

E-Commerce with Secure Mobile Trade Agent

Sattar J Aboud

Amman Arab University for Graduate Studies, Amman – Jordan

E-mail: sattar_aboud@yahoo.com

Ghassan Farid Issa

Applied Science University, Amman – Jordan

E-mail: issa@asu.edu.jo

ABSTRACT

E-commerce on the Internet has the ability to produce millions of trades at the same time the number of merchants supplying commodities on the Internet is considerable, but it is difficult for individuals to tour every site on the Internet and choose where it is best to trades. In this paper we introduce Mobile Trade Agent (MTA) that rove a network, gather and examine the information from merchant servers on the Internet and make decisions to trade commodities on behalf of users. The unifications of public key encryption scheme and Distributed Object Technology (DOT) makes the MTA secure. We prove that (DOT) is an allowing technology for MTA.

Key words: e-commerce, mobile trade agent (MTA), public key encryption, distributed objects technology (DOT).

1. Introduction

The undertaking of high bandwidth at very low price has digested types of a data highway that turns into the world biggest shopping mall [1]. The quantity of data that is accessible on the Internet is so large that becomes difficult for individuals to see every site on the Internet [2], study the information and create reliable commerce decisions to buy and sell of commodities. Users require agent who can rove every site on the Internet and buy or sell on their behalf [3, 4, 5].

In this paper we introduce MTA that have the capability to rove each site on the Internet, gather related information and employ this information to take perfect decisions to trades on a behalf of its user. Also we illustrate the uses of an Authorization Server (AS) that permit trading and give payment for commodities purchased with MTA. Also the MTA should visit various

other merchant servers and run at these servers. Once it runs at an exotic server it is at risk to be attacked from these servers [6, 7]. So we illustrate that MTA executed as distributed objects, can rationally tour various servers, but actually stays protected at the secure borders of an Agent Depository (AD). The MTA is additionally protected by encrypting all messages between agents and other individual on the Internet by public key encryption scheme.

The remaining of the paper is as follows. In section 2 we introduce MTA that rove the sites on the Internet, gather and examine the data from merchants and make sound decisions to trade goods on behalf of users. The proposed MAT approach is described in section 3. Section 4 depicts the security matters in the program for instance secure messages and authentication. The applications of MTA are shown in section 5. Section 6 is represented the

potential technology of MTA. Section 7 concludes with paper notes and references.

2. Mobile Trade Agent

MTA is perhaps one of the rapid growing aspects of IT [8, 9]. It is employed, and roved for uses as various as e-commerce, information system, etc. MTA can be considered as a program that activates an individual relationship by performing certain things that another individual might perform [10]. Also it is an independent program that able to managing its perfect decision, and in detection one or more goals [11]. However, there are more than one kind of agent is available. In its uncomplicated structure it is software program that shifts by a huge quantity of information and set out a version of this information as assistance data to another agent. For instance of this is an agent that read and study the receiving e-mail, and direct it to a suitable agent for respond [12].

The MTA have the capability to travel around many sites on the Internet and achieve its jobs and send backs their results. This MTA would usually collect and examine information from crowds of sites on the Internet, and show this information to the user [13]. For instance of this is an agent of book shop that visits all convenient bookstore, and show to its user a list of favorite books existing and the best price offered for every one [14]. The MTA has several benefits. For instance it can let traders to react rapidly to market opportunities and give them the competitive marches that are necessary in present day commerce universal. Also, The MTA has the capability to tour various sites on a network, examine the information at every site and take sound decisions when commodities must be traded at the

chosen site. In addition the MTA is an independent and it can determine where to move on a network and what commodities to trade with no person involvement.

It should be able to halt agent from roving the network and order it to return back to centre. However, the centre is not the user client computer since user does not all the time employ the same client computer and can not even be get access whereas the agent tours the sites. Therefore, we present the idea of the (AD) where all agents are kept and centrally managed. MTA is by no means reserved at a user client computer. The user of the MTA dose not mails its MTA right away to any server. It gives order to the AD to simulate the MTA which will give orders to the MTA to rove the sites. The AD has a security benefit; it will just simulate MTA for its legal user, and it will initially authenticate the MTA user prior to it receives any orders from the MTA user [15]. The MTA should be able to pay for the commodities purchased and accept payment for commodities vend (16). We employ a scheme where the MTA supply to a merchant a user credit card number. The merchant employs this data to demand payment from the Authorization Server (AS) which works as a bank. The user credit card number is encrypted by a public key encryption scheme. The AS verifies that merchant just demand payment for commodities purchased by the MTA and check that merchant be given payment when MTA purchases commodities from him. Figure 1 displays the relevant steps included in of the program and explains the secure payment scheme that is employ. Also the figure shows that the MTA roving a network, trades commodities at three variants servers on a network.

- client computer and allow the agent to trade alone.
4. The AD gives orders to the MTA to rove the sites on the Internet which results the MTA to sift to merchant server₁.
 5. The MTA trade commodities from the merchant at server₁. The MTA should be able to pay for commodities purchased. So in this part we illustrate the authorization of trades and payment provided. The payment manner should be secure. In this case we employ a public key encryption scheme.
 - 5.1. The MTA provides merchant at server₁ its user credit card number. This data is encrypted by the user with AS_{pub} and user_{priv}. The AS saves a copy of the encrypted type of the user credit card number. This means that just the AS be able to decrypt the message and user only can find the meaning.
 - 5.2. The MTA generates a message point out that commodities is purchased. This data is encrypted by AS_{pub} and MTA_{priv}. This denotes that just the AS be able to decrypt the message and it can just be a MTA that generated the message. The MTA mail this message to the merchant at server₁.
 - 5.3. Merchant at server₁ requires the AS to authorize the trades and confirm payment. The MTA is by now given the merchant at server₁ user monetary information and a message signifying what it purchased. The AS will simply authorize the trades if merchant at server₁ and the MTA can accord that they traded precisely the same merchandise for the identical cost. To do this the merchant at server₁ creates the same report of the merchandise sold as the MTA carried out. This message is encrypted by server_{1priv} and AS_{pub}.
 - 5.4. The AS decrypts all the messages employing AS_{priv}, server_{1pub}, MTA_{pub} and verifies when merchant at server₁ report and the MTA report of the commodities traded are identical. The AS would naturally be a bank which will verify whether user has enough money and if so the trade is authorize and the AS will give the merchant at server₁ the money. The AS will employ traditional funds transfer methods to guarantee that payment is transferred to the merchant at server₁ bank account. The detail of how the AS transfers funds from user bank account to the merchant at server₁ bank account is not applicable. At this stage the trade is accomplished.
 6. The MTA roves the sites on the Internet and trades with new merchant servers. If necessary, the AS authorizes trades.
 7. The user give orders to the MTA through the AD to end trading and return to centre, it is also feasible to form the MTA in such a way that it mechanically ends trading when particular conditions are encountered, for instance a some number of commodities have been purchased.
 8. The AD bides for the MTA to turn back and orders it to simultaneously come back to the AD.
 9. The user will scan the MTA to view what commodities traded.

4. Protecting the MTA

However while an agent runs in the memory space of an alien merchant

servers, it is at risk to attacks from such servers. So in the following section we are going to illustrate MTA employing distributed objects. There are many security topics to be studied in MTA, for example authentication of the user i.e., the sender of MTA, secure message between the MTA and other MTAs, determination of the agent integrity and calculation of the agent capability to pay for commodities traded. However, in this section we explain secure MTA and illustrate the communication amongst a user, AD, MTA and server object are protected by a public key encryption scheme.

Figure 1 illustrates the MTA touring from merchant at first server to next server to trade with every merchant server. The capability of the agent to rove the Internet has the benefit that the agent can traverse several merchant servers to specify the top available merchants to trade commodities with them. When the MTA travels from one server to next it means that it runs in the memory of these servers. No question how we guard the MTA; whilst a version of MAT is in the memory of an alien server, it is at risk to attacks from such server it means that its secret key can be pickings out and illegal trades run by the server.

We require a structural design that will permit the MTA to traverse exotic servers to buy and sell with them, but actually stay in the protecting borders of the AD. This represents that conceptually the MTA still roves from one merchant server to another, but actually it stays at one protect position. The design that makes this type of roving practicable is DOT.

The Java object encapsulates data and functions, can be dedicated by inheritance, but can not get to across address memory boundaries. In difference, distributed objects are packaged as binary elements which are

accessible to remote clients by ways of technique invocations. Clients do not recognize which compiler built a server object [17]. They require knowing just its name and the partition it issues.

To employ MTA as a distributed object and have every merchant display its merchandise to another distributed object, then these distributed objects can carry out techniques on every other without being in the same memory space. The figure also show that the MTA applied as a distributed object, trading with a merchant object, carrying out methods on a merchant distributed object on a remote server, to get a list of commodities vend by its merchant. The MTA chooses to buy these commodities from the merchant who causes them to create a signed message, signifying what they trade, and give these messages to an authorization server.

It is essential to observe that every signed message is encrypted with the public and secret keys as illustrated in the last section. The MTA secret key shifted with it to the server which denoted that the merchant at server can attack the MTA and recovered MTA_{priv} . With a distributed object structural design, the MTA is not transferred to the server, but in fact remotely calls methods on the server object. This indicates that the MTA remains within the protected borders of the AD and the MTA and therefore MTA_{priv} is not subjected to attacks from any server. So to generate protected messages we employ the public key encryption scheme. So a message between the merchant, MTA, AS and the AD is encrypted by RSA scheme.

Assume a merchant server sends a message (m) to the MTA. The message is encrypted as follows. A merchant server creates a private key d , encrypt m by d so $m_2 = e(m, d)$, merchant at server after that encrypts the private key d by the MTA public key so $m_3 = e(d,$

MTA_{pub}). The encrypted message m_2 and m_3 both construct a digital envelope [18] that is sent to the MTA. On receiving the digital envelope, the MTA decrypts the RSA key with its secret key and employs the private key to decrypt the message. The public keys of the MTA and the application servers should be issued in the AD.

5. Applications of MTA

The MTA touring the sites on the Internet trading commodities with the capability to securely and rapidly receiving or paying payment makes a great number of applications feasible such as demand and supply agents which we will discuss in this section.

Agents in trade are categorized as either user agents trading on behalf of the user, or business agents representing suppliers [19]. There is no ground why the MTA, when controlled properly, can not reflect a user and business agent. Such an agent will evaluate the market and synchronously it can recognize a demand for an exact product, begin roving the sites on the Internet and purchase these merchandises from merchants that can provide them at the cheapest cost. The MTA then returns back to the source of the demand and vends the commodities with a gain. This demand and supply create earnings for its owner by link both in that demand. The real commodities never reach the MTA owner, instead of MTA insure that any commodities purchased are traded instantly and sent to another possessor.

6. The Potential Technology of MTA

Just some years ago, it has been impractical to employ MTA on the Internet permitting agents to securely traverse sites and trade commodities. A certain solution, like General Magic [16], permits for roving agents and create agent based e-commerce

potential but it is a predetermination with a restricted development conditions [20]. MTA will only be practical in an open market where they can rove easily to a huge number of sites and doing business with them.

DOT creates a great flexible network system, since it encapsulates data and functions in objects that can rove any sites on the Internet, execute on various layer, address to inheritance applications using technique of object receptacle, and directs them and the resources they manage [21]. This picture of DOT illustrates that it is a fantastic respondent technology to apply the MTA with. We stresses that agents roving of sites on a network, recommending individuals when to trade merchandise, for instance mobile trader [22], but MTA securely roving thousands of sites over the Internet with the capability to trade merchandise if they believe it is apposite, is only become probable with the growing up of DOT.

7. Conclusions

MTA have the capacity to determine what commodities to trade and with which merchants. MTA generate businesses more respondent to market variations and permit them to use trade chances once they come out. Through DOT growing to a point were it is potential to apply MTA that can rove sites on the Internet over the world, MTA can provide trades the capability to respond rapidly to market prospects and increase income.

This paper illustrates the MTA roving the markets of the world to trade on behalf of its user. In another study this MTA could be applied in an existing Internet to look into the real results of these agents in a natural environment. We are curious in the performance cost these agents might produce. It is also essential to examine the maturity of present object demand as a way to

employ the communication between servers and MTA distributed objects.

References

- [1] Suri, N., Brandshaw, J.M., Breedy, M.R., Groth, P.T., Hill, G.A., Jeffers, R., and Mitrovi T. S. An Overview of the NOMADS Mobile Agent System. Sixth ECOOP Workshop on Mobile Object Systems. U.S.A, 2000.
- [2] Canas, A.J., Carvalho, M., Arguedas, M., Mining the Web to Suggest Concepts During Concept Mapping: Preliminary Results. XIII Simposio Brasileiro de Informatica na Educacao, Porto Alegre, Brasil (Nov, 2002).
- [3] Canas, A., Leak, D.B., Maguitman, A., Combining Concept Mapping with CBR: Towards Experience-Based Support for Knowledge Modeling. AAI 2001.
- [4] Cavaalho, M. Hewett, R. Canas, A. Enhancing Web Searches from Concept Map-based knowledge Models. SCI – World Multiconference on Systemics, Cybernetic and Informatics, July, 2001.
- [5] Lawrence E., Newton, S., Lawrence, J., Dann, S. Corbitt, B. and Thanasankit, T. 2003 Internt Commerce: Digital Models for Business, (rrd edition, Brisbane: John Wiley and sons.
- [6] Elaine Lavreence and John Lawrence, Threats to the Mobile Enterprise, International Conference on Information Technology 5-7 April 2004, Las Vegas, Nevada, USA.
- [7] Stanifor, S., Paxson, V., Weaver, N, How to Own the Internet in Your Spare Time., Proceedings of the 11th USENIX Security Symposium. San Fransicso, CA. August 2002.
- [8] Suri, N., Bradshaw, J.M., Breedy, M.R., Groth, P.T., Hill C.A., and Jeffers., R. Strong Mobility and Fine-Grained Resource Control in NOMADS. Proceedings of the 2nd International Symposium on Agents Systems and Applications and the 4th International Symposium on Mobile Agents (ASA/MA 2000). Springer-Verlag.
- [9] Marco Carvalho, Thomas Cowin and Niranjan Suri. MAST – A Mobile Agent based Security Tool, Journal of Systemics, Cybernetics and Informatics, Volume 2 – Number 6 – 2005, USA.
- [10] T. Selker, A Teaching Agent that Learns, Communications of the ACM 37 (7), 1994, pp. 92-99
- [11] N. Jennings and M. Wooldridge, Software Agents, IEEE Review, January 1996, pp 17-20.
- [12] L. Wirthman, Gradient DCE has sign-on feature, PC Week, March 1996, p 31.
- [13] Suri, N. Carvalho, M., Brandshaw, R., Brandshtems, J., Small Mobile Agent Platforms. Autonomous Agent & MultiAgent Systems Workshop on Ubiquitous Agents on Embedded, Wearable and Mobile Devives . July 2002.
- [14] Netsurfer Digest, Book' A good Idea that needs work, Vol 2 (17), 6 June 1996.
- [15] Elliott, G. & Phillips, N 2004 Mobile Commerce and Wireless Computing Systems, Pearson Addison Wesley 2004.
- [16] Advanced Information Management Strategies, Payment Systems for the Internet, The Meta Group, August 1996.
- [17] Suri, N., Bradshaw, J.M., Breedy, M. R., Ford, K.M., Groth, T., Hill, G.A., and Saavedra, R., State Captaure and Resource Control for Java: The

Design and Implementation of the Aroma Virtual Machine. White Paper, 2004.

[18]P. Fahn, About Today's Cryptography, Answers to Frequently Asked Questions, RSA Laboratories, September 1993.

[19] C. Harrison, D. M. Chess and A. Kershenbaum, Mobile Agents: Are they a good idea? IBM Research Report (T.J. Watson Research Center), March 1995.

[20] R. Orfali and D. Harkey, Client/Server Survival Guide with OS/2, John Wiley and Sons, 1994.

[21] R. Orfali, D. Harkey and J. Edwards, the Essential Distributed Objects Survival Guide, John Wiley and Sons, 1996.

[22] J. Horberg, Talk to My Agent: Software Agent in Virtual Reality, Computer – Mediated Communication Magazine, Vol 2 (2), 1 February 1995, p. 3.