Scalability of Agent-Based Onion Routing Network

Song, Ronggong; Korba, Larry

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

Scalability of Agent-Based Onion Routing Network *

Song, R., and Korba, L.
March 2004

* published in Proceedings of the 19th International Conference on Computers and their Applications (CATA-2004). Seattle, USA. March 18-20, 2004. NRC 46541.

Canada

Scalability of Agent-based Onion Routing Network

Ronggong Song and Larry Korba
Institute for Information Technology
National Research Council of Canada
Ottawa, Ontario K1A 0R6, Canada
{Ronggong.Song, Larry.Korba}@nrc.ca

Abstract

Security and anonymity are vital for some types of agent-based e-commerce applications. In order to provide secure and anonymous communication protection for multi-agent systems, we have developed an alternate Onion Routing approach based on agile agents under JADE multi-agent platform. In this paper, we present a simulation of the protocol and analyze its scalability.

1 INTRODUCTION

Multi-agent applications have been expected to take an important role in the future information society. However, security and privacy protection for multi-agent applications are becoming critical issue. In order to provide secure and anonymous protection for the multi-agent communications, we have developed an agent-based Onion Routing approach [1] using agile agents.

In the agent-based Onion Routing network, we use many security functionalities such as multi-layer encryption and decryption, public-key certificate management, onion routing channel setup, etc. These security and privacy protection features may have the different effect on the system scalability when they are used under the different environments. On the other hand, in order to make the agent-based onion routing approach more practical and efficiency, the scalability of the agent-based onion routing approach becomes another important issue.

In this paper, according to the agent-based Onion Routing network proposal, we first design several simulation models. Based on these models, we then simulate the agent-based Onion Routing network under the JADE multi-agent platform [2] and Network Simulator software (NS-2) [3], and present an analysis of its scalability problem.

The rest of the paper is organized as follows. An agent-based Onion Routing network is briefly introduced in the next section. In Section 3, several simulation models are designed for the testing. In Section 4, the simulation and testing metrics are discussed. In Section 5, we show the simulation results and analyze the scalability problems. In Section6, we present some concluding remarks.

NRC Paper number: NRC- 46541

2 Agent-based Onion Routing Network

The primary goal of onion routing [4, 5, 6] is to provide strongly anonymous communications in real time over a public network with reasonable cost and efficiency. In onion routing, initiating applications make connections through a sequence of onion routers instead of making socket connections directly to responding machine. Onion routers are computer programs that perform application-layer routing for the network. Onion routing builds anonymous connections within a network of onion routers.

In order to provide anonymous communication for multiple agent applications we have developed an agent-based onion routing network. It is implemented using the JADE multi-agent platform. The detail is described as follows.

The agent-based onion routing network consists of many multi-agent platforms. Each agent platform has several onion node agents and a single onion monitor agent. The onion node agents can be located in different containers. The onion monitor agent usually is located in the main container. The onion node agents connect to each other via ACL Message [2]. The onion monitor agents communicate to each other via a multicast mechanism. Every onion node agent accepts the data stream from its customer application agents or other onion node agents, and forwards the data stream to the next onion node agent according to the routing information. The agent-based onion routing topology is illustrated in Figure 1.

To begin an anonymous session, the initiator application agent sends its request message to the onion node agent that was registered to act on its behalf using a secure connection. We call the onion node agent an initiator onion proxy for the initiator application agent. According to the destination application agent address, the initiator onion node agent randomly picks several onion agents to form the anonymous route, and encrypts the original communication data using the nested encryption algorithm. The onion not only protects the payload, but also provides a means for safely distributing the symmetric keys required for the nested encryption algorithm. The onion node agent then encapsulates the

encryption data payload using the ACL Message and sends it to the next onion node agent. Finally, the original communication data is forwarded to the responder application agent. In addition, the expiration time of each anonymous onion channel can be set up according to the privacy protection requirements.

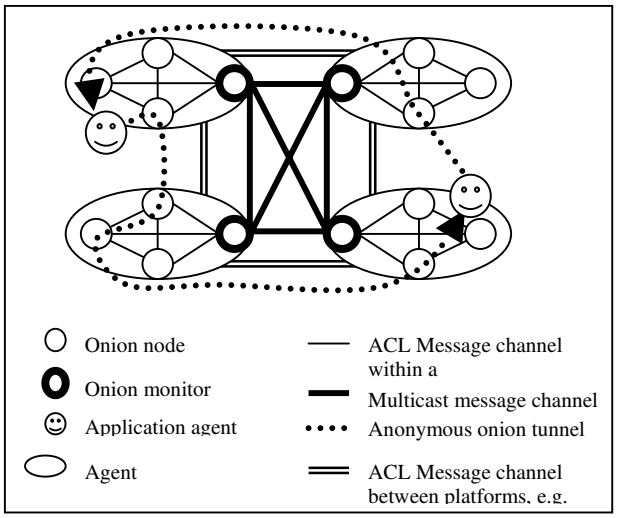

Figure 1. Agent-based Onion Routing Topology

Since the above agent-based onion routing network is implemented based on many cryptographic mechanisms such as the RSA public-key cryptography [7], the Rijndael (AES) symmetric key cryptography [8], etc., it will have a different effect on the system scalability when it is run on different environments, for instance each computer only running one onion node agent, or one computer running many onion node agents.

3 Simulation Model

The onion routing network is complex. Its scalability depends on how it is used within the multi-agent systems. In order to perform refinement testing, we propose several testing models for the different environments, which the onion routing network is deployed in the multi-agent systems.

- ***Model 1:*** In this model, we compare the scalability of two situations. The first situation is where each onion node agent is run on different hosts. The second situation is where all onion node agents are run on the same host. Figure 2 depicts the two situations. For the testing, we only choose four onion node agents.

- ***Model 2:*** In this model, under the above situations, we do further testing on the system scalability when the anonymous path length varies -- the path through three, four, …, seven onion node agents. Figure 3 depicts the two situations.

- ***Model 3:*** In this model, under the situations in the model 1, we want to compare the system scalability when the user agent size changes but in the situation where they use the same path and the total messages they send also are the same. Figure 4 depicts the two testing situations.

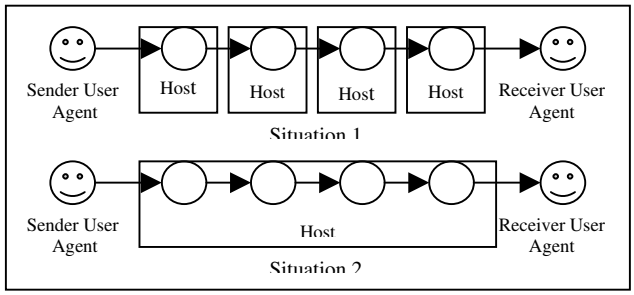

Figure 2. Testing model 1 for onion routing network

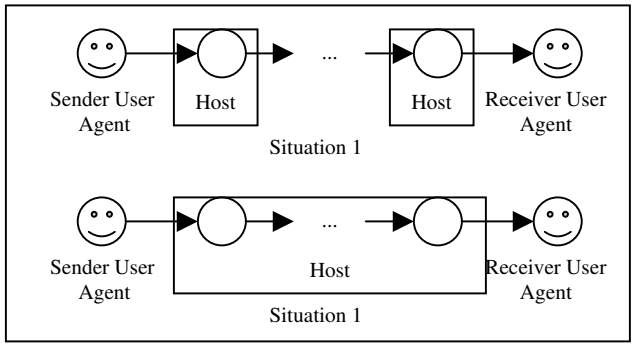

Figure3. Testing model 2 for onion routing network

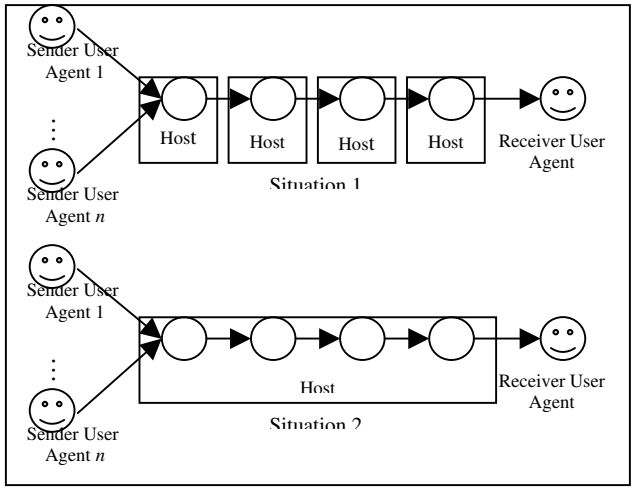

Figure4. Testing model 3 for onion routing network

4 Simulation Platforms and Metrics

The testing platform includes the hardware and software. The hardware used for the testing includes two computers and local Ethernet. The main testing is on the Intel Pentium 4, the CPU and Memory are 1.50GHz and 256 MB respectively, and the operation system is Windows 2000. The network used for the testing is the local 100Mbps Ethernet.

The software used for the testing includes the operating system and testing software platform. In this paper, all testing is on the Windows 2000 operation system. The testing software platforms include JADE (3.0) multi-agent platform, and Network simulator (NS-2). During testing, we use JAVA as the programming language, and the Java™ 2 Platform, Standard Edition (J2SE™) version 1.4.2 as the essential Java tools and APIs for developing the simulation applications.

In the simulation, the main simulation parameters include user size, total processing time for all messages through the onion routing network. The total processing time includes the computing complexity cost for privacy and security processing in the above model.

- Message size: the number of the messages sent by the sender user agents, where each message contains 1Kbits content;
- User agent size: the number of the sender user agents;
- S_Time: the total processing time for an onion routing security channel setup;
- T_Time: the total processing time that the sender user agents send all messages to the receiver user agent and the receiver user agent receives all messages from the sender user agents.

5 Simulation Results

Based on the JADE platform, we first test the basic parameters like a security channel setup time (S_Time) through the onion routing network, and a message processing time (i.e., data transfer) through the onion routing channel. Table 1 and Figure 5 depict the testing parameters, where we use the 2048bit RSA algorithm as public key cryptography in the testing, the one of the onion nodes in the onion routing works as the proxy node, and the message processing time (including Rijndael encryption and decryption) through each onion node is about 10ms.

We then test the different models under the JADE multi-agent platform and NS-2 based on the above parameters. The simulation testing is done according to the user agents using the onion routing network under the different environments in the models. In addition, the same a pair of sender user agent and receiver user agent will use the same security channel after the secure channel setup in the following testing for the message transmission.

Table1. S_Time for the onion routing channel setup

Onion node hops	3 nodes	4 nodes	5 nodes	6 nodes	7 nodes
S_Time (ms)	1483	1629	2513	2997	3615

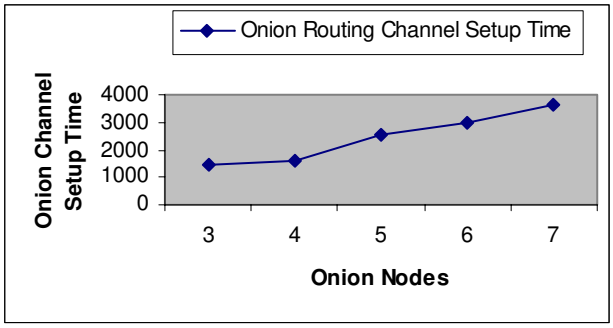

Figure 5. S_Time for the onion routing channel setup

(1) Model 1

In Model 1, we test the effect of the number of the messages on the T_Time under the situation 1 and 2. The scalability of the messages is from 100 to 12800, where all messages sent from sender user agent to the receiver user agent are through the onion routing network. Table 2 and Figure 6 depict the total processing time.

Table 2. T_Time for the model 1 under JADE platform

Messages	100	200	400	800	1600	3200	6400	12800
Situation 1 (ms)	2680	3672	5685	9580	17212	32444	62697	123494
Situation 2 (ms)	5615	9080	16350	30911	59843	117706	233101	464144

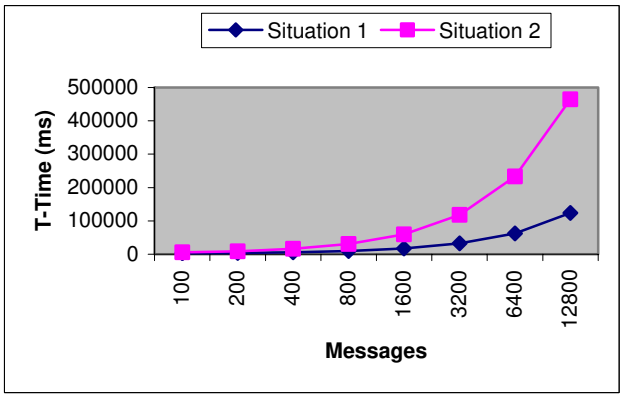

Figure 6. T_Time for Model 1 under JADE platform

Table 3 and Figure 7 depict the total processing time under the NS-2 platform.

Table 3. T_Time for the model 1 under NS-2 platform

Messages	100	200	400	800	1600	3200	6400	12800
Situation 1 (ms)	2679	3679	5679	9679	17679	33679	65679	129679
Situation 2 (ms)	5649	9649	17649	33649	65649	129649	257649	513649

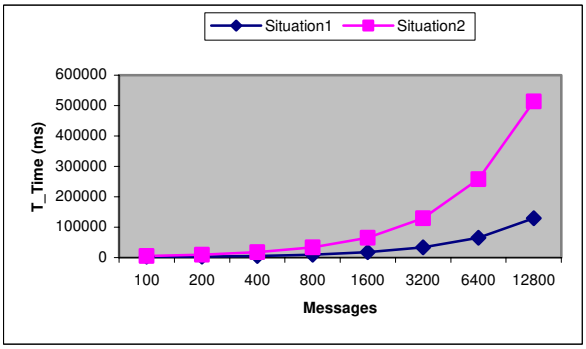

Figure 7. T_Time for Model 1 under NS-2 platform

The testing results under the JADE platform is very close the testing results under the NS-2 platform.

From the testing results, we know the situation where the onion nodes are distributed on different computers has much better scalability than the situation where the onion nodes are run on the same computer. On the other hand, the former also is much better than the latter from security and privacy protection perspective.

(2) Model 2

In the Model 2, we test the effect of the number of the onion nodes on the T_Time under the situation 1 and 2, and the scalability of the onion nodes from 3 to 7, where the sender user agent sends 100, 200, …, 12800 messages to the receiver user agent through the onion routing network respectively. Table 4, and Figure 8 depict the total processing time.

From the testing results, we see that situation 1 has much better scalability than situation 2. In addition, the onion path length only has very small impact on situation 1, but it has a large impact on the situation 2. Thus, the distributed system (i.e., the onion routing nodes are distributed on different computers) has much better scalability than the centralized system.

Table 4. T_Time for the model 2

Messages / Nodes		100	200	400	800	1600	3200	6400	12800
Situ. 1 (ms)	3	2534	3526	5539	9434	17066	32298	62551	123348
	4	2680	3672	5685	9580	17212	32444	62697	123494
	5	3564	4556	6569	10464	18096	33328	63581	124378
	6	4048	5040	7053	10948	18580	33812	64065	124862
	7	4666	5658	7671	11566	19198	34430	64683	125480
Situ.2 (ms)	3	4269	6934	12204	22765	43697	85560	168955	335998
	4	5415	9080	16350	30911	59843	117706	233101	464144
	5	7299	11964	21234	39795	76727	150590	297985	593028
	6	8783	14448	25718	48279	93211	183074	362469	721512
	7	10401	17066	30336	56897	109829	215692	427087	850130

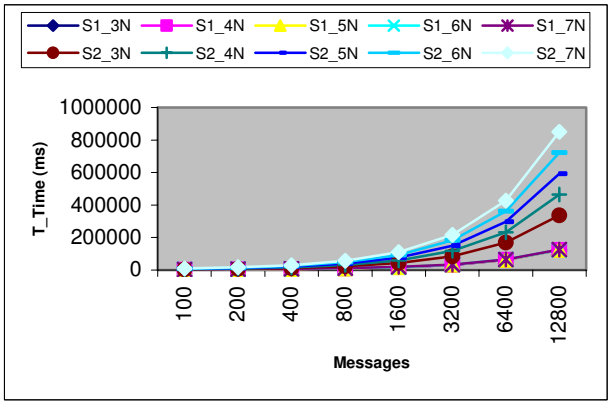

Figure 8. T_Time for the model 2

(3) Model 3

In the Model 3, we test the effect of the number of the user agents on the T_Time under the situation 1 and 2, the scalability of the sender user agents from 100 to 1000, and the scalability of the messages from 1000 to 8000 totally sent by the sender user agents.

During testing, there would be many cases that depend on whether or not the sender user agents use the same or different onion routing nodes. The best case is that each user agent uses different onion routing nodes for its secure and anonymous communications. The reason is, under this case, the variation of the number of the sender user agents does not have such an impact on the scalability of the onion routing network since the scalability relies on the receiver user agent. The worst case is that all sender user agents use the same onion routing nodes for their secure channels. Our testing is under the above worst-case scenario. Table 5 and Figure 9 depict the total processing time.

Table 5. T_Time for the model 3

Agents \ Messages		1000	2000	3000	4000
Situ. 1 (ms)	100	172755	182208	191641	201395
	500	824355	833808	843241	852995
	1000	1638855	1648308	1657741	1667495
Situ. 2 (ms)	100	199272	235445	271236	307178
	500	850872	887045	922836	958778
	1000	1665372	1701545	1737336	1773278

Agents \ Messages		5000	6000	7000	8000
Situ. 1 (ms)	100	210548	219972	229375	238699
	500	862148	871572	880975	890299
	1000	1676648	1686072	1695475	1704799
Situ. 2 (ms)	100	343159	379090	415213	451104
	500	994759	1030690	1066813	1102704
	1000	1809259	1845190	1881313	1917204

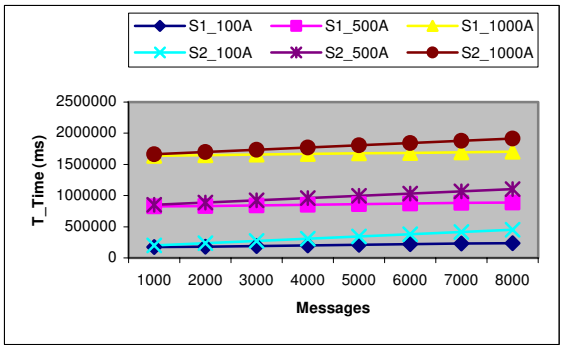

Figure 9. T_Time for the model 3

From the testing results, we know that, under the worst case, the number of the sender user agents has a huge impact on the scalability of the onion routing network. Thus, we suggest the system should choose the light workload onion nodes to build the secure channel in order to make the system more scalable.

6 Conclusions

Multi-agent systems will play important roles in the future information society, especially for e-business applications, in which security and privacy are considered to be the gating factors for their success. Thus security, privacy and trust mechanisms have become the desiderata for multi-agent applications. This paper tests the scalability of an alternate agent-based onion routing network that provides data protection against traffic analysis for multi-agent systems. Simulations show that the distributed onion routing system has much better scalability than the centralized system; the onion path length only has very small impact on the scalability of the distributed system but it has a large impact on the scalability of the centralized system; the balance of workload of the onion routers also has a huge impact on the onion routing system scalability.

Acknowledgements

We would like to thank the Communications Security Establishment of Canada for their support towards our Security and Privacy R&D program, and our IST-EU Fifth Framework Project, Privacy Incorporated Software Agent (PISA), partners [9].

References

[1] L. Korba, R. Song, and G. Yee, "Anonymous Communications for Mobile Agents", Proc. MATA'02, LNCS, Vol. 2521, pp. 171-181, 2002. NRC 44948.

[2] JADE -- Java Agent Development Framework. http://sharon.cselt.it/projects/jade/.

[3] Network Simulator. http://www.isi.edu/nsnam/ns/

[4] D. Goldschlag, M. Reed, and P. Syverson, "Onion Routing for Anonymous and Private Internet Connections", Communication of the ACM, Vol.42, No.2, pp. 39-41, 1999.

[5] D. Goldschlag, M. Reed, and P. Syverson, "Hiding Routing Information", Proc. Information Hiding: First International Workshop, LNCS, Vol. 1174, pp. 137-150, 1996.

[6] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connections and Onion Routing", IEEE Journal on Selected Areas in Communications, Vol.16, No.4, pp. 482-494, 1998.

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A Method For Obtaining Digital Signatures and Public-key Cryptosystems", *Communications of ACM*, Vol.21, No.2, pp. 120-126, 1978.

[8] Advanced Encryption Standard. FIPS 197, USA, Nov 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[9] PISA web site: http://pet-pisa.openspace.nl/.