ARGUMENTATIVE NEGOTIATIONS WITH ANONYMOUS INFORMER AGENTS

Javier CARBO, José MOLINA and Jorge DAVILA

Introduction

Internet brings together people geographically and culturally unrelated to each other. This is one of the most remarkable features of electronic communities. In such context there is an extended sense of anonymity where trust and confidence might take place easier than in real life. Information Agencies may benefit from this feature of electronic communication in their endeavour to acquire secret information from previously unknown sources.

All this can be achieved through the use of autonomous software agents. However, the success of agents has not met the expectations. Among the possible reasons, we could mention the fear of users of being cheated, and of revealing unconsciously their personal opinion and preferences.

Users would feel comfortable delegating their duties to agents providing the behaviour of these agents exhibits intelligence, in other words, if the agents act rationally and could justify their decisions. Intelligence in negotiation is used to consider and evaluate offerings according to the particular preferences of the user. Nevertheless, success in negotiations does not depend only on the details of each offering. A certain number of arguments can be used to persuade the other party in the negotiation.

In security and military scenarios, the information that could be collected about an informer has a strategic value. For that reason, informers should avoid revealing unnecessary information, and a certain level of ambiguity is required. They can achieve it if they could reason with arguments and at the same time keep the anonymity of the informer.

Negotiations take place with the aim to persuade potential informers offering certain compensation (money, new identity, etc.). Agents may play a relevant role in this process since the potential informer would be able to negotiate in a rational and quick manner with several intelligence agencies at a time and a customised procedure for this could be devised.

Previous work on negotiation

Negotiations take place by the exchange of messages that aim at reaching an agreement satisfactory to both parties. Negotiations have been extensively studied in Game Theory.[1] The major issues in any negotiation are protocols and strategies.[2] Protocols rule the communication acts allowed at each moment of a negotiation. They should be public and accepted previously by both parties. Strategies rule the particular behaviour of each agent in a negotiation. They are private because they have to reflect the personal preferences of the user represented by the agent.

Game Theory assumes that the negotiating parties have complete knowledge and total rationality. The former means to know the preferences and beliefs of all the participants, the latter means the ability to reproduce the computations of any other participant. When we study negotiations from an agent-mediated perspective,[3] these two assumptions are too restrictive, especially in open and dynamic environments of heterogeneous – and possibly malicious – agents.[4].

The alternative provided by the adoption of software agents is based on a shared ontology of universally accepted terms in the domain;[5] only the protocols are publicly known, and the strategies are not optimal but computed in real time. So the protocol has a strong influence on the strategies adopted by the agents.[6]

The protocols are characterised by their cardinality, the environment, the negotiation issues, the temporal requirements, and the attitude of the participants.[7] These parameters establish the space of possible modes of acting. The larger the negotiation space, the more probable is the agreement. At the same time, this entails an increase in communication and computational costs. Considering these characteristics, different types of negotiation processes can be distinguished.

Among them, auctions have become the most popular type of electronic negotiation. They are usually focused on a single issue (price), with cardinality 1-to-n and a very complex and predetermined interaction. The number of alternatives that can be considered is very limited; hence the results of the negotiation are restricted.[8] Some researchers do not regard auctions as a negotiation.[9] Further, simple protocols, such as Contract Net, have also been proposed.[10] Here, an agent could simply accept or reject totally the offering of the merchants. Provided the user agent is able to propose counter-offerings, a greater level of sophistication can be achieved.[11]

However, auctions are very different from the daily bargaining at markets. Most people are not familiar with their rules. If agents intend to reflect the real behaviour in a society, then a human-like negotiation would be needed.[12] Humans explain and deliberate rational arguments to persuade the other party to improve its offering. This is often called persuasive argumentation in negotiation.[13] These arguments are represented with illocutions. Researchers in psychology have studied several illocutions involved in persuasive negotiations, for instance threats, rewards, and appeals.[14] These types of arguments were applied to the domain of labour negotiations by Sycara [15] and formalised in the works of Sierra *et.al.* [16] and Kraus.[17]

Security Services and Mechanisms

The security architecture of communications considers the following services achieved by cryptographic mechanisms: privacy, authentication, non-repudiation, integrity, and access control.[18]

1. Privacy provides the confidentiality of data exchange between entities. An encryption algorithm can provide this protection, making it computationally impossible for unauthorised users to access the information.
2. Authentication ensures that an entity is not supplanted by another. When a digital signature is used for providing authentication, then it is known as "strong authentication".
3. Non-repudiation can be provided by the source or by the destination in communication. In the first case, non-repudiation of sending, the sender of the message cannot repudiate its emission. On the other hand, non-repudiation of receipt implies that the receiver of the message cannot deny getting it.
4. Integrity supposes the detection or prevention of the unauthorised modification of the information. This service is aimed to ensure that the information is correct and complete.
5. Access control is frequently confused with the authentication service. However the access control is in charge of providing the appropriate privileges to the users.

From the group of cryptographic mechanisms used to provide such services, we describe the general properties of symmetric and asymmetric encryption, and hash functions. Interested readers can gather more information on these issues in Schneider's book.[19]

Symmetric (also called conventional) encryption has been largely used from the very beginning of cryptography. This type of ciphering provides balance between security and performance. However, it is necessary that the parties involved agree on a secret key through a secure channel. This is a clear limitation of this type of encryption due to the fact that in open and populated systems it is not an easy task to establish secure channels between parties that do not know each other.

On the other hand, asymmetric encryption relies on a pair of related keys, one of them is secret (only known by the owner) and the other is public (which is known, ideally, by everybody). The private key is used to decrypt (or sign), while only the public key can encrypt (or verify a signature).

The main advantage of asymmetric cryptography compared to symmetric cryptography is that it does not require a secure channel to exchange keys. An entity can get privacy of its messages just ciphering those messages with the public key of the destination entity. In this way, only the owner of the private key will be able to decrypt such messages.

Although slower than symmetric encryption, public key cryptography is preferable when dealing with very populated systems. However, every asymmetric encryption scheme needs a complete infrastructure to certify public keys and to protect the private keys. This infrastructure, denoted PKI (Public Key Infrastructure), involves a considerable number of resources that sometimes are not affordable by information systems. In other cases the investments needed to implement a PKI cannot be outweighed by the benefits that can be obtained. In such cases the asymmetric cryptography is not used and, therefore, other cryptographic mechanisms – with lower cost – are chosen.

A hash function is a mathematical transformation that takes as input a set of bits of variable length and computes a short fixed-length output. This output has the important property that there is no other way to find what input produced it but the one of trying all possible messages. This feature of hash functions is used in some micro-payment schemes (such as Payword) to achieve origin's authentication by establishing a link between consecutive hash values, and the first one was digitally signed. [20] This approach is an example of how hash functions can be used to reduce the number of public-key operations and, therefore, increase the efficiency at the expense of relaxing security. In a similar manner, our system will take advantage of hash functions, this way reducing the computational cost of ensuring security.

The Proposed Scheme of Negotiation

We intend to use informer agents that announce the knowledge of relevant secrets and that persuade intelligence agencies to improve their offering. In order to allow elaborated negotiations, the space of negotiation will be very open. To this end, we propose an extremely simple protocol: a sequence of offerings and argumentation-based counterproposals. The protocol follows the execution cycle described below:

1. The informer agent presents its credentials showing the knowledge of a relevant secret, but without revealing it.
2. The intelligence agency verifies the existence of such knowledge, and then it makes an offering to the informer agent.
3. The informer agent may then reject the offering sending a counterproposal with arguments to persuade the governmental agent. These arguments would take the form of rewards, appeals and threats. The counterproposal may also suggest what the agent expects to be improved.
4. Next, the two agents exchange offerings and counterproposal-based rejections sequentially.
5. Negotiation ends when the informer agent accepts the offering (an agreement is reached), or when any of the participants withdraws from the negotiation.

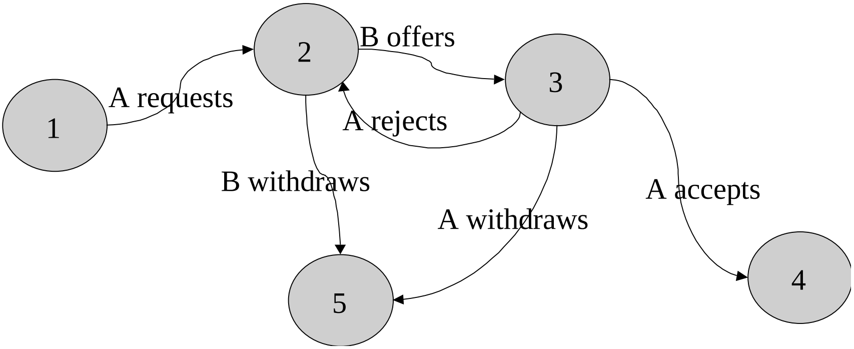

Figure 1: State Diagram of the proposed negotiation protocol

In order to reflect the expressiveness of human bargaining, each message has an illocution associated with the Speech Act theory.[21] These are: request, offer, accept, reject, and withdrawal. They will be codified using KQML (Knowledge Query and Manipulation Language).[22]

Proving the knowledge of secrets

The first step in negotiation is not trivial. We want an informer to present himself (herself) showing the knowledge of a certain secret without revealing the details of this secret. If the informer furnishes some information about the secret, it will not be fair due to the fact that exactly the secrecy of the information is the goal of negotiation, while, in response, the destination agent is not committed at all. In order to avoid such a disadvantage, we would like to protect the knowledge of the details regarding the secret information.

When the verification of the knowledge may be shown using algebraic properties, these requirements are analogous to the problems known as *two-party secure computations*. In them, both parties 1 and 2 know the definition of a function $f(x, y)$. Each party knows just only certain information, a_i, but not the information known by the other parties, $a_j \forall j \neq i$. So, both parties want to know the output of the function $f(a_1, a_2)$ without revealing much information about their own secrets.

For example, Yao [23] applied public key encryption in a well known example of this particular problem: the millionaires problem, in which two players want to know who is richer, but they do not wish to disclose the exact amounts they own. Another proposed domain of application is voting scenarios were votes are secrets and some participants have veto ability.

However, the use of this technique is very limited. In these computations, the security of the solutions relies on certain algebraic properties that the adopted encryption scheme maintains. These encrypted outputs are homomorphic with the inputs, so they partially preserve the multiplicative group of operations (associativity, complementation, neutral element). This common algebraic structure is used to verify the existence of certain properties of the inputs without revealing them.

Previous work of the authors of this paper has presented a way to compute similarity between subjective shopping preferences without revealing the purchasing profile.[24] In them, we have applied the millionaires' problem to the four squares of the corresponding trapezium that represents a fuzzy set. Based on this idea, we could define a variant of a voting scheme where some questions to certain secrets are posed. Some of them will be known by the intelligence agency, other secrets are desirable to uncover. All the parties will know how many questions were posed by the other party, and how many of the answers coincided. As the secrets that form the questionnaire are proposed by both parties, the output of the function will give a fuzzy idea of the relevance and sincerity of the potential informer. The interpretation of such uncertain information will help intelligence agencies to estimate the quality of the potential informer.

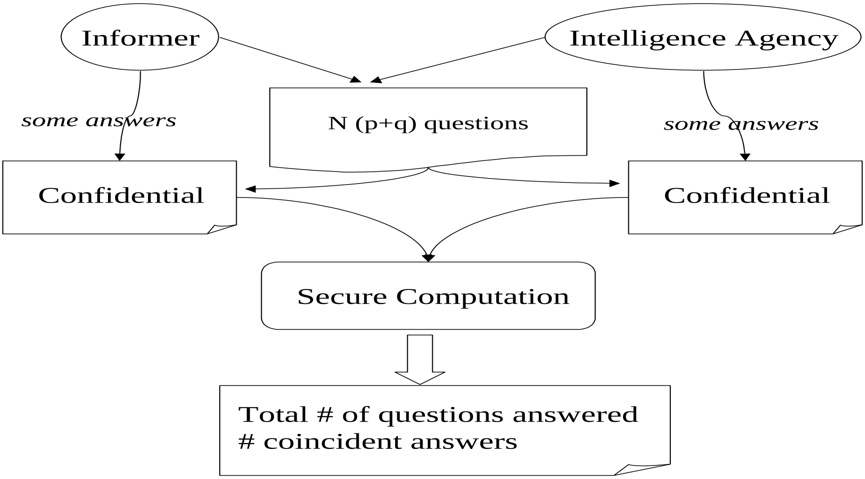

Figure 2: Sample introduction of informers.

Exchanging arguments

The attention in persuasive negotiations is focused on the representation of the arguments which support the counterproposals. In this paper we describe a subset of the possible rational arguments in negotiations of secrets between an informer and an intelligence agency.

One of the most frequently used arguments in such real-life negotiations are the threats of withdrawing from the negotiation. The threats, called ultimatums, are arguments of the type “take it or leave it.” Deadline Time could be represented in two different ways: as a temporal limit, or as the number of messages to be exchanged in advance. Urgency would represent a critical factor in the strategy of negotiation. We can represent this argument as a threat by:

threat $(a, b, \varepsilon, [not]\ \psi, t)$,

where *a* and *b* are agents, *ε* represents the desired improvement of the offering, *ψ* stands for the withdrawal used by agent *a* to threaten agent *b* at time *t*. This withdrawal would take place unless agent *b* accepts the improvements detailed in *ε*.

We propose another argument that is commonly used in such type of negotiations: possible rewards for revealing better secrets in the future. In other words, informer agents would try to persuade the intelligence agency demonstrating their quality as informers. The agency would estimate useless past secrets known by informer in order to compute how much the offering improvement could be rewarded in the future. The next illocution would help us represent such an argument:

reward $(a, b, \varepsilon, \psi, t)$,

where *a* and *b* are agents, *ε* represents the desired improvements of the offering, *ψ* stands for the proofs of knowledge of other secrets revealed by agent *a* before time *t*. The privacy of the related secrets may be achieved by the secure computations mentioned above. And, finally, these proofs should be considered as a reward if agent *b* would accept *ε*.

Finally, we also propose an argument useful for introducing competence among intelligence agencies, as additional reward to the informers. An informer agent could appeal to the offering of another intelligence agency, demanding an improvement in the offering at least as good as the offering of the other agency. This argument can be represented by the following illocution:

appeal $(a, b, \varepsilon, \varphi, t)$,

where *a* and *b* are agents, *ε* represents the desired improvements of the offering, *φ* stands for the offering received from another intelligence agency. An informer agent *a* would send at time instant *t* the offering from a third party to intelligence agency *b* in order to support the desired improvements contained in *ε*.

Achieving anonymity

Due to the secret nature of the information, informer agents will probably desire anonymity until an agreement is not yet reached, and while negotiation is still in progress.

Appealing anonymously to the offerings from other intelligence agencies entails certain relevant security problems:

1. The intelligence agency should be able to verify the authenticity and the integrity of such offering without asking directly the source of such offering.
2. Since possible improvements depend on the ownership of the offerings from other intelligence agencies, an informer should be able to show that such offerings belong to him/her, and no third party may eavesdrop them in order to use them inappropriately in other negotiations.
3. Besides hiding the real identity of the informer in each of the offerings, the proofs of ownership may not be linked. However, when the informer accepts the offering from an intelligence agency, this agent should reveal the real identity of the informer showing a verifiable link between such identity and each of the proofs of ownership of offerings used during the negotiation.

The first of the requirements mentioned above can be easily satisfied through the digital signature (SK_{ia}) of the intelligence agency over the corresponding offering. These signed offerings might not be transferable if they include the identity public key of the informer (PK_{id}). However, such a solution will not satisfy the third requirement.

Therefore, we propose as an alternative to use of a different one-use key pair for each offering that has to be proved. The informer agent will generate locally such a pair of keys. The public-key (PK_{off}) will be included in the signed offering from the other intelligence agency. In this way, the informer agent will be able to use offerings from other intelligence agencies by showing the knowledge of the corresponding private key (SK_{off}) without revealing it. These processes are usually called *zero-knowledge proofs*. One party may show the knowledge of such private key, because it shows the ability to compute certain operations that strongly require the knowledge of the factorisation of that key pair. Then the offerings from the agencies can not be transferred, because even when the agreement is reached, the other party does not know the private key of the offering, and therefore, it will not be able to eavesdrop such offerings. The problem here is that the computational cost of generating, keeping and encrypting/decrypting with asymmetric ciphering may not be affordable.

A faster alternative is to use one-way hash functions to show afterwards the ownership of the offerings. Such offerings should include the hash function of a random seed (large enough). The one-way nature of such functions will make it very difficult to compute the reverse process. This alternative satisfies the third requirement, but once the agreement is reached, and, therefore, the random seed is shown to the intelligence agency in order to proof the ownership of such offering, that intelligence agency may freely eavesdrop such proofs in future negotiations. This circumstance hinders the satisfaction of the second requirement, so the offerings should include also a link between the real identity of the informer and the large random number used as input to the hash function.

Therefore, in the beginning of each negotiation, the informer agent will send a certificate linking the input of the one-way function with the real identity public key together with the computed hash output. It will take the following form:

Hash (*random_input*), {*PK*$_{id}$, *random_input*} encrypted with SKid

When negotiations succeed, such a link will be revealed when the real identity of the informer (Public Key of the informer) will be known and the authenticity of the offering may be verified but not eavesdropped (due to the inclusion of such certificate in the offering).

Figure 3 summarises the requirements that each alternative meets in a graphical way.

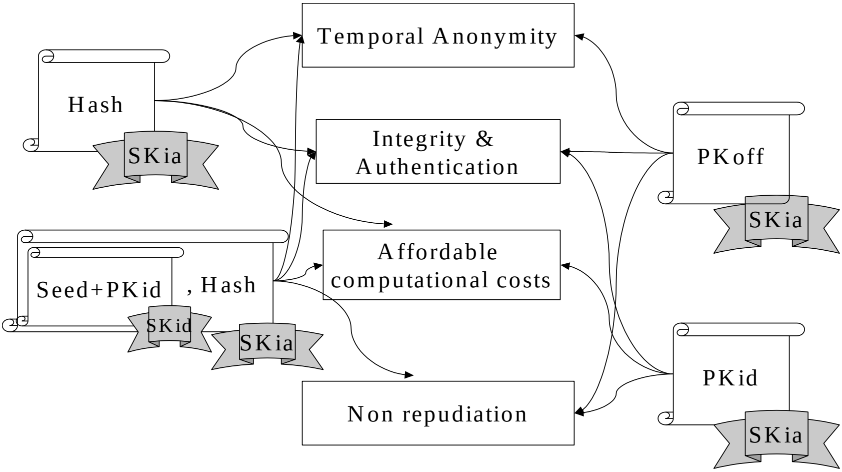

Figure 3: Overview of the proposed alternatives for achieving anonymity.

The inclusion of the identity public key (PKid) satisfies integrity, non-repudiation, authentication, and it may be affordable. The incorporation of an one-use-key pair for each offering (PKoff) satisfies anonymity but the implementation costs may become unaffordable. Nevertheless hash functions apparently solve this problem, but at the cost of sacrificing non-repudiation. Finally, our proposal satisfies all the requirements.

Conclusions

The negotiation protocol presented in this paper imposes few restrictions on its execution, and the space of negotiation is very open. Although it breaks the symmetry between the parties, informers would feel more comfortable if their own agents were leading the negotiation.

Intelligence agencies may have much more computational and storage capacity than informers. This circumstance may unbalance any negotiation, and therefore a certain level of anonymity is intended to diminish this disadvantage.

We have also studied how to prove certain knowledge without revealing the corresponding details, and how to preserve anonymity during negotiations when arguments such as past payoffs and offerings from other intelligence agencies are available.

Our proposal tries to make the negotiation dialogue more human through arguments commonly used in real-life negotiations; it also introduces competence among intelligent agencies and among informers. Further, our negotiation model intends to protect the interests of informers using secure computations, chains of hashes, etc. All these issues are tackled by our approach in a satisfactory manner.

Notes:

[1] J. Von Neumann and O. Morgenstern, *The Theory of Games and Economic Behaviour* (Princeton University Press, 1944).

[2] K. Binmore, *Fun and Games. A Text on Game Theory* (Lexington, MA: D.C. Heath, 1992).

[3] J. Rosenchein and M. Genesereth, "Deals among rational agents," in Proceedings of the International Joined Conference on Artificial Intelligence (1985): pp. 91-99.

[4] K. Binmore and N. Vulkan, "Applying game theory to automated negotiation," *Netnomics* 1-9 (Baltzer Science Publishers BV, 1999).

[5] T.R. Gruber, "The role of common ontology in achieving sharable, reusable knowledge bases," in *Proceedings of the 2nd International Conference on Principles of Knowledge Representation and Reasoning*, (Morgan Kauffman, 1991).

[6] J. Rosenchein and G. Zlotkin, *Rules of Encounter: Designing conventions for automated negotiation among computers,* (MIT Press, 1994).

[7] H. Raiffa, *The Art and Science of Negotiation*, (Cambridge, Mass.: Harvard University Press, 1982).

[8] Sandholm and Lesser, "Issues in automated negotiation and electronic commerce," in *Proceedings of the International Conference on MultiAgent Systems ICMAS'95*, (1995).

[9] J. Broersen, M. Dastani and L. van der Torre, "Levelled commitment and trust in negotiation," in *Proceedings of the Autonomous Agents 2000*, Workshop on Deception, Fraud and Trust in Agent Societies, (Barcelona, 2000).

[10] R.G. Smith and R. David, "Frameworks for cooperation in distributed problem solving," *IEEE Transactions on Systems, Man and Cybernetics* 11, 1 (1981): 61-70.

[11] C. Sierra, N.R. Jennings, P. Noriega, S. Parsons, "A framework for argumentation-based negotiation," *Intelligent Agents IV*, in *Lecture Notes in Artificial Intelligence*, no. 1365 (Springer, 1997), pp. 177-192,

[12] Gasser, "Social conceptions of knowledge and action: DAI foundations and open systems semantics," *Artificial Intelligence*, 47: 107-138.

[13] S. Parsons and N.R. Jennings, "Negotiation through argumentation," in *Proceedings of the Second International Conference On Multiagent Systems ICMAS'96*, (Kyoto, Japan, 1996): pp.267-274.

[14] M. Karlins and H.I. Abelson, *Persuasion*, (London, UK: Crosby Lockwood, 1970).

[15] Katya P. Sycara, "Persuasive argumentation in negotiation," *Theory and Decision*, 28 (1990): 203-242.

[16] Sierra, Jennings, Noriega, and Parsons, "A framework for argumentation-based negotiation."

[17] Kraus, "Reaching agreements through argumentation: A logical model," in *DAI Workshop'93*, (1993): pp.233-247.

[18] ISO 7498-2 1989 *ISO/IEC 7498 Security Architecture, part 2.* Open System Interconnection Reference Model. (1989).

[19] B. Schneider, *Applied Cryptography: Protocols, Algorithms and Source Code in C,* 2nd Ed., (New York: John Wiley and Sons, 1996).

[20] R. Rivest and A. Shamir, "Payword and Micromint: two simple micro-payment schemes," in *Proceedings of 1996 International Workshop on Security Protocols*, ed. Mark Lomas, *Lecture Notes in Computer Science* no. 1189, (Springer, 1997), pp.69-87.

[21] J. Searle, *Speech Acts*, (Cambridge University Press, 1969).

[22] R. Neches, R.S. Patil, R.E. Fikes, P.F. Patel-Schneider, D. McKay, T. Finin, and T. Gruber, "DARPA Knowledge Sharing Effort," in *Proceedings of the Annual International Conference on Knowledge Acquisition*, (Cambridge, MA, October, 1992).

[23] A. Yao, "Protocols for secure computations," in *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science*, (1982): pp. 80-91.

[24] J. Carbo, J.M. Molina, and J. Davila, "Privacy of Trust in Similarity Estimation through Secure Computations," in *Proceedings of the International Workshop on Trust and Privacy in Digital Business, 13th International Conference on Database and Expert Systems Applications*, (Aix-en-Provence, 2002).

JAVIER CARBO is currently lecturer at the Computer Science Department of the Carlos III University of Madrid (SPAIN). He is with the Laboratory of Adaptive Complex Systems at the department. He has previously worked at the Artificial Intelligence Laboratory of the University of Savoie (FRANCE). He is currently finalising a Ph.D. on reputation and trust issues of agent-mediated electronic commerce. He obtained a Computer Science degree from the Politecnica University of Madrid in 1997. Mr. Carbo has published over 15 papers. He acts as a reviewer of IASTED international conferences on Artificial Intelligence. He has also acted as a session chair of the IEEE International Conference on Systems, Man and Cybernetics. He took part in an U.N. funded research project, two ESPRIT programs and other national projects. His interests are in automated negotiations, multi-agent systems, electronic payments and fuzzy logic. E-mail: jcarbo@inf.uc3m.es, Phone +34 916249105, Despacho 21B12, Depto. Informatica, Univ. Carlos III, Av. Universidad 30, Leganes 28911 Madrid (SPAIN)

JOSÉ M. MOLINA received a degree in Telecommunication Engineering from the Universidad Politecnica de Madrid in 1993 and a Ph.D. from the same university in 1997. He has worked in the Signal Processing and Simulation Group of the same university since 1992, participating in several national and European projects related to Radar Processing. In 1993 he also joined the Computer Science Department of the University Carlos III of Madrid, being enrolled in the Systems, Complex and Adaptive Laboratory performing research on soft computing techniques (NN, Evolutionary Computation, Fuzzy Logic and Multiagent Systems). He is author of more than 10 journal papers and 70 conference papers. His current research focuses on the application of soft computing techniques to security in e-commerce, information retrieval from web, problem solving in web domains, radar processing, air traffic control, etc. E-mail: molina@ia.uc3m.es, Phone +34 916249116, Despacho 21B15, Depto. Informatica, Univ. Carlos III, Av. Universidad 30, Leganes 28911 Madrid (SPAIN).

JORGE DAVILA received a degree in Chemistry from the Universidad Complutense de Madrid and a Ph.D. from the same university. In 1991 he joined the Computer Science Faculty of the Universidad Politecnica de Madrid, where he is teaching and researching in Cryptography and Information Security since then. From 1993 he leads the Cryptology Laboratory of the Faculty. E-mail: jdavila@fi.upm.es, Ph. +34 913366934, DLSIIS, Facultad de Informática, Univ. Politécnica, Campus de Montegancedo, Boadilla del Monte 28660 Madrid (SPAIN).