

Secure Mobile Agent Mediated System for Online Mutual Fund Trading

Tieyan Li & Yan Jiang Yang
Information Security Group,
Ubiquitous Computing Program,
Lab. Of Information Technology,
Singapore 119613
litieyan, yanjiang@lit.org.sg

Abstract:

The trend of Do-It-Yourself (DIY) personal financing is fueled by the Internet. Toward mutual fund industry, it offers small or individual investors chances to share professional finance management provided by mutual fund companies. In this paper, we propose a novel secure mobile agent based mutual fund trading system (based on our former system [9]), which can provide complete Internet-based and inexpensive services to DIY investors such as expertise funds selection tools and online investing. The new features include a p2p interactive model and mobile agent assistant payment scheme. Security mechanisms are emphasized in our system design for the wide acceptance of such electronic commerce system. A transaction protocol, Mobile Secure Mutual Fund Transaction (M-SMFT), is described in detail and issues of security and performance are analyzed.

1. Introduction

E-Commerce has been initiating an upheaval in business world for its potential of lower costs, lower business cycle time, faster customer response and improved service quality. As more and more products and services are traded on the Internet, the needs for better and customized online trading systems are increasing. Software agent technology seems able to propose attractive solutions for E-commerce. The introduction of Personal finance software agent is helping individual investors a lot in diversification and management of their financial assets while the Internet motivate the concept of instant transaction through the Internet.

The mutual fund industry has exploded to more than 12,000 in number, holding a total asset of 6 trillion

US dollars. Many mutual funds companies have reacted to the challenges from E-Commerce. They set up web sites, put account services online, and allow partially online accomplishment of transactions. Fidelity [1], an individual investor oriented mutual fund family, has built a mutual fund "supermarket" that consists of over 4,100 mutual funds, where investors can access their accounts and search for information about stocks, funds and policies. For transactions such as investing on funds, dividend and capital gains distributions, automatic investing every month or quarter and redemption, Fidelity provides online accomplishment through Electronic Funds Transfer (EFT). It is an expensive legacy fund transfer system based on financial Electronic Data Interchange (EDI), which has been proved by the business practices that cannot meet the requirements of lower cost, flexibility and adaptability for enterprises conducting e-commerce. Other big mutual funds families such as Vanguard [2], Charles Schwab [3], provide similar services for cyberspace investors.

Nevertheless, we feel a need to go beyond information retrieval to more active investor counseling to aid their personal finance planning. Also the stumble transaction process can be substituted with an Internet based, streamlined, secure and cheaper online accomplishment. Thus, we built a secure mutual fund system in an Internet Banking and Payment environment [9]. We discover some new features such as p2p interactive model (i.e. [5]) and mobile agent payment scheme (i.e. [13]). The new system can take much more benefit to the online investors than before.

This paper presents a new mutual funds market system that assists DIY investors to select and to manage their portfolio with intelligent agents and expert systems. We also design a secure online transaction protocol that imports an online banking (e-banking) agent, Internet Banking and Payment (IBP) to coordinate mutual companies and banks to provide investors a completely Internet-based solution. In the

next section, we propose our framework and address the design issues. Section 3 depicts the whole procedure and typical transactions (M-SMFT) in details. Section 4 highlights the security and performance issues. Section 5 discusses some of the improvements of the system. In the closing section 6, we summarize our conclusions and thoughts about future works.

2. System Design

We introduce the various functions of the system in this section. We also describe the system architecture as well as new techniques used here.

2.1 Participants

There are three main participants in our system: the investor (I), the mutual fund company (MFC) and the Internet Banking and Payment (IBP). Their functions are described in the following (refer to figure 1):

[1] **The Investor:** the investor is a person that invests money on one or more mutual funds provided by MFCs. All tasks to accomplish her investment is:

- Having a registered account in an IBP that already keeps a balance.
- Selecting interactively the p2p/web sites of MFCs and IBPs for browsing, consulting, managing or negotiating.
- Giving orders of investment, redemption and exchange of mutual funds using secure mobile agents.
- Checking accounts' status, transaction history and portfolio if necessary.

[2] **The Mutual Fund Company (MFC):** MFC is the company that creates and manages the mutual funds. Its p2p/web site acts as the interface and front-end to streamline the investor's online investing experience. We also carefully design its business service architecture at the back end to provide secure online transaction as well as assistance for better decision and management of their mutual fund assets. MFC should provide the following services:

- Assist investors to select suitable mutual funds according to their preference, constraints, and the economic climate. Online chat and instant messaging via p2p are supported to make it more interactive.
- New investors set up mutual fund accounts and invest on mutual funds at the current price or "net asset value".
- The investor redeems her fund shares at the current price or "net asset value". The money

can be transferred to her account on IBP or directly to the real bank.

- The company distributes the dividend and capital gains in the way the investor defines, transferring to her bank account or re-invest.
- Allow investors to invest automatically every month or quarter. e.g., every month \$50 will be automatically transferred from the investor's IBP or bank account to the mutual fund account.
- Investors can retrieve (using mobile agent) necessary information about mutual funds through MFC, such as portfolio, performance and policies.

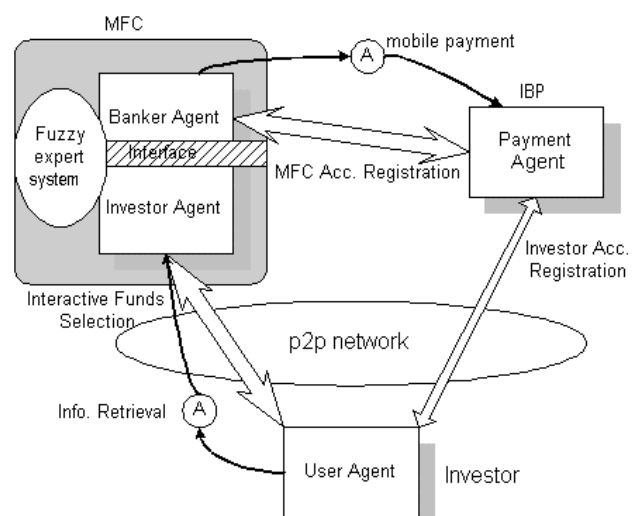


Figure 1. System architecture

[3] **The Internet Banking and Payment (IBP):** IBP is an open electronic payment system that settles mutual fund transactions via fund transfer between accounts of the investor and the MFC. It can act as a virtual bank or be associated with real banks on the base of a set of open data transmission standards and security protocols. We avoid much involvement of the real bank in the transactions by using IBP. The services it provides are:

- The investor and the MFC open accounts online in IBPs.
- The investor and the MFC deposit money on IBP. Or verse visa, both can withdraw money from IBPs.
- The IBP provides a gamut of services for online transaction including transaction authorization and payment capture. All the transactions between the MFC and the investor such as redemption, dividend and capital gains distributions, automatic investing can be accomplished in IBP transparently to both MFC and the investor.

- IBP keeps log files of the investor's transactions for future non-repudiation query and send batch files or report of transaction records daily.

2.2 Agents and p2p network

Our system architecture is show in Figure 1 above. In that figure, we also have a mobile agent mediated information retrieval process and payment process. An additional p2p interactive model is also included in the mutual fund selection part.

[User agent (UA)]: UA is the intelligent interface between the investor and the system, which can provide the services described above friendly to the investor.

[Investor agent (IA)]: IA is one part of MFC, it will process the requests and provide the services to the investor. It also has an interface with the Banker Agent.

[Banker agent (BA)]: BA is another part of MFC, it will mainly deal with payment issues, such as account balance check, purchase of mutual fund.

[Payment agent (PA)]: PA is a functional entity in IBP to process the payment request in a transaction.

[Mobile agents (MA)]: Mobile agent can be launched by UA and BA separately for performing the relevant tasks such as information retrieval, payment etc...

[P2P network (P2P)]: P2P is now integrated with UA and IA for direct cooperation via instant chatting or messaging. We are still investigating the p2p platforms such as [5] and [14].

Note: The IBP is a distributed system that may be distributed around the world. Each IBP is localized and customized to local customers and local banks. One IBP is associated with one or more banks, so is the bank. Every IBP has complete information about any other IBP so that a global communication and transaction system is set up. The scenario that the investor invests on any mutual fund she wants anywhere, anytime can be realized. The future p2p network can also be implemented for searching suitable MFCs or IBPs.

3. The whole procedure

We have defined the functional parts in the system. Thereafter, we introduce the procedure of completing a single transaction in this section. The procedures

consist of registration, selection, ordering and purchasing (see the following subsections).

3.1 Registration procedure

The sequence of events must begin with the following registration stages:

Investor account registration: the investor firstly obtains an account from IBP. After suitable verification of identity, the investor receives a X.509v3 digital certificate, which is signed by CA. The investor's key pair for key exchange is optional.

MFC account registration: the MFC must owns two certificates for two key pairs: one for signing message and one for key exchange. The MFC also needs a copy of CA's public key certificate.

Note that here we have ignored the procedure of investor's choosing a proper MFC and IBP, also MFC's choosing a proper IBP. In practical, the investor must choose the beneficial one. For example, an investor can evaluate the reputation of a MFC from her knowledge both coming from p2p groups (i.e. other members' opinions) or MFC's web site. A direct interaction with the certain MFC via p2p can also help her judge the company. A mobile agent can hereby launched for assistantly searching more useful information (we need to embed the retrieval logic into the agent). Therefore, the registration can be started upon making her selection.

3.2 Mutual fund selection procedure

The objective of mutual fund selection process is to select economically rational mutual funds from a large universe of funds. The investor will first define their own preferences or constraints, based on which, the investor agent will autonomously determine suitable funds with the help of the fuzzy expert system [6, 7]. The selection process can be an autonomous procedure described as a sequence of three steps, in which the user agent and the investor agent stand for the investor and the MFC respectively.

Step 1: Identification and analysis of the investor's goals, needs, and constraints;

The first step is to build the investor's profile, and to try to find the investor's investment objectives. An individual investor will first fill in the questionnaire provided by the MFC, in which he will answer the questions about age, experiences, forecasting ability, risk tolerance, etc. Based on this information, the expert system can make fuzzy terms

such as age, risk and so on. Then it will define fuzzy sets and related fuzzy rules to build the investor's profile. This step deploys part of the fuzzy system, as well as part of the functions provided by the investor agent. Again, IA can embed the selection logic into a mobile agent and launch it for completing this task.

Step 2: analysis of all the available mutual funds;

Similarly, the banker agent deploys another part of the fuzzy system to analyze the funds based on their underlying investment objectives, risk profiles, fund manager's reputation, expensive rate and so on. Finally it can also define those funds' fuzzy sets and fuzzy rules to establish the funds' profiles.

Step 3: selection of appropriate mutual funds.

This step is to find a match between the investor's profile and the funds profiles. The match actually decides the appropriate funds for the particular investor.

The investor will then determine if some or all funds are selected. She may also do this manually. This negotiation procedure may loop for several rounds. At last, for example, the investor selects several funds and wants to buy them. She then follows the purchase and payment procedure described next.

3.3 Purchase and payment procedure

We design our transaction procedure based on SET protocol [4, 8]. SET protocol is developed by VISA and MasterCard to secure payment card transaction over open networks. It provides important properties like authentication of participants, non-repudiation, data integrity and confidentiality. These features effectively guarantee the security during payment procedure. As SET has defined a variety of transaction protocols that using cryptographic technologies to conduct electronic commerce securely, we have built secure mutual fund transaction (SMFT) [9] procedure according to SET which also

1. provides secure communication channel among all parties involved in a transaction.
2. provides trust by the use of X.509v3 digital certificates.
3. ensures that the information is only available to parties in a transaction when and where necessary.

Different from the three participants in SET, the Cardholder, Merchant and Issuer, in SMFT, the three main participants are: the investor (I), the MFC (M)

and the IBP (B), as well as the certificate authority (CA) that is trusted to issue X.509v3 public-key certificate for the participants. We also define a mobile agent assistant mobile payment scheme as the new feature, and name the Mobile agent mediated Secure Mutual Fund Transaction protocol (M-SMFT).

Usually, the IBP acts as a financial institution with which the MFC and the investor establish their accounts for processing payment online. Each of these characters may possess two kinds of key certificates, one for key-exchange, which is used for encryption and decryption operations, and the other for creation and verification of digital signatures.

Some definitions we used are described below:

- ENC_k[M]: Encrypt message M with key k.
- K_{Ri}: IA's private key.
- K_{Ran}: Random symmetric key generated by IA.
- K_{Ub}: IBP's public key.
- H: Hash function (i.e. SHA-1).
- ||: Concatenation.
- DS: Dual Signature.
DS=ENC_{K_{Ri}}[H(H(PI)||H(OI))]
- PI: Confirmed Payment Information.
- OI: Selected funds (Order Information).
- Cert(X): X's certificate authorized by CA.
- ID: Transaction IDentification.

The outline of the transaction is described as follows: (also illustrated in figure 2)

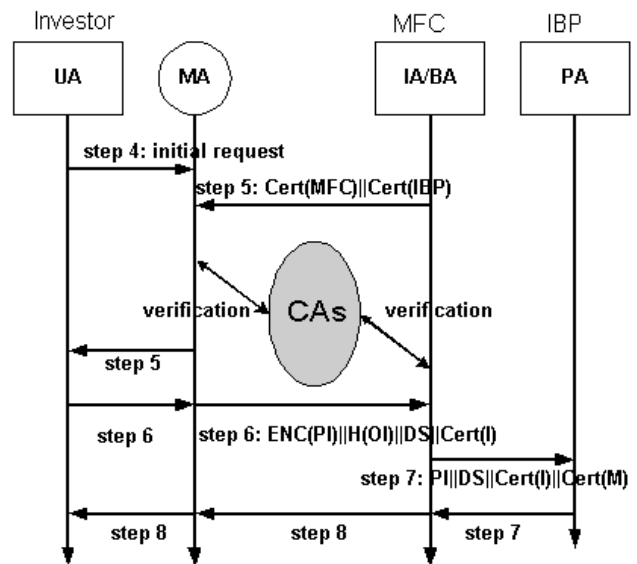


Figure 2: Transaction Procedure

Step 4: UA (on behalf of the investor) submits its funds selection form to MA generated at the same time, in which the selected mutual funds will be

described in detail. The funds selection form will be later used as mutual fund order information (OI). MA then launched and resided at IA of the MFC for performing the payment task.

Step 5: IA that receives OI from MA will simply transfer this message to BA, which will then check the investor's account balance. If there is enough money to be balanced, no money transfer from the IBP is needed. The confirmation message will be sent back to MA to inform the investor and process the investor's portfolio management based on the request. Otherwise, the banker agent will assign a unique transaction identifier to the message and then pass its own signature certificate $Cert(M)$ and the IBP's key-exchange certificate $Cert(IBP)$ along with the transaction ID to MA. (Here we suppose that the investor and the MFC have registered their account at the same IBP.)

MA verifies MFC and IBP's certificates by tracing through the certificate authorities (CAs). It then holds them to be used later during purchasing process. UA continues to create the approved selection form together with its payment info. (PI).

Step 6: UA dually signs on the two parts of the message (OI and PI) to generate DS. One part (OI) is the selected mutual funds. The other part (PI) is the payment information. It then generates a random symmetric encryption key (K_{ran}) and uses it to encrypt the dual signed payment information. Next, the UA encrypts the PI as well as K_{ran} into a digital envelope using K_{Ub} . Finally, the UA transmits the whole message to MA together with its certificate $Cert(I)$. MA launched again to IA/BA at the MFC.

Step 7: BA verifies the investor's certificate and the dual signature on the first part and then forwards the digital envelope to the IBP for authorization. If the authorization response from IBP indicates that the transaction is approved, BA pursues the service stated in the request form and at the same time generates and sends the purchase complete message back to MA.

Step 8: when UA retracts MA and receives the response message from MFC, it verifies the MFC's signature certificate by traversing the trust CAs. It also uses the MFC's public key to check the MFC's digital signature. If everything is correct, it takes on those actions indicated in the response message.

In M-SMFT procedure, most payment processes are done by MA. UA does not need to be online all the time as described in SET protocol. Instead, it only accesses the Internet in case of launching or retracting

MA. This new feature is especially useful if UA is pursuing multiple processes simultaneously.

But while MA reduces UA's load, there must be proved security in the whole transaction. Following on, we discuss the security issues.

4. Analysis and evaluation

The purpose of our research is trying to implement a practical and secure payment framework for mutual fund online transaction. So security and performance issues are our focus. In this section, we will discuss the advantages of the proposed framework for these two aspects and point out the potential problems.

4.1 Security issues

Our proposed payment scheme is based on the SET protocol and takes the same security mechanisms as SET. Thus M-SMFT also provides a secure and efficient procedure to pursue the mutual fund transaction. All the confidential actions such as signing, authentication, key generation and encryption are performed in the investor's computer (In SET, it is the cardholder who performs these operations). In the transaction procedure, the sensitive messages are encrypted with the secret key. Only the entities who hold the public key can decrypt it and read the messages. The transaction will finally be securely completed in IBP.

Note that in [10], MA has to compose OI, PI and generate random symmetric key while residing at the Merchant server. This is a very dangerous operation since there is no highly secure way to protect MA from malicious hosts [11]. Although there are approaches such as [12] of computing certain simple functions with the method of Hiding Encrypted Functions (HEF); [13] of building a secure mobile agent that can produce digital signature, no clear evidence shows that key material can be generated securely at remote server. Therefore, we put the key generation part in step 6 on UA, not on MA to provide secure transaction.

4.2 Performance

The main obstacle to an efficient mutual fund system is the complexity of payment during the whole procedure. It delays the responses from the investors, and thus brings the true compromise to this kind of business. How to make it more concise to pay becomes the crux of adapting M-SMFT to the real environment. The payment system in the real world is still a real bank based with off-line scheme.

In the mutual fund selection procedure of our system, when the user selects the mutual funds, she can trigger the auto-selection process and in most cases, with the help of MA and the fuzzy expert system used here. The user will lose no time on searching, while still can get the reasonable choices. It will not only save the time of both investors and consultants, but also make the choices more suitable to the investor.

In the transaction procedure, the investor will only pay from her online checking account, which is the account in the virtual bank (IBP) together with the certification from CA. Whenever there exists a real deal, it only needs to transfer the account info. From the MFC's point of view, it may not even involve deeply into the details of the transaction procedure. It will save the investor's time, as well as the MFC's time. The IBPs will also benefit from this procedure since they all registered on the IBPs, hence reduce the workload for fund transferring between IBPs and real banks.

5. Miscellaneous

Beyond meeting the fundamental security and performance requirements, the system shall also have the following potential improvements.

Scalability: The proposed system can also be scaled to an international environment. Let us imagine such a scenario: in the near future where we can have an online network purchase and payment system around the world. There are many IBPs running at different levels, and different MFCs and investors from all over the world. The investors in one country can search for the MFCs from another country, and pay for her investment from an IBP from the third country, in which she has registered. Compared with the traditional system, the larger the application scenario, the more efficient the transaction.

Practicability: The whole system we describe here is a mutual fund system in the IBP environment. In fact, with the IBPs as the international financial service in the near future, we can also implement other transaction systems by referring to our online payment scheme. The transparent p2p network we described here is independent both of the lower layer network protocols and the upper layer transaction protocols.

Mobility: More and more mobile users are taking the convenience of mobile network. For example, the WAP users can enjoy great benefits from this system. Only with the mini-browser on her hand-phone, the

investor can browse the investment information easily. Because the message exchanged online in this system is limited, with only a few clicks, the investor can finish the transaction assisted by MA in several minutes anywhere anytime via air.

Applicability: In this paper, we proposed a transaction scheme based on SET. It is fully compatible to the original SET. From the investor's point of view, she needs not to make any modification to her SET related software except embedding an agent that executes the investment functions. She may complete the whole transaction in a few steps without knowing the transaction details. This feature enables investors to provide uniform payment method to both online purchase and online investment on mutual funds with only one electronic IBP account, which improves the applicability of the proposed system.

6. Summary and Future Work

In this paper, we have presented a secure mobile agent mediated framework for online mutual fund trading. In which three main participants are the investor, the MFC, and the IBP. Among them are the novel features like p2p assistant interactive model and mobile agent embedded payment scheme. We analyze the procedures about the mutual fund selection and propose our M-SMFT. This system is actually a specific application based on the Internet banking system. Finally, we analyze the security and performance issues of the system, as well as some related improvements of it. For empirical evaluation, we eventually would like to implement these additional features on our demo system (Java 2, XML programming) to outside participants over the Internet. Our work raises several interesting problems for future research:

1. *P2P environment*, we are considering the p2p platform JXTA [14] to be used in our system. We are also designing JXTA peers with mobile agent functions. All of them are Java based.
2. *Mobile agent security* must be considered first and carefully before we use them. As to implementation, how to establish a *large scale secure mobile agent architecture* over Internet, especially a dynamic and intelligent one, where our system can be based on still needs to be solved.
3. *Inter-IBP fund transfer protocol*, as well as message exchange protocol must be defined

before the provided system can be used under international environment.

14. Sun microsystem, ``JXTA v1.0 Protocol Specification", June 27, 2001.

Reference:

1. <http://www.fidelity.com>
2. <http://www.vanguard.com>
3. <http://www.morningstar.com>
4. <http://www.setco.org>
5. <http://www.groove.net>
6. Talluru, L. R., "A Fuzzy System for Mutual Fund Selection." IEEE international Conference on Systems, Man, and Cybernetics, 1997.
7. Krishna,V., Ramesh,V., "Portfolio Management Using Cyberagents." IEEE international Conference on Systems, Man, and Cybernetics, 1998.
8. VISA INTERNATIONAL, and MASTERCARD INTERNATIONAL. "Secure Electronic Transaction (SET) Specification." Version 1.0, May 1997.
9. Tieyan Li, Ling Ge. "A secure agent based mutual fund system", International ICSC Symposium on Multi-Agents and Mobile Agents in Virtual Organizations and E-Commerce (MAMA'2000) December 11-13, 2000, Wollongong, Australia.
10. Artur Romao and Miguel Mira da Silva. "An Agent-Based Secure Internet Payment System for Mobile Computing", Trends in Distributed Systems'98. Electronic Commerce, Hamberg, German, LNCS, June 3-5, 1998.
11. G.Vigna (Ed.). Mobile Agents and Security. Springer Verlag, LNCS 1419, 1998.
12. Sander,Tomas; Tschudin,Christian: On Software Protection via Function Hiding. Submitted to the 2nd International Workshop on Information Hiding, Dec 1998.
<http://www.icsi.berkeley.edu/~sander/publications/hiding.ps>
13. P. Kotzanikolaou et. al, "Secure Transactions with Mobile Agents in Hostile Environments", LNCS1841, proceeding of 5th Australasian Conference, ACISP 2000, Brisbane, Australia, July 2000.