Abstract

The last decade has seen an exponential growth in the number of devices connected to the networks without precedent. Devices are becoming more powerful, autonomous and portable. Internet is evolving by huge leaps toward the *Internet of Things* where *all is connected* being a part of the daily life of a person. The systems are increasingly distributed both geographically and in terms of functionality.

Distributed systems and services are becoming of particular relevance over traditional centralized services. The paradigm of the distributed environment is perfectly suited to the current situation in which there is a large variety of networks, with thousand of geographically distributed devices spread over them. The classic Internet protocols do not handle this type of scenario and work quite poorly in such situations.

Data Distribution Service, known by the acronym *DDS*, appeared in 2004 to meet the need of distributed network systems. This technology works over the classic Internet protocols, standing as an interface layer between the transport and application layers within the model of TCP/IP Internet reference. Such arrangement are achieving great success in the current scenario, with the number of developers who use them is growing increasingly. DDS is utilised in critical communications, like the military, and also in multimedia communications. This is possible because DDS has been developed from the initial design as a piece of powerful and versatile *middleware*.

As important as the type of technologies used to develop the systems is the issue of information security. This is a quite important problem today. It is noteworthy that security was not a central factor in the develpment of the Internet protocols, from the beginning. Security is a crucial issue for both home users to large corporations. Confidentiality, authentication, data integrity, are examples of issues that include information security. The field of information security is a good case of a science where theorical experts are in conflict with the experimental experts. This originate from the myth that information security and cryptography are the same thing. Cryptography is not enough to ensure information security in distributed systems. This complex environment requires a more advanced design to provide the various necessary safety features.

DDS technology does not provide any safety feature. This task has been left to software companies that sell this technology. As for any other settings, the provision of security is also a critical aspect. This project tackles the design, development and implementation of an alternative solution to other existing security for the provision of security issues in distributed environments. It is intended to be accesible to anyone who needs to code a DDS system.

This document aims to solve this problem both from a theorical and experimental point of view. It proposes an ideal design for a system of this type and how to carry out the implementation. This implementation aims to study the problems of information security in a real enviroment as well as getting a working prototype of the proposed design.

First there is a study of the context and the current situation of the state of art, focusing on the analysis of existing business solutions. After this, it proposes a security design, treating each security feature individually, ensuring compliance. Finally an implementation of the design is done, tackling numerous problems that pertain to it. It intends to work in real environments. It is noteworthy that the prototype software has been released as free software, in order to be able to use by anyone.