring by analyzing historical transaction records to evaluate each participants' trustworthiness in transactions.

2.3 Broker's Role

Broker's role is multiple in business establishment, payment, transaction processing and logistics. Customers communicate with merchants through Broker and merchants deliver goods by the aids of Broker. Electronic money in customers' accounts is of value and settlement can be handled totally online. Customers also complain through Broker if treated unfair. Broker's roles in virtual card payment protocol is like the following:

Trusted third party Customer's personal information is saved in Broker. Customers are assumed to authorize Broker to pay the goods if Broker receives valid request. Merchants assume Broker debits customers' accounts and will transfer the amount to their accounts after the goods are delivered. Merchants also believe that they can deposit the cash from Broker's Bank.

Virtual financial conglomerate The account in Broker stores valuable money and Broker can take up some financial services, such as transfer between accounts and payment. Broker is a virtual financial conglomerate bridging electronic money and physical money.

Logistics assistant This protocol acknowledges Internet is a convenient logistics for electronic products. Broker is an aid for goods logistics by offering unique *PickID* and certifying arrival. This unique *PickID* is sent to customer's mailbox. Customers can complain and require merchants to deliver the goods again if it is not satisfactory.

Performance scoring creditor we define a new term called *performance score* to evaluate the merchants' and customers' performance in transaction from his historical records. Broker can evaluate the performance scores of both sides on the basis of transactions and complaint processing in *table history*. If a transaction is completed successfully, both the merchant's and the customer's performance score should be increased. The merchant's performance score should be decreased if he is always providing unsatisfactory products and being complained.

2.4 Evaluation of Virtual Card Payment System

Tomi Poutanen[14] identifies several desirable properties of electronic payment protocols, including payment range, speed of vendor validation, dependence on customer specific hardware, ACID, double spending prevention[15], scalability, electronic transferability, multiple currency interoperability, transaction anonymity, and non-repudiation. The following figure (Table 1) illustrates the comparative analysis of several payment protocols. Our protocol achieves all properties in other protocols. This protocol is flexible in payment ranging from several cents to hundreds of dollars, and does not take up heavy computational load (fast vendor validation). It does not rely on specific hardware. Transaction's ACID properties are satisfied and our protocol allows the proof of what is delivered. Double spending is prevented to assure to minimize the cost of fraud, too. Our protocol is scalable and distributed, interoperable to support multiple currencies and the electronic currency is transferable between customers. It makes sure buyer's identity to be hidden in transaction and supports non-repudiation.

Property	Anonymous Offline	CyberCash	NetBill	DigiCash	SET	MiniPay	Agora	PayWord	SmartCard	Millicent	NetCents	First Virtual	Virtual Card
Large-Payment		✓	✓	✓	✓				✓	✓	✓		✓
Small Payment	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Micro payment	✓					✓	✓	✓	✓	✓	✓	✓	✓
Fast Vendor Validation	✓	✓		✓		✓		✓	✓	✓	✓	✓	✓
No Customer HW	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
Money Atomicity	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓
Goods Atomicity			✓								✓		✓
Certified Delivery			✓										✓
No double Spending		✓	✓	✓	✓				✓	✓	✓		✓
Scalable	✓				✓	✓		✓	✓	✓	✓	✓	✓
Distributed	✓					✓	✓	✓	✓	✓	✓	✓	✓
Divisible		✓	✓	✓	✓				✓	✓	✓	✓	✓
Transferable				✓					✓		✓	✓	✓
Interoperable					✓	✓					✓		✓
Partial anonymity	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Full anonymity	✓			✓					✓		✓	✓	✓
Non-reputation			✓				✓		✓		✓	✓	✓
Instantaneous													✓
Online Settlement													✓
Transaction Selectivity													✓

Table 1. Comparative analysis of payment protocols properties

Our protocol has some properties other protocols do not support. Unlike other protocols, the transaction is instantaneous to accomplish completely online, including settlement and delivery. Customers get nothing about history of merchants' transaction processing. Merchants don't know customers' attitude to transaction before. Here we intro-duce transaction selectivity, which means business is established and transactions are processed selectively. Before business establishment, customers can understand merchant's transaction history and merchants can privilege Broker to process transactions selectively based on customers' history. Transaction is anonymous but the customer and merchant do not establish the business or process the transaction blindly.

This protocol is also applicable and Broker's risk is low. Customers can conveniently add some money into their accounts in Broker through buying the single-use physical store-valued card Broker presents. Basically only after the customer has stored some money in her/his account in Broker, can she/he complete the payment when ordering goods online. Broker needn't take risks coming from the customer's refusal to pay the goods and the merchant's refusal to deliver the goods. Our protocol is competitive compared to other payment systems.

3 Performance Scoring in Our Protocol

In real banking systems, credit scoring is to determine whether credit to be given timely[1,2]. These models predict a customer's willingness to pay in a timely manner rather than his ability to pay. A credit scoring system awards points for each factor that helps predict who is most likely to repay a debt. A total number of points -- a credit score -- helps predict how creditworthy the customer is, that is, how likely that the customer will repay a loan and make the payments when due. A typical score ranges from 1 (highest risk) to 100 (lowest risk). [5]

In our protocol, Broker can monitor the processing of each transaction and each account in transaction. Broker should predict customers' reliability according to their billing history and merchants' trustworthiness based on their delivery history. Scoring system is developed to select all historical records specifying a certain customer or merchant, and analyze it statistically to identify characteristics related to credit worthiness. However, since the customers can open their accounts in Broker remotely and anonymously, it is impossible to trace each account owner's financial conditions in physical world timely. In addition, every customer may estimate different merchants of his own. It is necessary to quantify the reliability of each customer and each merchant. Since then, we develop a model for Broker to evaluate the customer and the merchant's trustworthiness based on their transaction history using statistical analysis.

We assume only those involved in the business can evaluate their business partners, so we can select only those transactions specifying the customers and the merchants. Broker can only trace the customer's transaction history and the merchant's process for complaints from the customers. Some attributes necessary for performance evaluation is displayed in *table history* (Table 2). Since the reliability is associated with transaction history, we define performance score to assess reliability.

HID	Ecode	Account	Merchant	Amount	Currency	Order_time	complaint_	complaint_time	process_time
H01	xcdb102d	user01	merchant01	100	usd	10/5/00	3	13/05/00	0
H02	exmc3212	user01	merchant02	200	usd	18/5/00	6	30/05/00	3
H03	mcde7890	user01	merchant02	300	usd	6/6/00	0	null	null
H04	gads3122	user02	merchant01	400	usd	9/6/00	1	12/06/00	0
H05	etwe4534	user02	merchant02	500	usd	5/5/00	7	29/05/00	3
H06	casd3412	user03	Merchant03	300	usd	5/6/00	5	10/06/00	3

Table 2, illustration of the view from transaction history

Performance score is to evaluate an account's reliability in third party by assessing the account's transaction history. If some complaints take place in one transaction, Broker should evaluate who is responsible for the complaints, so as to determine how much the trustworthiness of each participant in the transaction should be decreased. Customer's score is to determine whether the customer owning this account is serious about the transaction and whether he is intent to abuse the account. Merchant's score is helpful to predict whether the merchant is dependable and the service it provides is satisfactory or not. Each complaint will decrease the involved participants' performance scores. Following is how to determine *Performance score* and how *performance scoring* takes place. Since each complaint is to decrease the performance score of both the customer and the merchant, we compute decrement of performance score (also performance decrement) more conveniently. Suppose we define:

$X_{c,m,j}$: j^{th} transaction between customer c and merchant m

$S_{c,m,j}$: The decrement of performance score of customer c in the transaction $X_{c,m,j}$

$S_{m,c,j}$: The decrement of performance score of merchant m in the transaction $X_{c,m,j}$

T_j : Complaint times in a transaction $X_{c,m,j}$

f_j : Frequency of complaints for transaction $X_{c,m,j}$ =complaint_times /(complaint_time-order_time)

C_j : Contribution of all complaints in transaction $X_{c,m,j}$ to customer c's performance decrement

$C_{j,t}$: Contribution of No. t complaint in transaction $X_{c,m,j}$ to customer c's performance decrement

$C_j^{'}$: Contribution of all complaints in transaction $X_{c,m,j}$ to merchant m's performance decrement

$C_{j,t}^{'}$: Contribution of No. t complaint in transaction $X_{c,m,j}$ to merchant m's performance decrement

P_j : Cumulative process time for the merchant to process all complaints in transaction $X_{c,m,j}$

Process time is cumulative cost time for merchant to process all complaints. It is computed when every complaint is processed by adding the difference between Broker's machine time when a positive response from the merchant and the time when the complaint is received.

In any transaction $X_{c,m,j}$, we assume the decrement of performance score of a customer is contributed by complaint frequency and complaint times, and the performance decrement of a merchant is contributed by complaint times and process time. In $X_{c,m,j}$, the performance decrement is $s_{c,m,j} = \sigma_c f_j + \mu_c c_j$ -(1) while $\sigma_c + \mu_c = 1$ to customer c, $s_{m,c,j} = \mu_m c'_j + \sigma_m p_j$ -(2) while $\sigma_m + \mu_m = 1$ to merchant m. According to equality principle in business, the weigh of complaints should contribute the decrement of performance scores equally($\mu_c = \mu_m$). We can replace the above constraints with $\mu + \sigma = 1$. In a transaction $X_{c,m,j}$ with T_j complaints, we can obtain from definitions

$C'_j = \sum_{t=1}^{T_j} C'_{j,t}$ ----(3) $C_j = \sum_{t=1}^{T_j} C_{j,t}$ ---(4)

We get the constraint to each complaint t: $c_{j,t} + c'_{j,t} = 1$ since customer c and merchant m share the performance decrement by each complaint. Since $c_{j,t} + c'_{j,t} = 1$, we derive: $C_j + C'_j = \sum_1^{T_j} C_{j,t} + \sum_1^{T_j} C'_{j,t} = T_j$ -------(5)

We define without any complaints the performance is zero ($f_j = 0$ $p_j = 0$ and $c_j = 0$).

Since customers are more stochastic, we compute $C'_{j,t}$ more reasonably. Each complaint must be caused by merchant's abuse or not. If it is caused by merchant's abuse, the performance score of the merchant is decreased by 1 otherwise 0, which is described as: $C'_{j,t} = \begin{cases} 0 ----- not \\ 1 ----- abuse \end{cases}$. According to statistics, contribution of performance decrement $C'_{j,t}$ by each complaint should abide by Poisson distribution. Since C'_j is the cumulative performance decrement after T_j times of complaints ($C'_j = \sum_{t=1}^{T_j} C'_{j,t}$), each of which is in a Poisson process, ($C'_{j,t}, t$) abides by Gamma Distribution. [9] Suppose r (>1) is a positive number to be determined by merchants' greatest number of complaints to be allowed, and f_j is frequency of complaints in $X_{c,m,j}$, we can formulate as the following:

$C'_{j,t} = e^{-f_j t} \frac{(f_j t)^{r-1}}{(r-1)!} f_j$ --(6)

(density function)

$C'_j = \sum_{t=1}^{T_j} e^{-f_j t} \frac{(f_j t)^{r-1}}{(r-1)!} f_j$ --(7)

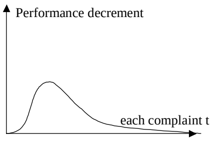


Figure 5 Each complaint contributes performance decrement

We can easily determine the maximum of $C'_{j,t}$:

When $t = \frac{r-1}{f_j}$, $\max(C'_{j,t}) = e^{-(r-1)} \frac{(r-1)^{r-1}}{(r-1)!} f_j$ - (8)

We define $T_t = \frac{r-1}{f_j}$ -(9), now we can clarify the relation between r and m's greatest tolerated number of complaints. When the greatest number of complaints is processed, merchants take up all responsibility. Clearly from (8)and (9), T_t is the greatest number of complaints in one transaction and if the merchant receives the $T_t + 1$ complaints in one transaction, merchants considers the customer is in abuse. To normalize the formula (6) and (7) by the maximum (8), we can derive:

$$C'_{j,t} = \frac{e^{-f_j t} \frac{(f_j t)^{r-1}}{(r-1)!} f_j}{e^{-(r-1)} \frac{(r-1)^{r-1}}{(r-1)!} f_j} = \frac{(f_j t)^{r-1} e^{-f_j t}}{e^{-(r-1)} (r-1)^{r-1}} \text{----(10)}$$

$$C'_j = \frac{\sum_{t=1}^{T_j} e^{-f_j t} \frac{(f_j t)^{r-1}}{(r-1)!} f_j}{e^{-(r-1)} \frac{(r-1)^{r-1}}{(r-1)!} f_j} = \frac{\sum_{t=1}^{T_j} (f_j t)^{r-1} e^{-f_j t}}{e^{-(r-1)} (r-1)^{r-1}} \text{--(11)}$$

According to formula (5) and (11),

$$C_j = T_j - C'_j = T_j - \frac{\sum_{t=1}^{T_j} (f_j t)^{r-1} e^{-f_j t}}{e^{-(r-1)} (r-1)^{r-1}} \text{-----------(12)}$$

To all transactions $X_{c,m,j}$ between merchant m and customer c, we can summarize the whole decrement of performance score. Thus the whole decrement of performance score in those transactions $X_{c,m,j}$ ($j = 1 ... j$) is:

$$S_{c,m} = \frac{\sum_j s_{c,m,j}}{\sum_j X_{c,m,j}} \text{------(13) for customer c,}$$

$$S_{m,c} = \frac{\sum_j s_{m,c,j}}{\sum_j X_{c,m,j}} \text{------(14) for merchant m.}$$

Since each merchant can establish transactions with different customers and *vice versa,* we should compute the decrement of the customer's performance score according to the business ratio of each merchant he

0-7695-0990-8/01/$10.00 (C) 2001 IEEE

establishes business with. We can conclude that this customer's overall decrement of the performance score is

$$S_c = \sum_m \left(\frac{\sum_j X_{c,m,j}}{\sum_{m,j} X_{c,m,j}} S_{c,m}\right) = \frac{\sum_m \sum_j S_{c,m,j}}{\sum_{m,j} X_{c,m,j}} \text{--------(15)}$$

for customer c

$$S_m = \sum_c \left(\frac{\sum_j X_{c,m,j}}{\sum_{c,j} X_{c,m,j}} S_{m,c}\right) = \frac{\sum_c \sum_j S_{m,c,j}}{\sum_{c,j} X_{c,m,j}} \text{------(16)}$$

for merchant m

According to the business premise that every new business participant is innocent and honest, we define the original performance score of each new participant is 0. Thus, the performance score of each participant after transactions with some complaints is illustrated as following:

$$P_c = 0 - S_c = -\frac{\sum_m \sum_j S_{c,m,j}}{\sum_{m,j} X_{c,m,j}} = -\frac{\sum_m \sum_j (\sigma f_j + \mu C_j)}{\sum_{m,j} X_{c,m,j}} \text{----(17)}$$

for any customer c

$$P_m = 0 - S_m = -\frac{\sum_c \sum_j S_{m,c,j}}{\sum_{c,j} X_{c,m,j}} = -\frac{\sum_c \sum_j (\sigma T_j + \mu C'_j)}{\sum_{c,j} X_{c,m,j}} \text{----(18)}$$

for any customer m

If there're N customers (labeled as $C_n, n = 1,2,...N$) and K merchants (labeled as M $M_k, k = 1,2,...K$) in *table history*, the performance scores of each customer and merchant are evaluated as $P_c(C_n, n = 1,2,....N)$ and $P_m(M_k, k = 1,2,...K)$. Thus we can queue those values to easily understand which one is more reliable. The process to implement the algorithm above mentioned is very simple. To implement the algorithm above, two queries can be processed to the *table history:*

```
SELECT HID, Ecode, account, merchant, order_time,
complaint_times, complaint_time, process_time FROM history
GROUPBY merchant where account=@userid
SELECT HID, Ecode, merchant, account, order_time,
complaint_times, complaint_time, process_time FROM history
GROUPBY account where merchant=@merchantID
```

For example, we can analyze the query results (5 records) from *table history* (table 2) with two customers (user01, user02) and two merchants (merchant01, merchant02) respectively. Assuming merchant01 can accept 2 times of complaints to one transaction and merchant02 can accept 4 times of complaints to one transaction, which is determined by merchants themselves, we can easily extract some data to compute the merchant's and the customer's performance score. Merchant01 processes complaints once every day and merchant02 processes complaints every other day. For each transaction, we can describe in table 3.

Transaction	T_t	f_j	$r = T_t \times f_j + 1$	$C'_{j,t}$
H01	2	1	3	$\frac{1}{4e^{-2}} t^2 e^{-t}$
H02	4	1/2	3	$\frac{1}{16} t^2 e^{\frac{4-t}{2}}$
H03	4	0	N/a	0
H04	2	1	3	$\frac{1}{4e^{-2}} t^2 e^{-t}$
H05	4	1/2	3	$\frac{1}{16} t^2 e^{\frac{4-t}{2}}$

Table 3 illustrations of some parameters for each transaction

Since $c_{j,t} + c'_{j,t} = 1$, we easily compute $c_{j,t}$ after we compute $C'_{j,t}$. Then C_j and C'_j is cumulated. For instance, we get cumulative from 7 complaints in merchant01-user01 transactions. Merchant01 should take responsibility for 3.5909 while user01 is responsible for 3.4091 complaints. Assuming μ=σ=1/2, which means the two factors' weighs in determining the performance score are equal, we can compute the results according to formula (1, 11-16). (See Table 4)

Customer/ Merchant	User01			User02			Merchant01		Merchant02		
HID	H01	H02	H03	H04	H05		H01	H04	H02	H03	H05
Transaction (User-merchant)	01-01	01-02	01-02	02-01	02-02		01-01	02-01	01-02	01-02	02-02
Complaint times	3	6	0	1	7		3	1	6	0	7
fj	1	1/2	0	1	1/2	*Pj*	0	0	3	0	3
Cj	0.508	1.33	0	0.336	1.654	*C'j*	2.491	0.663	4.662	0	5.345
Pc,j	0.790	0.918	0	0.668	1.077	*Pm,j*	1.246	0.332	3.831	0	4.172
Pc	-0.569			-0.827		*Pm*	-0.789		-2.668		

Table 4 illustration of the performance scoring of each participants involved in transactions

As you can concern in Table 4, in customer pool, since *Pc*(user01)>*Pc*(user02), user01 is more trustable than user02. In merchant pool, since *Pm*(merchant01)> *Pm*(merchant02), merchant01 is more dependable than merchant02. Since merchant02 processes complaints every other day, it receives more complaints and processes complaints more slowly, thus merchant02 is not as dependable as merchant01, which is compatible with our analysis result. However, though user01 complains more than user02, user01 is still more honest. This is because user01 completes 33 percent of transactions with merchant02 without any complaints.

This model to determine the customers' and merchants' trustworthiness is helpful for all participants before they establish business. It computes the customers' and merchant's dependability based on their transaction history. Broker also can easily to exclude those who abuses in virtual card payment protocol, so that the risk in Broker is reduced. Performance score is important in customers' control. On anonymous Internet business, the performance scoring system can contribute risk management promisingly.

4. Conclusions and contributions

Our protocol is simple, inexpensive, fair, convenient, secure, dependable, and recoverable. It uses cheap management of temporal *Ecode* and *PickID* to replace expensive management of cryptographic keys. It's atomic, authentic, anonymous and scalable. It can prevent eavesdropping, tampering, masquerading and replay effectively. The system is internationally compatible and globally reachable but has low impact on the existing business relationships[5]. Processing of transaction can be accomplished through traditional participants. The protocol divides transaction procedure into three parts on different security requirement, which can improve efficiency in transaction processing. This model facilitates Internet payment. Our contribution is listed in following:

Integrate the complete transaction online together

Almost all payment protocols care little about integration of the transaction's 3 parts: data communication, payment and logistics but focused on relationship between data communication and payment. Few of them, such as NetBill, though integrating payment and logistics together, do not handle settlement online since the accounts do not store value. Our protocol has virtualized and integrated all parts in transaction. The stored-value accounts can handle settlement online in no time.

Introduce complaint-processing to certify delivery

In First Virtual, [3] there is a premise that customers do not judge whether the products are satisfactory or not before they receive the goods. Delivery first cannot ensure product atomicity. NetBill [13] solves the problem using twice delivery of one purchase but customers have to take more confirmation steps to complete on transaction. In our protocol, delivery is ensured through complaint processing, so is product atomicity. Customers can complain the purchase quality and merchants cannot receive the money if the customer is not satisfied.

Broker takes up much more responsibility

Broker in our protocol takes up responsibility of an arbiter to solve disputes in transaction, like in NetCents[14] and Agora[7], of an agent to protect customers' privacy, like in NetBill [16] and GC Tech, and of a transferring buffer and a currency issuer to make money atomicity, like in First Virtual and NetCash[6]. Broker is also responsible to help logistics of the goods and commit customers' account management. Transaction is completed conveniently since Broker takes up most responsibility. Broker can evaluate every participant's trust in transaction and index every merchant and customer by analysis of historical records. Broker can classify participants with trustworthiness.

Build consumer trust and dissipate risk concentration

Risk management is key in financial conglomerates. [4,5,8] In our protocol, we assume that risk is concentrated in the dishonest users so that the performance scoring plays a key role to reduce risks. The performance scoring system provides a good tool to monitor each participant involved in the transactions, to spin off the users committing abuse and to help establish business selectively. The model qualifies the users' reliability to prevent the dishonest involved by employing customers' response of each transaction to evaluate participants' performance. Only the business partners can estimate the performance. Thus performance scoring is a good method to reduce Broker's risk and to protect participants' interest. Our model is more reliable than poll systems to a merchant and can be associated with other crediting systems to provide more objective performance scoring or credit scoring.

References:

[1].Andreas Crede et al Electronic Commerce and the Banking Industry http://jcmc.huji.ac.il/vol1/issue3/crede.html

[2].Bill Power, E commerce growth requires attention to risk management, Houston Business Journal May 2000

[3].Darren New, Internet information commerce the first virtual approach Proceedings of the 1st USENIX workshop on Electronic Commerce NY 1995

[4].Donna L Hoffman et al Building Consumer Trust in online environments The case for Information privacy http://www2000.ogsm.vanderbilt.edu/papers.html

[5].FSTC projects, BIPS: leading the way to electronic commerce http://www.fstc.org/projects/bips/index.html

[6].Gennady Medvinsky NetCash: A design for practical electronic currency on the Internet ACM 1993

[7].Jan Camenisch et al An efficient Fair Payment System CCS96 New Delhi, India

[8].Jiang Xiaozhong et al Online Financial Risk Management http://web.singnet.com.sg/~limhkiat/online.htm

[9].Jim Pitman Probability Springer Verlag 1993 286-287

[10].Lam Kwok Yan, Cryptographic techniques and Data Security 1998 National University of Singapore

[11].Larry Loeb, SET:introduction and technical reference, Artech House, 1998

[12].Sherif M.H. et al SET and SSL: Electronic payments on the Internet 1998 IEEE

[13].Sirbu M., J.D.Tygar. NetBill: An Internet Commerce system Optimized for Network Delivered services. IEEE Personal Communications, 2(4), pp. 34-39, August 1995

[14].Tomi Poutanen NetCents: a lightweight protocol for Secure micropayments Proceedings of the 3rd USENIX workshop on Electronic Commerce 1998 Boston

[15].Tygar JD, Atomicity in electronic commerce Proceedings of the 15th Annual ACM Symposium on Principles of Distributed Computing

[16]. Yasushi Kawakura et al Flexible and scalable credential structures: NetBill Implementation and experience