# Collective Intelligence for Anonymous Systems

Rodolfo Leonardo Sumoza Matos[1], Ana Lucila Sandoval Orozco[1],
Luis Javier García Villalba[1], and Tai-hoon Kim[2,3]

[1] Group of Analysis, Security and Systems (GASS)
Department of Software Engineering and Artificial Intelligence (DISIA)
School of Computer Science, Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases s/n
Ciudad Universitaria, 28040 Madrid, Spain
E-mail: {rlsumoza, asandoval, javiergv}@fdi.ucm.es
[2] Department of Multimedia Engineering
Hannam University
133 Ojeong-dong, Daedeok-gu
Daejeon, Korea
E-mail: taihoonn@hannam.ac.kr
[3] Department of Information Technologies
Global Vision School Australia (GVSA)
20 Virgina Court, Sandy Bay
Tasmania, Australia
E-mail: taihoonn@gvsa.asia

**Abstract.** In this paper we propose to use some of the tools provided by the Distributed Artificial Intelligence (DAI), in particular Artificial Ant Colony Systems, building anonymous systems that have the virtue of having acceptable levels of Anonymity at a low cost. This cost refers to the performance criteria typically used in the process of routing telecommunications systems, such as response times (latency), the consumption of network resources, among others.

## 1 Introduction

To preserve privacy on each person's data who participate in interaction network, such as the Internet, we must to use tools that are capable of providing protection against some types of attack. The attacks in this particular study case are intended to get (without authorization) users' "private information", including their own identity. For this type of attack have been proposed several ideas to help establish certain levels of Anonymity, which in most cases have tended to undermine the communications' performance. This still is an open problem: the anonymous systems still need to ensure the Anonymity at low cost (low response times, low resources consumption, usability of the system, etc.), this is to have *efficient Anonymity.* This paper presents a first approach to Distributed Artificial Intelligence to this branch of Information Technologies Security, that is, it intends to delegate the responsibility to achieve efficient Anonymity levels to the Distributed Artificial Intelligence, we propose to use Artificial Ant Colony systems.

## 2 Artificial Systems Ant Colony in Anonymity

Considering the ideas proposed for probabilistic Anonymity systems [1][2][3][4], and Artificial Ant Colony Systems' features used in telecommunications networks [5][6][7], this proposal is based on select messages' routes in a probabilistic way, using the probabilities set by mobile adaptive agents (the ants). These routes, having probabilistic components may include, depending the network parameters' configuration, certain controlled levels of Anonymity, in this way, we could have "intelligent control" on generated response times and we could have "intelligent control" on another indexes that they can be incorporated, such as resource consumption (load balancing).

We propose *mimic* real messages to agents, that is, each message has the same structure as the ants, and the only difference between them lies in the message payload, these mimic messages are encrypted with the destination node's public key. To match their sizes, we propose to use a single size for each agent, including the data structure to stores information to update the tables at each node, plus useless filler and the destination's public key encryption. Each message has the same size as the agents, each one is fractionated or filled, and the the message's payload is sent encrypted with the the destination node's public key. Each message is re-assembled at the destination node, using a numbering sequence established in the sending node. To have the messages the same structure that ants, they also contribute to the routing tables update, thus the attackers can't distinguish between the ants and the real messages. In this way, we can compare the messages with the ants having the task of loading the food into the nest, for this reason there are two types of ants in our system, *the scouts and the load* both without apparent differences.

We use an encryption layers strategy, so each node that an ant visits encrypts information related to the previous node with a symmetric encryption technique involves only each previously node key and to reach each destinations, including the final, we can log only the previous node, and not the entire sequence to the origin. To do the reverse route, the node sends final response to the previous node, and it decrypts the layer that contains the node information before him, and so on until the initial node (the sender).

To optimize the performance criteria typically used in routing systems, while achieving increased levels of Anonymity, we must to set properly the update routing tables' rules. To do this, every time an ant moves from one place to another, update the routing table. To enhance the route's probability, it's selected based in performance criteria.

The following steps show the process:

**A.** We consider a system of $N$ nodes forming a P2P network (such as Gnutella or other with similar characteristics), along with their servers (bootstrap).

**B.** Sets the parameters' values used, like uniformity index. In cases where you consider other performance criteria involved in the calculation, are initialized in this step.

**C.** Each participating node requests the list of other nodes to one or more servers in the P2P network. This list contains their public key.

**D.** The routes tables are initialized with probability $1/M$. $M$ depends on the number of neighbors each node has.

**E.** The system is represented by a graph forming the solution space that will be traveled by the ants.

**F.** The following procedure is repeated on the graph until reach a stable solution:

  **1.** Is placed $m$ scout ants in each node.

  **2.** For each $N-1$ places from every node in particular, are sent $m$ scout ants that choose the next hop (neighbor node) using the transition probabilities of the routing table.

  **3.** Routing tables are updated.

**G.** When a node sends a message anonymously, it encrypts that with the recipient's public key and place a data structure similar to the scout ants, ie, creates a *load ant*. Each one carries a message part, which is split in order to match its size with the scout ant. Each fragment of the message contains a sequence number.

**H.** For each ant's jump, the intermediate node encrypt the previous node's identity with its private key.

**I.** When a load ant reaches the end node, and all the others load ants have reached, it is possible to complete the original message is decrypted with its private key, and re-assembled it using the corresponding sequence numbers.

**J.** To send the reply message, the end node uses the return path encrypted in layers.

## 3 Conclusion

It is proposed to implement in a distributed P2P System based probabilistic Anonymous Artificial Ant Colony Systems. To do that we can use a set of participating nodes as potential routers of anonymous messages. The routes for sending messages are constructed based on the strategies proposed for telecommunications systems that optimize performance criteria through the use of *Artificial Ant Colony Systems.* Once routes are created, Anonymity is achieved by selecting a probabilistic message routes and through the use of encryption in layers down the route of return or response.

## Acknowledgements

This work was supported by the Ministerio de Industria, Turismo y Comercio (MITyC, Spain) through the Project Avanza Competitividad I+D+I TSI-020100-2011-165 and the Agencia Española de Cooperación Internacional para el Desarrollo (AECID, Spain) through Acción Integrada MAEC-AECID MEDITERRÁNEO A1/037528/11. Rodolfo Sumoza is also supported by the Programme Al$\beta$an, the European Union Programme of High Level Scholarships for Latin America, scholarship No. E07D401826VE. This work was also supported by the

Security Engineering Research Center, granted by the Ministry of Knowledge Economy (MKE, Korea).

## References

1. D. L. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,” *Communications of the ACM*, vol. 24, pp. 84–90, February 1981.
2. G. Danezis, R. Dingledine, and N. Mathewson, “Mixminion: Design of a Type III Anonymous Remailer Protocol,” in *Proceedings of the Symposium on Security and Privacy*, pp. 2–15, may 2003.
3. C. Diaz and A. Serjantov, “Generalising Mixes,” in *Proceedings of the Privacy Enhancing Technologies Workshop*, no. LNCS 2760, pp. 18–31, March 2003.
4. R. Dingledine, N. Mathewson, and P. Syverson, “Tor: the second-generation onion router,” in *Proceedings of the 13th conference on USENIX Security Symposium*, vol. 13, (Berkeley, CA, USA), pp. 21–21, 2004.
5. G. Di Caro and M. Dorigo, “AntNet: Distributed Stigmergetic Control for Communications Networks,” *Journal of Artificial Intelligence Research*, vol. 9, pp. 317–365, December 1998.
6. T. White, B. Pagurek, and F. Oppacher, “Connection Management using Adaptive Mobile Agents,” in *Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications*, pp. 802–809, 1998.
7. R. Schoonderwoerd, J. L. Bruten, O. E. Holland, and L. J. M. Rothkrantz, “Ant-Based Load Balancing in Telecommunications Networks,” *Adaptive Behavior*, vol. 5, pp. 169–207, September 1996.