

Such systems, henceforth referred to as Distributed Sensor Networks (DSNs), are expected to have a strong connection to our everyday life, and at least economic losses are expected in case of failures during their operation. The additional value of wireless DSNs is largely in their flexible deployment and communication capability. However, this also opens up most of the security<sup>1</sup> vulnerabilities of such systems.

There are known attack methods to compromise the ad-hoc communication channel between the nodes of a network. There are also precaution mechanisms built into the communication standards, to support the generation of network keys as well as the encryption and decryption of the messages. But increased security usually translates to increased cost, both in terms of development effort and run-time resource consumption. At the same time, the system must be maintenance-free or at least easily manageable even by non-technical users. To make matters worse, most of the security aids provided to the application developer are specific to the networking technology being used, i.e., there is the risk of having to re-define security-related protocols and implementations as part of the system's evolution. Hard application coding and the lack of portability of the security logic – or low security and reliability – can turn out to be an obstacle for the DSN technology penetration to the mass market. Motivated by these challenges, this paper presents a lightweight and portable security solution for DSNs designed by the authors in the POBICOS project [1]. The solution enables the user to manage such a system in a straightforward way and achieves sufficient data confidentiality at the application level.

The rest of this paper is organized as follows: Section 2 briefly discusses the related work. Section 3 provides a short introduction to the DSNs and their inherent vulnerabilities, security threats and requirements. In section 4 we propose two novel approaches to manage security in the DSNs, thus providing practical mechanisms and security protocols for implementation in typical DSN context. Section 5 discusses implementation issues of the security abstraction and, finally, section 6 summarizes the paper and delineates the future work.

## 2 Related Work

Existing security methods are available for many of the threats present in sensor networks but they are usually too resource consuming to be used in DSNs [2,3,4]. Actuator nodes, when present in the DNS, introduce increased risk. However, most of the research done in the field of DSNs does not consider that actuator nodes could exist in the network. A security related work that takes actuator nodes into account has been published in [5,6,7]. DSN security issues and a public key cryptography based key establishment scheme for DSNs are given in [7]. A cluster based communication architecture around each actuator of a DNS could be used to reduce the key management overhead. To suit this demand, a suchlike, scalable, energy efficient routing algorithm is introduced in [5].

---

<sup>1</sup> In this paper, the term security is used to refer to information security as well as protection against unauthorized access and control.