International Journal of New Technology and Research (IJNTR)
ISSN:2454-4116, Volume-4, Issue-4, April 2018 Pages 116-120

Performance Evaluation Models for a Secure Agent-Based Electronic Commerce

Araoye Olalekan I., Akintoye Kayode A. ,Adu Micheal K

***Abstract*— Agent-based applications on internet are gaining more attention because of tremendous benefits one can derive from it, especially when you can dispatch your agent to do shopping for you. However security has been a major challenge to its development. Several security techniques such as cryptography, steganography have been deployed to combat security vulnerabilities of mobile agent system and certain reliable level of security has been obtained. This research paper shows how to evaluate the performance of a secure agent-based system. In this research, a secure agent-based application was developed using crypto-steganography security technique which is a combination of cryptography and steganography. Performance evaluation models were formulated based on work load and execution time of the agent.**

***IndexTerms*—Agent-basedapplications,Crypto-steganography, Evaluation, Models.**

I. INTRODUCTION

Mobile agents are autonomous software that can transport itself from one node to another node in a computer network system [1]. Mobile agent suspends execution on one node and resumes on another node [2].As an executing program, a mobile agent is made up of code, data and execution state; embedded with some intelligence and ability to autonomously migrate across the network [3]. The use of mobile agent for electronic transaction has some interesting advantages. The user can go offline after the agent is sent out and can come online again when the agent has performed it tasks [4]. This is good for a situation where a user cannot stay online for a long time. Giovanni [5] stated that mobile agents lower the bandwidth need and relief the consumer from time consuming and difficult search for relevant information.

The advantages of using mobile agent in electronic commerce include optimization decisions, mobility, flexibility and autonomy [6]. Another important advantage of mobile agent is that it saves the consumption power of sending devices because it performs its task locally. This means PDA, laptop or mobile phone with limited computing power can be used [7]. A feature being frequently attributed to mobile agents is autonomy, the ability to perform certain tasks without guidance or intervention by a human user [8].
Mobile agent is a form of code mobility which is an aggregate of code on demand and client-server. Mobile agent is yet to be received in the internet community, since issues such as reliability and security are yet to receive developer's confidence [5]. However because of available tools, mobile agents have become extensively popular not only in the research community but also in industrial projects [9]. One of the most attractive applications of mobile agents is the notion of distributed information processing. This is shown in the mobile computing scenarios where users have portable computing devices with only intermittent, low bandwidth connections to the main network. A mobile agent can migrate from its home, move on to the site of the required information resource and perform a locally custom-retrieval task. Only the results are transmitted back to its home [10].
Moreover, the mobile agent can carry on a task while the connection to destination server is temporarily lost and then continue once the link returns to send the found result. Mobile agent can exploit the high processing power available in the server machines by shifting the computations into the server side.
Mobile agents provide a solution for the dynamic environment of the mobile devices because they do not rely on server operations. The mobile agent appears to tackle significant problems whether in wired or wireless communication such as disconnection operations, increased network traffic and others. Moreover, mobile agents can play a major role in the wireless communication after the failure of the Java RMI in increasing the performance over slow wireless links [11]. Once the mobile agent has migrated, the connection between client and server will be disconnected. This saves network bandwidth, especially in a wireless environment. When a mobile agent finishes its job at the server, it will then be ready to reconnect to its host or to migrate to another node to perform other duties within the network.
Mobile agents are also well suited for network management applications such as remote network management, software distribution, and adaptive response to network, events. Most of the current network management software is based on the Simple Network Management Protocol (SNMP). The developers of SNMP designed it in the mid-1980s as a temporary measure with known problems and inherent limitations until industry could provide a better solution. Mobile agents allow for greater control of network devices and aren't limited by whatever parameters the manufacturer of the device decides to make available via SNMP. Mobile agents can also provide adaptive responses to network events. Without mobile agents, all of the software required to support and respond to all possible scenarios must be kept loaded and available on a device at all times. The network manager must take the time to respond to each event, and interact with each device individually. In contrast, mobile agents can be dispatched to respond to network events, and only the software required for normal operation needs to be loaded onto the device. Upgrading network software to add new functionality involves a significant roll-out effort on behalf of

Araoye, Olalekan I, Department of Computer Science, Federal Polytechnic, Ado-Ekiti, Ngeria.
Akintoye, Kayode A, Department of Computer Science, Federal Polytechnic, Ado-Ekiti, Ngeria.
AduMicheal K, Department of Computer Science, Federal Polytechnic, Ado-Ekiti, Ngeria.

network administrators. Installing new software, upgrading existing software or reconfiguring network hardware can be accomplished by simply dispatching mobile agents to the appropriate machines [12].

Mobile agents use the capabilities and resources of remote servers to process their tasks. When a user wants to do tasks beyond the capabilities of his or her computers, the agents that perform the tasks can migrate to and be executed at a remote server. Mobile agents can also mask temporal disconnections in networks. Mobile computers are not always connected to networks, because their wired networks are disconnected before they are moved to other locations or wireless networks become unstable or non-available due to deteriorating radio conditions or are not uncovered by the area at all.

A stable connection is only requested at the beginning to send the agent, and to take the agent back at the end of the task, but this is not requested during the execution of the whole application execution. Several researchers have explored mechanisms for migrating agents through unstable networks [13]. When a mobile agent requests a runtime system to migrate itself, the system tries to transmit the moving agent to the destination. If the destination cannot be reached, the system automatically stores the moving agent in a queue and then periodically tries to transmit the waiting agent to either the destination or another runtime system on a reachable intermediate node as close to the destination as possible. These relay runtime systems repeat the process until the agent arrives at its destination.

II. LITERATURE REVIEW

There can be seven types of attack by malicious hosts according to [14] which are spying out and manipulation of code, spying out and manipulation of data, spying out and manipulation of control flow, incorrect execution of code, masquerading of the host, spying out and manipulation of interaction with other agents; and returning wrong results of system calls to agents

There are a number of solutions proposed by [15] to protect agents against malicious hosts, which are:

a. Establishing a closed network: limiting the set of hosts among which agents travel, such that agents travel only to hosts that are trusted.
b. Agent tampering detection: using specially designed state-appraisal functions to detect whether agent states have been changed maliciously during its travel.
c. Agent tampering prevention: hiding from hosts the data possessed by agents and the functions to be computed by agents, by messing up code and data of agents, or using cryptographic techniques

[16],[17] proposed the following solutions to protect mobile agent respectively.

a. Protected agent state when is basically signing and encrypting of agent states based on public-key cryptography.
b. Mobile cryptography for code integrity. Code integrity should be maintained

[18] stated that security of agents for e-commerce must be viewed in a realistic and pragmatic way.

a. Some host in the network can be trusted
b. More than one agent can be used in order in order to build a secure mobile agent environment.

A lot of researchers have developed mobile agent- based electronic commerce applications such as [19], [20], [8], [21], [22],[23], [24] and [25].

However security is a major problem of mobile agent technology as discussed in [26], [14], [19], [8], [21], [22],[23], [24], [25], [1].

People who have worked on the security of mobile agent-based electronic commerce include [19], [21], [27], [25].

[21] stated that like any distributed system, the mobile agent system is subject to security threats such as eaves dropping, corruption, masquerading, denial of service, replaying and repudiation. They stated that issues such as encryption, authorization, authentication and non-repudiation, therefore must be addressed in a mobile agent system.

A secured agent-based electronic commerce using crypto-steganography was developed by [28]. Experiment was performed on the agent using work load and execution time and results were shown and analysed. Performance model is shown in section 3 and section 4 of this paper.

III. AGENT MOBILITY AND INTERACTION MODEL

The mobility behaviour of the agent is described by a destination vector $S = (S_0 ..., S_n)$. For the $i-th$ interaction, the agent moves to destination location S_i . Thus migration takes place between $(i-1)-th$ and $i-th$ interaction only if $S_i \neq S_{i-1}$.

Let $J = (I_i ,..., I_n)$ be a sequence of interactions, the i-th interaction is described by

$I_i = \{R_i, m_i . B_{qry}, B_{res}, \sigma_i\}$ (1)

Where $R_{i,}$ is the remote location with which the communication should take place. Each communication consists of m_i (local or remote) procedure calls with request size, $B_{qry,}$ reply size $B_{res,}$ and selectivity σ_i . The size of the agent after interaction iismodelled for $i = 0,\ldots,n$ by

$$B_{Ai} = (B_{codei}, B_{datai}, B_{statei}) \quad (2)$$

where B_{codei} and B_{statei} remain fixed while

$$B_{datai} = (B_{datai-1} + m_i(1-\sigma_i)B_{resi},) \quad (3)$$

In the context of agent interaction, the remote function call (RFC) is used to call procedures (methods) that are provided by the communication partner. RFC includes binding to the server, marshalling, transfer, unmarshalling of the request parameters, execution of the request, marshalling, transfer and unmarshalling of the reply. Marshalling is dependent of the size of the request parameters only. The performance model therefore concentrates on the communication dependent part of the RFC.

The network load B_{RFC} (in bytes) for a simple remote function call from location S_{i-1} to location S_i consists of the size of the request B_{qry} and the size of the reply B_{res}

$$B_{RFC}(S_{i-1}, S_i, B_{qry}, B_{res}) = \begin{cases} & B_{qry} + B_{res} S_{i-1} \neq S_i \\ 0 & else \end{cases} \quad (4)$$

The execution time T_{RPC} for a simple remote procedure call from location S_{i-1} to location S_i consists of the time for marshalling and unmarshalling of request and reply (factorμ) plus the time for the transfer of the data on a network with throughput $\tau(L_1, L_2)$ and delay $\delta(L_1, L_2)$

$(S_{i-1}, S_i, B_{qry}, B_{res}) =$

$2\delta(S_{i-1}, S_i) + \left(\frac{1}{\tau(S_{i-1}, S_i)} + 2\right) B_{RFC}(S_{i-1}, S_i, B_{qry}, B_{res})$ (5)

An interaction is performed by the migration of the agent to the communication partner, a local or remote procedure call, the processing of the data received and the transfer of the processed data back to the source location. A classical migration includes marshalling, transport and unmarshalling of code, data and execution state of the agent to the server. Marshalling increases linear with the size of data and execution status of the agent, while the code of the agent is already stored in transport format and is only transferred on demand (i.e. if the code is not yet available at the server). The agent consists of B_{code} bytes of code, B_{data} bytes of data and B_{state} bytes of execution state and is described by the triple $B_A = (B_{code}, B_{data}, B_{state})$ .The size of the request to the procedure B_{qry} is yet contained in B_{data}. The size of the reply from the procedure B_{res} is reduced by remote processing to $(1-\sigma)B_{rep}$ with $(0 \leq \sigma \leq 1)$ by the agent where σ models the selectivity of the agent.

The network load for the migration of an agent A from location S_{i-1} to location S_i is calculated by

$$B_{Mig}(S_{i-1}, S_i, B_A) = \begin{cases} 0 & if\ S_{i-1} = S_i \\ P(B_{cr} + B_{code}) + B_{data} + B_{state} & otherwise \end{cases} \quad (6)$$

Where P denotes the probability that the code is not yet available at location S_i and B_{cr} is the size of the request from S_{i-1} to S_i to transfer the code. If the agent additionally sends back a reply message to location S_{i-1}, the network load amounts

$B_{MR}(S_{i-1}, S_i, B_A, \sigma. B_{res}) =$

$$B_{Mig}(S_{i-1}, S_i, B_A) + \begin{cases} 0 & if\ S_{i-1} = S_i \\ (1-\sigma)B_{res} & otherwise \end{cases} \quad (7)$$

Where B_{rep} is the size of the reply and σ denotes the selectivity of the agent.

IV. SYSTEM PERFORMANCE EVALUATION MODEL

The execution time T_{RFC} for a simple remote call from location S_{i-1} to location S_i consists of time for marshalling and unmarshalling of request and reply factorμ plus the time for the transfer of data on network with throughput τ and delay δ

$$T_{RFC} = 2\sigma(S_{i-1}, S_i) + \left[\frac{1}{\tau(S_{i-1}, S_i)}\right] + 2\mu B_{RFC}(S_{i-1}, S_i, B_{qry}, B_{res}) \quad (8)$$

The network load B_{seq} and execution time T_{seq} for a mixed sequence of remote function calls and agent migration are calculated thus

$$B_{seq}(M, S, B_{Ai-1}) = \sum_{i=1}^{n} \left(B_{mig}(S_{i-1}, S_i, A_i) + m_i B_{RFC}(S_i, R_i, B_{qry}, B_{res})\right) \quad (9)$$

$$T_{seq}(M, D, B_{A0}) = \sum_{i=1}^{n} \left(T_{mig}(D_{i-1}, D_i, B_{Ai-1}) + m_i T_{RFC}(D_i, R_i, B_{reqi}, B_{repi})\right) \quad (10)$$

V. PERFORMANCE EVALUATION FOR AGENT SEARCH

In this performance model, it is assumed that all servers have the probability (p) of finding data item. The client sends a request (BC_{req}) from location L_1 to $L_{2...}L_n$. The request in byte is taken as (BC_{req}) to the firs host server to get item price I_p and then the next host sever in itineraries until the last host server. The process is assumed to be a search process. The system call returns a found data B_F or not found B_{NF} reply. For a client-server the search terminated when the item is found.

The Algorithm for Client-Server Search

BEGIN

Search for an Item

IF FOUND Reply = B_F

Else

Reply= B_{NF}

END.

The network load (B_{NL}) is calculated thus:

$$B_{NL} = P_1(BC_{req} + B_F) + P_2(1-P_1)(BC_{req} + B_{NF} + B_F) + P_3(1-P_1)(1-P_2)(BC_{req} + 2B_{NF} + B_F) + \cdots P_n(1-P_1)(1-P_2)(1-P_3)\ldots(1-P_{n-1})(nBC_{req} + (n-1)B_{NF}) + B_F \quad (11)$$

B_{NL} can be expressed as

$$B_{NL} = \sum_{i=1}^{n} P_i \prod_{j=1}^{i-1} (i - P_j)\,(iBC_{req} + (i-1)B_{NF} + B_F) \quad (12)$$

If all severs have the same probability then B_{NL} can be re-written as

$$B_{NL} = nP \sum_{i=1}^{n} (1-P)^{i-1}\,(iB_{NF} + (i-1)B_{NF} + B_F) \quad (13)$$

Then performance measure for execution time (E_t) which is time measured from lunching to returning back for a single search in a client-server can be modelled thus:

The time to process the request is taken as R_t , the time to transfer one byte form location $L_1$to L_2 is taken as $(L_1\text{-}L_2)B_t$

$$E_t = P_1(BC_{req} + B_F)B_t + R_t + P_2(1-P_1)(BC_{req} + B_{NF})B_t + (BC_{req} + B_F)2B_t + 2R_t + P_3(1-P_1)(1-P_2)(BC_{req} + B_{NF})B_t + (BC_{req} + B_{NF})2B_t + (BC_{req} + B_F)3B_t + 3R_t + \cdots P_n(1-P_1)(1-P_2)(1-P_3)\ldots(1 - P_{n-1})(BC_{req} + B_{NF})B_t + 2B_t + n(n-1)B_t + (BC_{req} + B_F)nB_t + nR_t \quad (14)$$

This can be written as

$$E_t = \sum_{i=1}^{n} P_i \prod_{j=1}^{i-1}(i - P_j)\left(BC_{req} + B_{NF}\right) \sum_{j=1}^{i-1} jB_t + iB_t\left(BC_{req} + B_F\right) + iR_t \quad (15)$$

This equation can be simplified as

$$E_t = nP \sum_{i=1}^{n} (1 - P)^{i-1}\left(BC_{req} + iB_F\right) + (i - 1)B_{NF} + iR_t \quad (16)$$

VI. CONCLUSION

Performance evaluation of a secure agent-based application is germane to measure its efficiency when deploy for use on the internet. Workload and execution time are two major parameters for its evaluation. This research paper has shown how to evaluate a secure agent-based application based on workload of the agent and its execution time.

Agent-based applications will gain more popularity and will be widely accepted by Merchants and Customers on the internet if its security isguaranteed. This models will also ensure reliability of the system.

REFERENCES

[1] O. I. Araoye, O. S.Adewale, B. K,Aleseand O. R. Akinyede, "The design of a secured mobile agent-based electronic commerce using crypto-steganography,"Book of abstract, 4th Annual Conference, School of Sciences, The Federal University of Technology, Akure, Nigeria 2016.

[2] A.Koliousis and, J.S. Sventek, "A trustworthy mobile agent infrastructure for network management," The tenth IFIP/IEEE International Symposium on Integrated Network Management, Munich, Germany, pp.383-390, 2007.

[3] S. A.Arekete, O. C.Akinyokun, O.Olabode, and B. KAlese, "Design of mobile agent for monitoring activities of users,"*Computer Engineering and Intelligent Systems*, vol.4, no. 3, pp.12-25, 2013.

[4] B. L. Dannyand O. Mitsuru, "Seven good reasons for mobile agents", *Communication of the ACM*, vol. 42, no.3, pp. 88-89,1999.

[5] V. Giovanni,"Mobile agent: ten reasons for failure", International Conference on Mobile Data Management, IEEE, pp.298, 2004.

[6] J. A. Bakos,"Strategic analysis of electronic marketplace", *MIS Quarterly*, vol. 11, no.4, pp. 295-310, 1991..

[7] S. Daveand P. Bart,"Secure e-commerce using mobile agents on untrusted hosts",COSIC Internal Report.2004.

[8] O. I. Araoye, "Market information agent system (mias). security and reliability issues", M.Tech Thesis, The Federal University of Technology, Akure, Nigeria, 2005.

[9] E.Christian, B. Peter,R.Wilhelm,"Some thoughts on migration intelligence for mobile agents", *Technical Report*, Friedrich-Schiller University, vol.1, no. 9, 2001.

[10] S. G.Robert, , K. David, A. P. Ronald,"Mobile agents versus client-server performance, scalability in an information retrieval task", Proceedings of the fifth IEEE International Conference on Mobile Agents, Atlanta, Georgia, pp. 229-243, 2001.

[11] S.Campadello, O.Koskimies, K.Raatikainen, H. Helin,"Wireless java rmi, enterprise distributed object",Computing Conference, EDOC Proceedings, fourth International, 25(28), pp.114 –123, 2000.

[12] C.David, G.H.Benjamin Colin, L.David, P.Colin, T. Gene,"ItinerantAgentsfor Mobile Computing",IEEE Personal Communications,vol. 2, no. 5, pp. 34-49, 1994.

[13] I. Satoh,"Selection of mobile agents," Proceedings of 24th IEEE International Conference on Distributed Computing Systems (ICDCSb2004), IEEE Computer Society, pp. 484-493, 2004.

[14] F. Hohl,"A Model of Attacks of Malicious Hosts Against Mobile Agents", Proceedings of the ECOOP Workshop on Distributed Object Security and 4th Workshop on Mobile Object Systems: Secure Internet Mobile Computations, INRIA, France, pp.105 -120, 1998.

[15] C. Tschudin,"Mobile agent security, intelligent information agents: agent based informationdiscovery and management in the internet",*Springer*, pp. 431 – 446, 1999.

[16] J.Page, A.Zaslavsky, M.Indrawan,"A Buddy model of security for mobile agent communities operating in pervasive scenarios", ACM International Conference Proceeding Series; Proceedings of the Second Workshop on Australian Information Security, Data Mining and Web Intelligence and Software Internationalization, (54),1725, 2004.

[17] T.Sander, C. F.Tschudin, "Protecting mobile agents against malicious hosts", In:GiovanniVigna, ed.,Springer, Mobile Agents and Security, LNCS 1419, pp. 44-60, 1998.

[18] J. M.Paulo, M.S.Luis, G. B.Joao,"Security mechanisms for using mobile agents in electronic commerce", Departmento de EngenhariaInformatica, Universidedede`Coimbra,Portugal,2000.

[19] A. Chan,"Mobile agent security and reliability issues in electronic commerce". A Thesis Submitted in Partial fulfillment of the Requirements for the DegreeofMaster of Philosophy, In computer Science and Engineering, The Chinese University of Hong Kong, 2000.

[20] J. Rahul,"Mobile agents for e-commerce", KR School of Information Technology, Indian Institute of Technology, Bombay, 2002.

[21] A. KannamalN. Ch.S.N.lyenger, "A model for mobile agent security in e- business applications", *International Journal of Business and Information*, vol. 2, no. 2, pp.185-198, 2007.

[22] D.Michal, G.Maria, G.Maciej,K.Panel, P. Marcin,"Designing and implementing data mart for an agent-based e-commerce system", *IADIS International Journal*, vol. 6, no. 1, pp.37-49, 2008.

[23] S.Richard,G.O. Jose, "Security analysis of an agent-mediated book trading application", *International Journal of computing and ICT Research*, vol. 3, no.1, 2009.

[24] Z. Ziming, "An Agent-based Online Shopping System in E-Commerce", *Computer and Information Science*, vo. 2, no.4, pp. 14-19, 2009.

[25] K.Sougata, D.Arifit, Y.Zhang, L.Li, Ch.S.N. lyengar,"Agent-based secured e-shopping using elliptic curve cryptography", *International Journal of Advanced Science and Technology*, vol. 38, pp. 93-115, 2012.

[26] M. F.William, D. G.Joshua, S. Vipin, "Security for mobile agents: authentication and state appraisal", In Proceedings of the Fourth European Symposium on Research inComputerSecurity,Rome,Italy, pp.118–13, 1996.

[27] R. Vikas,"E-commerce security using pki approach", *International Journal on Computer Science and Engineering*,vol. 2, no. 5, pp. 1439-1444, 2012.

[28] O.I. Araoye,"Securing mobile agent-based electronic commerce using crypto-steganography", Ph.D Thesis, The Federal University of Technology, Akure, Nigeria, 2017.