DOI: http://dx.doi.org/10.14201/0AQ02876983

DISTRIBUTION OF QUANTUM KEYS OVER COMMERCIAL NETWORKS

Iván García-Cobo

Universidad de Salamanca. Salamanca, Spain
ORCID: 0000-0002-9472-5613
ivangarciacobo@usal.es

Abstract: Modern cryptography – as it was conceived – is under a threat by the development of quantum mechanics applications. The abilities of quantum computers for solving complex mathematical problems, as a strong computational novelty, is the root of that risk. The main challenge is to find commercial exploits of quantum properties and developments, following these directions for both, theoretic and test tube environments.

This work proposes a pilot experiment that implements a quantum communication system on a commercial fiber optic network, covering an area of almost 100,000 km^2.

Keywords: modern cryptography; quantum cryptography; quantum key exchange; quantum key distribution; QKD.

1 Introducción

We can place the origins of computing as a modern discipline in the works of Sir Alan Turing. The exercise of mathematical and algorithmic abstraction led him to design knowledge as Turing's Machine: a formal device capable of solving any mathematical problem that could be represented by an algorithm [1-10].

One of the main theoretical challenges facing modern cryptography is its vulnerability to future quantum computers. According to Shor's algorithm [11-18], once quantum computers exist, most public key encryption algorithms can be compromised in linear time. This is a major problem, not only in terms of secure communication, but also in terms of protecting data – both future and present –.

To address the threats that quantum computing poses to classic cryptography, we can use applications of quantum mechanics itself to implement new solutions. Talking about encrypted communication, quantum cryptography allows us to design algorithms that, on the one hand, manage to overcome the limitations of classical physics and on the other hand, are not vulnerable to attacks from quantum computers. However, one of the main problems associated with such algorithms is the distribution of so-called quantum keys, given their physical properties.

There are numerous successful experiments on quantum communication over distances of up to 100 km^2 on fibre optic channels (e.g. [19-27]). However, trying to put a necessary realistic approach in a commercial implementation, distances below 50 km^2 ([28-35][1]).

The aim of this work is to propose a new way of creating a quantum key distribution network that allows providing service over a fibre optic network in a de-terminated territory. For this purpose, the fibre optic network of a commercial operator over the territory of Castilla y León has been studied. With this information, a methodology is proposed, based on grouping algorithms, that tries to minimize the number of quantum key repeaters over that specific territory, so that not only the distribution network is created, but also it is optimized.

In the case of a maximum distance of 35 km^2, it would be sufficient to use the available network by coupling 100 repeaters on it. This would guarantee secure communications using quantum encryption in Castilla y León, a territory that currently occupies 100.000 km^2.

2 Quantum communication protocol

For the explanation of the protocol, we will then use the traditional actors: Bob, Alice and Eve.

---

[1] Este dispositivo [4] permite intercambiar del orden de 20000 claves cuánticas en una hora

2.1 BB84

The BB84 protocol is considered the first quantum key distribution protocol. It was proposed by Bennett and Brassard in 1984 [36-45]. It uses quantum properties. This protocol uses four states and two alphabets, each with two states.

After the execution of the algorithm and once the key has been generated by BB84, Alice will use this key to encrypt her message. Later Bob will be able to decrypt the message with the shared key. The guarantee of the security of the use of the key lies in the fact that both its creation and transmission are based on the fundamentals of quantum mechanics.

The presence of a potential spy –Eve– could compromise the exchange of the key. However, the security of the protocol is that it uses two alphabets with non-orthogonal states – Eve cannot simultaneously measure the x and z polarization for the same qbit.

2.2 Practical example of protocol use BB84

By using modern cryptography and quantum we can apply this algorithm to an exchange of messages between Alice and Bob. We will use the Vernam cipher applied to the encoding and decoding of the message; while the BB84 protocol will be used for the creation and exchange of the secure key.

Alice will locate the clear message she wants to transmit and transcribe it as a sequence of 0 and 1. BB84 is used to generate a key the same size (or larger) as the message to be transmitted. To do this, Alice generates a random sequence of 0 and 1. They follow the rest of the steps of the BB84 protocol to exchange the key. Remember that the last step of the BB84 algorithm discards the values that have not matched [46-53].

Once both share a secure one-time key, the message is encrypted with that key by Alice and sent to Bob, who, upon receiving it, will perform the binary addition with the key previously transferred to him by Alice and will be able to discover the sent clear text.

3 Quantum Key Distribution

To build a network that connects all municipalities, a distributed network of repeaters must be designed. To make the distribution, a methodology based on grouping municipalities, through a k-medoids algorithm, is used. This algorithm will help, given a set of municipalities, to select those that are physically close to each other. Then, the algorithm will facilitate the selection of the most central municipality, within the set of nearby municipalities. This municipality will be considered as a candidate, within the set, to host a repeater. Finally, the methodology will try to connect the possible repeaters to each other to generate a distribution network.

This type of problem is similar to the problem of the traveller, where the optimal route has to be selected for a traveller who intends to travel to a certain set of places. In this case, «the traveller» would correspond to the set of quantum keys, and «the places» would correspond to the municipalities. The problem of the traveller is NP-complete [54-62], and it requires approximation methods in order to find local solutions.

3.1 Basic Network of Municipalities

When selecting municipalities as potential candidates for placing repeaters, it is important to take into account two factors: the selected municipality must have all the other municipalities in its group within the range of distances required in the quantum distribution, and the municipality representative of the group must have at least one other representative municipality within the distance limit in order to generate the distribution network.

3.2 Identification of Representative Municipalities

The way to address the problem of distributing quantum keys over a given population implies not only knowing the physical limits that communication between nodes establishes, but also specific methodologies that allow for the optimal placement of repeaters. For this second part, clustering is used, a technique known within unsupervised machine learning [63-70].

3.3 Repeater Network

In order to ensure that any municipality within the network can communicate with any other, it is necessary to establish a repeater network based on the representative municipalities selected in the previous step. This network will be defined as follows:

1. Each representative municipality shall be connected with all the municipalities in its cluster. In this way, all municipalities in the same cluster will be able to exchange quantum keys using the repeater. In the previous step it is guaranteed that the repeater is at a distance less than D from each municipality in its cluster.
2. Each repeater will connect to all repeaters in its environment within a distance of D. Thus, if more than one repeater is close to another, different routing can be used.

These criteria when creating the network not only facilitate better routing, but also make it easy to identify possible isolated regions of the network. In order to find these regions, it is sufficient to calculate the number of related network components. Formally, the network is a non-directed G network, divided into V-points, representing the municipalities, and E-points, representing those municipalities that are either within a cluster and connected to its repeater, or are repeaters at a distance less than D from each other. The number of related network components is calculated by estimation using random paths [71-81].

4 Experimentation

The experiment shown below measures the quality of the networks with respect to the number of repeaters. The limiting distance is considered as a parameter and is manipulated together with the number of repeaters.

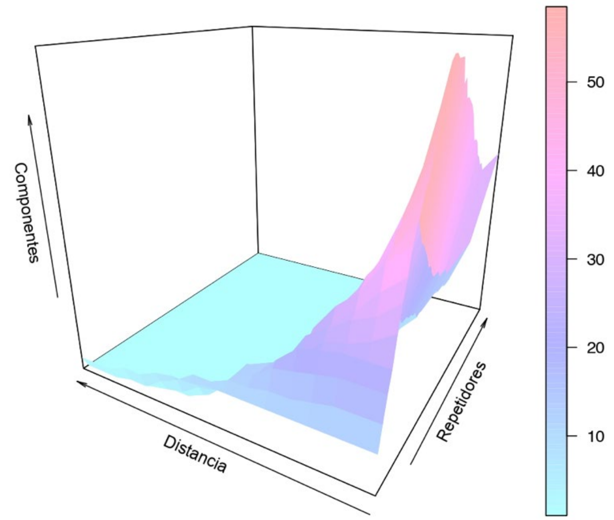

Figure 1. Display of the experimental results considering the two variables of the experiment: the limit distance of the repeaters (D) and the number of repeaters (k). The graph shows the number of connected components that the network has for different values of these parameters. It can be seen that the predominant value is 1 component in most cases, so the network would be connected.

Figure 1 shows the result of the experiment. It establishes a range of distances and a number of repeaters that varies between 20 and 100 km for the distances and between 10 and 250 for the repeaters [82-89]. The main goal of the experiment is to check at which points the complete network is reached. The lighter blue of the figures represents the lowest number of components, in these results, a single component. This means that the service can be provided to all municipalities without leaving any isolated ones. As you can see, the optimal distance values should be from 80 km in order to place the least number of repeaters possible (between 10 and 20), however, for distances around 40 km, about 100 repeaters should be enough to create the connected network.

5 Conclusion

The application of quantum to computing involves a paradigm shift. The move from classical computing to quantum computing is the starting point for finding solutions to historical problems that have long been unsolvable. It is necessary to strengthen the current communication systems by implementing algorithms resistant to such possible attacks while designing new applications of quantum to achieve secure communications faster and more efficient.

After showing the BB84 quantum key distribution (QKD) algorithm and referencing different tests in researchers' laboratories, it was found that it was necessary to implement a quantum key repetition system, since the maximum distance in practice at which the system could be made to work was relatively low. Together with this, we found the need for the designed system to be able to operate over a commercial (general purpose) fiber optic network.

An experiment has been designed to find the optimal way to distribute the repeaters to cover a wide area. Specifically, we have considered the area occupied by Castilla y León, an Autonomous Community of Spain. The municipalities that are the object of this experiment are those with 1000 or more inhabitants within the selected territory. The experimentation has served to show how the number of repeaters required varies according to the distance as well as the minimums necessary to cover the entire territory, interconnecting it in its entirety.

References

1. Bennett, C.H., Brassard, G.: Quantum Cryptography: Public Key Distribution, and Coin-Tossing. In Proc. 1984 IEEE International Conference on Computers, Systems, and Signal Processing. pp. 175–179 (1984). https://doi.org/10.1016/j.tcs.2011.08.039
2. Fröhlich, B., Lucamarini, M., Dynes, J.F., Comandar, L.C., Tam, W.W.S., Plews, A., Sharpe, A.W., Yuan, Z., Shields, A.J.: Long-distance quantum key distribution secure against coherent attacks. Optica 4 (1), 163 (1 2017). https://doi.org/10.1364/OPTICA.4.000163, http://arxiv.org/abs/1701.07252 http://dx.doi.org/10.1364/OPTICA.4.000163 https://www.osapublishing.org/abstract.cfm?URI=optica-4-1-163
3. Gobby, G., Yuan, Z.L., Shields, A.J.: Unconditionally secure quantum key distribution over 50km of standard telecom fibre. Electronics Letters 40 (25), 1603–1605 (12 2004). https://doi.org/10.1049/el:20045038, http://arxiv.org/abs/quant-ph/0412173 http://dx.doi.org/10.1049/el:20045038

4. IDQuantique: Cerberis QKD Blade (2015), https://www.idquantique.com/quantum-safe-security/products/cerberis-qkd-blade/
5. Larose, D.T., Larose, C.D.: Discovering knowledge in data: an introduction to datamining. John Wiley & Sons (2014)
6. Lawler, E.L.: The traveling salesman problem: a guided tour of combinatorial optimization. Wiley-Interscience Series in Discrete Mathematics (1985)
7. Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science. pp.124–134. IEEE Comput. Soc. Press (1994). https://doi.org/10.1109/SFCS.1994.365700, http://ieeexplore.ieee.org/document/365700
8. Turing, A.: On computable numbers. Proceedings of the London Mathematical Society 42 (1), 230–265 (3 1936). https://doi.org/10.2307/2268810, http://www.jstor.org/stable/2268810?origin=crossref
9. Von Luxburg, U.: A tutorial on spectral clustering. Statistics and computing 17 (4), 395–416 (2007)
10. Li, T., Sun, S., Corchado, J. M., & Siyau, M. F. (2014, July). Random finite set-based Bayesian filters using magnitude-adaptive target birth intensity. In 17th International Conference on Information Fusion (FUSION) (pp. 1-8). IEEE.
11. Rodríguez, S., Gil, O., De La Prieta, F., Zato, C., Corchado, J. M., Vega, P., & Francisco, M. (2010, May). People detection and stereoscopic analysis using MAS. In 2010 IEEE 14th International Conference on Intelligent Engineering Systems (pp. 159-164). IEEE.
12. Guillén, J. H., del Rey, A. M., & Casado-Vara, R. (2019). Security Countermeasures of a SCIRAS Model for Advanced Malware Propagation. IEEE Access, 7, 135472-135478.
13. Corchado, J. M. (1996). Artificial intelligence models: composed systems as a solution. In IEEE COLLOQUIUM ON KNOWLEDGE DISCOVERY. LONDON ENGLAND, UK.
14. Casado-Vara, R., De la Prieta, F., Rodriguez, S., Prieto, J., & Corchado, J. M. (2018, June). Cooperative Algorithm to Improve Temperature Control in Recovery Unit of Healthcare Facilities. In International Symposium on Distributed Computing and Artificial Intelligence (pp. 49-62). Springer, Cham.
15. Corchado, J. M. (1995). Hybrid cbr system for real-time temperature forecasting in the ocean. In IEEE COLLOQUIUM ON KNOWLEDGE DISCOVERY. LONDON, UK.
16. Corchado, J. M. (1995). A distributed recommendation system assos. In IEEE COLLOQUIUM ON KNOWLEDGE DISCOVERY. IEE, LONDON, UK.

17. Corchado, J. M. (1995). The use of kernel methods in cbr systems. In INTERNATIONAL CONFERENCE ON INTELLIGENT SYSTEMS. LONDON ENGLAND UK.
18. Corchado, J. M. (1995). Case based reasoning systems: automatic construction. In INTERNATIONAL CONFERENCE ON INTELLIGENT SYSTEMS. LONDON ENGLAND UK.
19. Casado-Vara, R., de la Prieta, F., Prieto, J., & Corchado, J. M. (2018, November). Blockchain framework for IoT data quality via edge computing. In Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems (pp. 19-24). ACM.
20. Gil, A. B., De la Prieta, F., & Rodríguez, S. (2011). Automatic Learning Object Extraction and Classification in Heterogeneous Environments. In Highlights in Practical Applications of Agents and Multiagent Systems (pp. 109-116). Springer, Berlin, Heidelberg.
21. Garcia, R. F., Rolle, J. L. C., Castelo, J. P., & Gomez, M. R. (2014). On the monitoring task of solar thermal fluid transfer systems using NN based models and rule based techniques. *Engineering Applications of Artificial Intelligence*, *27*, 129-136.
22. Di Mascio, T., Vittorini, P., Gennari, R., Melonio, A., De La Prieta, F., & Alrifai, M. (2012, July). The Learners' User Classes in the TERENCE Adaptive Learning System. In 2012 IEEE 12th International Conference on Advanced Learning Technologies (pp. 572-576). IEEE.
23. Mazuelas, S., Lorenzo, R. M., Bahillo, A., Fernández, P., Prieto, J., & Abril, E. J. (2010). Topology Assessment Provided by Weighted Barycentric Parameters in Harsh Environment Wireless Location Systems. IEEE Transactions on Signal Processing, 58(7), 3842–3857. doi:10.1109/TSP.2010.2047394
24. Prieto, J., Alonso, A. A., la Rosa, de, R., & Carrera, A. (2014). Adaptive Framework for Uncertainy Analysis in Electromagnetic Field Measurements. Radiation Protection Dosimetry. doi:10.1093/rpd/ncu260
25. Prieto, J., Bahillo, A., Mazuelas, S., Blas, J., Fernández, P., & Lorenzo, R. M. (2008). RTS/CTS mechanism with IEEE 802.11 for indoor location. Presented at the NAV08/ILA37, The Navigation Conference & Exhibition.
26. Prieto, J., Bahillo, A., Mazuelas, S., Fernández, P., Lorenzo, R. M., & Abril, E. J. (2012a). Self-Calibration of TOA/Distance Relationship for Wireless Localization in Harsh Environments. Presented at the 2012 IEEE International Conference on Communications (ICC 2012).
27. Prieto, J., Bahillo, A., Mazuelas, S., Lorenzo, R. M., Blas, J., & Fernández, P. (2009a). Adding indoor location capabilities to an IEEE 802.11 WLAN using real-time RTT measurements (pp. 113–119). IEEE Press. Retrieved from http://

dl.acm.org/citation.cfm?id=1689059.1689083&coll=DL&dl=GUIDE&CFID=647274630&CFTOKEN=45917612

28. Bullon, Juan, et al. «Manufacturing processes in the textile industry. Expert Systems for fabrics production.» ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 6.4 (2017): 15-23.
29. Souza de Castro, Lucas Fernando, Gleifer Vaz Alves, & André Pinz Borges. «Using trust degree for agents in order to assign spots in a Smart Parking.» (2017).
30. Moung, Ervin. «A Comparison of the YCBCR Color Space with Gray Scale for Face Recognition for Surveillance Applications.» ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal [Online], 6.4 (2017): 25-33.
31. Kethareswaran, V., & C. Sankar Ram. «An Indian Perspective on the adverse impact of Internet of Things (IoT).» ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 6.4 (2017): 35-40.
32. Cunha, Rafhael, Cleo Billa, & Diana Adamatti. «Development of a Graphical Tool to integrate the Prometheus AEOlus methodology and Jason Platform.» ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 6.2 (2017): 57-70.
33. Farias, Giovani Parente, et al. «Predicting Plan Failure by Monitoring Action Sequences and Duration.» ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 6.4 (2017): 55-69.
34. Vera, Jefferson Stewart Espinosa. «Human rights in the ethical protection of youth in social networks-the case of Colombia and Peru.» ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 6.4 (2017): 71-79.
35. Casado-Vara, R., Martin-del Rey, A., Affes, S., Prieto, J., & Corchado, J. M. (2020). IoT network slicing on virtual layers of homogeneous data for improved algorithm operation in smart buildings. *Future Generation Computer Systems*, *102*, 965-977.
36. Mateen, Abdul, et al. «Secure data access control with perception reasoning.» ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 7.1 (2018): 13-28.
37. Teixeira, Eduardo Porto, Eder Goncalves, & Diana F. Adamatti. «Ulises: A Agent-Based System For Timbre Classification.» ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 7.1 (2018): 29-40.
38. Van Haare Heijmeijer, Alexis, & Gleifer Vaz Alves. «Development of a Middleware between SUMO simulation tool and JaCaMo framework.» ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 7.2: 5-15.

39. Glaeser, Stefania da Silveira, et al. «Modeling of Circadian Rhythm under influence of Pain: an approach based on Multi-agent Simulation.» ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 7.2 (2018): 17-25.
40. Machón-González, I., López-García, H., & Calvo-Rolle, J. L. (2010, July). A hybrid batch SOM-NG algorithm. In The 2010 international joint conference on neural networks (IJCNN) (pp. 1-5). IEEE.
41. Ribeiro, Catarina, et al. «Customized normalization clustering meth-odology for consumers with heterogeneous characteristics.» ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 7.2 (2018): 53-69.
42. Becerril, Anahiby Anyel. «The value of our personal data in the Big Data and the Internet of all Things Era.» ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 7.2 (2018): 71-80.
43. Garcia, Ana Cristina Bicharra, & Adriana Santarosa Vivacqua. «ACoPla: a Multiagent Simulator to Study Individual Strategies in Dynamic Situations.» ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 7.2: 81-91.
44. Casado-Vara, R., Novais, P., Gil, A. B., Prieto, J., & Corchado, J. M. (2019). Distributed continuous-time fault estimation control for multiple devices in IoT networks. IEEE Access, 7, 11972-11984.
45. Jörg Bremer, Sebastian Lehnhoff. (2017) Decentralized Coalition Formation with Agent-based Combinatorial Heuristics. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal (ISSN: 2255-2863), Salamanca, v. 6, n. 3
46. Rafael Cauê Cardoso, Rafael Heitor Bordini. (2017) A Multi-Agent Extension of a Hierarchical Task Network Planning Formalism. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal (ISSN: 2255-2863), Salamanca, v. 6, n. 2
47. Enyo Gonçalves, Mariela Cortés, Marcos De Oliveira, Nécio Veras, Mário Falcão, Jaelson Castro (2017). An Analysis of Software Agents, Environments and Applications School: Retrospective, Relevance, and Trends. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal (ISSN: 2255-2863), Salamanca, v. 6, n. 2
48. Eduardo Porto Teixeira, Eder M. N. Goncalves, Diana F. Adamatti (2017). Ulises: A Agent-Based System For Timbre Classification. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal (ISSN: 2255-2863), Salamanca, v. 6, n. 2
49. Lucas Fernando Souza de Castro, Gleifer Vaz Alves, André Pinz Borges (2017). Using trust degree for agents in order to assign spots in a Smart Parking. ADCAIJ:

Advances in Distributed Computing and Artificial Intelligence Journal (ISSN: 2255-2863), Salamanca, v. 6, n. 2

50. Aversa, R., Petrescu, R. V., Akash, B., Bucinell, R., Corchado, J., Berto, F., ... & Petrescu, F. I. (2017). Kinematics and forces to a new model forging manipulator. American Journal of Applied Sciences, 14(1), 60-80.
51. Li, T., Sun, S., Bolić, M., & Corchado, J. M. (2016). Algorithm design for parallel implementation of the SMC-PHD filter. Signal Processing, 119, 115-127.
52. Corchado, J. M., Aiken, J., Corchado, E. S., & Fdez-Riverola, F. (2005). Evaluating the air–sea interactions and fluxes using an instance-based reasoning system. AI Communications, 18(4), 247-256.
53. Costa, Â., Novais, P., Corchado, J. M., & Neves, J. (2011). Increased performance and better patient attendance in an hospital with the use of smart agendas. Logic Journal of IGPL, 20(4), 689-698.
54. Rodríguez, S., de La Prieta, F., Tapia, D. I., & Corchado, J. M. (2010, June). Agents and computer vision for processing stereoscopic images. In International Conference on Hybrid Artificial Intelligence Systems (pp. 93-100). Springer, Berlin, Heidelberg.
55. Corchado, J. M., Corchado, E. S., & Pellicer, M. A. (2004, September). Design of cooperative agents for mobile devices. In International Conference on Cooperative Design, Visualization and Engineering (pp. 205-212). Springer, Berlin, Heidelberg.
56. Corchado, J. M., Laza, R., Borrajo, L., Yañez, J. C., De Luis, A., & Gonzalez-Bedia, M. (2003, July). Agent-based web engineering. In International Conference on Web Engineering (pp. 17-25). Springer, Berlin, Heidelberg.
57. Fdez-Riverola, F., & Corchado, J. M. (2003). Forecasting red tides using an hybrid neuro-symbolic system. AI Communications, 16(4), 221-233.
58. González-Briones, A., Prieto, J., De La Prieta, F., Herrera-Viedma, E., & Corchado, J. (2018). Energy optimization using a case-based reasoning strategy. Sensors, 18(3), 865.
59. Díaz, F., Fdez-Riverola, F., Glez-Peña, D., & Corchado, J. M. (2006, September). Using fuzzy patterns for gene selection and data reduction on microarray data. In International Conference on Intelligent Data Engineering and Automated Learning (pp. 1087-1094). Springer, Berlin, Heidelberg.
60. Koetsier, J., Corchado, E., MacDonald, D., Corchado, J., & Fyfe, C. (2004, June). Kernel maximum likelihood hebbian learning. In International Conference on Computational Science (pp. 650-653). Springer, Berlin, Heidelberg.
61. Pavón, J., & Corchado, J. (2004). Agents for the web. International journal of Web engineering and technology, 1(4), 393-396.

62. Fdez-Riverola, F., Díaz, F., Borrajo, M. L., Yáñez, J. C., & Corchado, J. M. (2005, August). Improving gene selection in microarray data analysis using fuzzy patterns inside a cbr system. In International Conference on Case-Based Reasoning (pp. 191-205). Springer, Berlin, Heidelberg.
63. Fernández-Riverola, F., & Corchado, J. M. (2003, November). Employing tsk fuzzy models to automate the revision stage of a cbr system. In Conference on Technology Transfer (pp. 302-311). Springer, Berlin, Heidelberg.
64. Corchado, J. M., & Aiken, J. (1998). Expert system for modelling water masses. In WORKSHOP ON DATA MINING. GLASGOW, SCOTLAND.
65. Corchado, J. M., & Aiken, J. (1998). Neuro-symbolic reasoning for real time oceanographic problems. In CONFERENCE ON DATA MINING. IEE, SAVOY PLACE, LONDON.
66. Corchado, J. M. (1998). Models for integrating artificial intelligence approaches. DOCTORAL CONSORTIUM ON KNOWLEDGE DISCOVERY AND DATA MINING. PAISLEY, UK.
67. Borrajo, M. L., Corchado, J. M., Yáñez, J. C., Fdez-Riverola, F., & Díaz, F. (2005, August). Autonomous internal control system for small to medium firms. In International Conference on Case-Based Reasoning (pp. 106-121). Springer, Berlin, Heidelberg.
68. Fdez-Riverola, F., Díaz, F., & Corchado, J. M. (2004, November). Applying rough sets reduction techniques to the construction of a fuzzy rule base for case based reasoning. In Ibero-American Conference on Artificial Intelligence (pp. 83-92). Springer, Berlin, Heidelberg.
69. Corchado, J., & Lees, B. (1998). Case based reasoning opportunities and technologies. In CONFERENCE ON KNOWLEDGE DISCOVERY. IEE, SAVOY PLACE, LONDON.
70. Corchado, J., & Lees, B. (1998). Artificial neural networks in pattern recognition: multicollinearity and heterocedasticity. In COLLOQUIUM ON KNOWLEDGE DISCOVERY. LONDON, UK.
71. Corchado, J., & Lees, B. (1998). An overview of intelligent frameworks. In COLLOQUIUM ON INTELLIGENT SYSTEMS. IEE, LONDON, UK.
72. Corchado, J. M., & Lees, B. (1998). Probis: Modelling intelligence with hybrid systems. In WORKSHOP ON DATA MINING. University of GLASGOW, SCOTLAND, UK.
73. Corchado, J. (1998). Real time forecast with intelligent systems. In CONFERENCE ON KNOWLEDGE DISCOVERY. IEE, SAVOY PLACE, LONDON.

74. Corchado, J. M. (1997). Bdi multiagent hybrid architecture for project management. In IEEE COLLOQUIUM ON KNOWLEDGE DISCOVERY AND DATA MINING. LONDON ENGLAND.
75. Corchado, J. M. (1997). System for decision making: a practical case. In CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING. IEE, LONDON, UK.
76. Corchado, J. (1995). Cbr systems, an overview. In INTERNATIONAL CONFERENCE ON INTELLIGENT SYSTEMS. LONDON, ENGLAND, UK.
77. Li, T., Sun, S., Corchado, J. M., & Siyau, M. F. (2014, July). A particle dyeing approach for track continuity for the SMC-PHD filter. In 17th International Conference on Information Fusion (FUSION) (pp. 1-8). IEEE.
78. Corchado, E. S., Corchado, J. M., Sáiz, L., & Lara, A. (2004, July). A beta-cooperative cbr system for constructing a business management model. In Industrial Conference on Data Mining (pp. 42-49). Springer, Berlin, Heidelberg.
79. Corchado, J. M., & Lees, B. (1998). Integration ai models. In WORKSHOP ON KNOWLEDGE DISCOVERY AND DATA MINING. PML-NERC, PLYMOUTHLONDON, UK.
80. Corchado, J. M., & Lees, B. (1998). Cognitive models for integrating artificial intelligence approaches. In AII WORKSHOP ON KNOWLEDGE DISCOVERY. GLASGOW, UK.
81. Corchado, J. M. (1997). Real time forecast with intelligent systems: Cbrs and anns. In WORKSHOP ON ARTIFICIAL NEURAL NETWORKS. ABERDEEN (pp. 1-3).
82. Casado-Vara, R., Prieto, J., De la Prieta, F., & Corchado, J. M. (2018). How blockchain improves the supply chain: Case study alimentary supply chain. Procedia computer science, 134, 393-398.
83. Corchado, J. M. (1996). Case-base reasoning recommendation system. In IEEE COLLOQUIUM ON KNOWLEDGE DISCOVERY. LONDON, UK.
84. Corchado, J. M. (1995). Neuro-symbolic reasoning-a solution for complex problemas. In INTERNATIONAL CONFERENCE ON INTELLIGENT SYSTEMS. LONDON, UK.
85. Corchado, J. M. (1995). Multi agent tools: a case study. In IEEE COLLOQUIUM ON KNOWLEDGE DISCOVERY. LONDON ENGLAND, UK.
86. Casado-Vara, R., Prieto-Castrillo, F., & Corchado, J. M. (2018). A game theory approach for cooperative control to improve data quality and false data detection in WSN. International Journal of Robust and Nonlinear Control, 28(16), 5087-5102.

87. Corchado, J. M., & Lees, B. (2001). Adaptation of cases for case based forecasting with neural network support. In Soft computing in case based reasoning (pp. 293-319). Springer, London.
88. Rodriguez, J. M. C. (2000). Neuro-symbolic model for real-time forecasting problems (Doctoral dissertation, University of Paisley).
89. Casado-Vara, R., Chamoso, P., De la Prieta, F., Prieto, J., & Corchado, J. M. (2019). Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management. Information Fusion, 49, 227-239.