Computer Communications 33 (2010) 1086–1093

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Trust management systems for wireless sensor networks: Best practices

Javier Lopez *, Rodrigo Roman, Isaac Agudo, Carmen Fernandez-Gago

Department of Computer Science, University of Malaga, Malaga 29071, Spain

ARTICLE INFO

Article history:
Received 14 September 2009
Received in revised form 1 February 2010
Accepted 4 February 2010
Available online 12 February 2010

Keywords:
Wireless sensor networks
Trust management
Best practices

ABSTRACT

Wireless sensor networks (WSNs) have been proven a useful technology for perceiving information about the physical world and as a consequence has been used in many applications such as measurement of temperature, radiation, flow of liquids, etc. The nature of this kind of technology, and also their vulnerabilities to attacks make the security tools required for them to be considered in a special way. The decision making in a WSN is essential for carrying out certain tasks as it aids sensors establish collaborations. In order to assist this process, trust management systems could play a relevant role. In this paper, we list the *best practices* that we consider are essential for developing a good trust management system for WSN and make an analysis of the state of the art related to these practices.

1. Introduction

Computer systems are not able to perceive the physical information of the real world by themselves. It is possible to use sensor hardware to convert a physical property (e.g. temperature, radiation) into a digital signal. However, it would be interesting to have a component, either application-specific or off-the-shelf, which provides the functionality of a *sensory system* to any kind of computer system. That is the task of wireless sensor networks (WSNs). The primary elements of a WSN, the sensor nodes, are constrained devices capable of sensing and processing the information of the environment. Besides, they can use a wireless channel to collaborate among themselves. Finally, they are able to send the information to powerful devices known as base stations, which act as front-ends of the WSN, providing data to any human or non-human user (e.g. a RTU in a SCADA system [1]). The benefits of using WSN technology are numerous: it is easy to deploy and not expensive mainly due to the use of a wireless interface (cf. [16] for an industrial example), and it is able to run unattended and survive in its deployment area for long periods of time (e.g. a year or more [12]).

While self-sufficiency is considered to be one of the major features of WSN, this property does not come into existence automatically: it needs to be enforced. The elements and protocols of a WSN must be prepared to cope with variable conditions, faulty nodes and malicious entities. One mechanism that can be used to support the decision-making processes of the network is a Trust Management System. It aids the members of WSN (trustors) to deal with uncertainty about the future actions of other participants (trustees). By evaluating and storing the reputation ("What is generally said or believed about a person or the character or standing of a thing") of other members, it is possible to calculate how much those members can be trusted ("the firm belief in the reliability or truth or strength of an entity") to perform a particular task.

The importance of trust management systems in WSN has been acknowledged by the research community, and there exist many approaches that pursue the creation of a functional and lightweight system. However, many of these approaches do not take into account some specific features of WSN that can influence over their construction and functionality.

It is the purpose of this paper to derive certain trust management *best practices* from the specific features of WSN, and to analyze the compliance of the actual state of the art on trust management systems with those *best practices*. As an output of this analysis, we can identify those aspects that need to be further developed in present and future systems.

The structure of this paper is as follows. In Section 2 we introduce the general characteristics of WSN, provide an overview of trust management systems, and show the importance of trust management systems for WSN. Section 3.1 provides an analysis of the actual state of the art and Section 4 discusses how the systems studied in the previous section fulfil certain *best practices*, which should be taken into account on the development of any trust system. Finally, we present our conclusions in Section 5.

2. Sensor networks and the importance of trust

2.1. Elements and features of sensor networks

While modern research on sensor networks started on the late seventies [6], this paradigm acquired an identity of its own at the

* Corresponding author. Tel.: +34 952131327; fax: +34 952131397.
E-mail addresses: jlm@lcc.uma.es (J. Lopez), roman@lcc.uma.es (R. Roman), isaac@lcc.uma.es (I. Agudo), mcgago@lcc.uma.es (C. Fernandez-Gago).

0140-3664/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2010.02.006

beginning of the 21 century [21]. Present-day sensor networks can be considered as *living beings*, usually *born* (configured) in a controlled environment, where all its nodes are *cells* that work selflessly towards a common goal. Such nodes can work autonomously and are able to perform various tasks. The overall architecture of a WSN is highly dependent on its intended functionality. Another relevant feature of these networks is that no human user directly controls the nodes: they are usually accessed through the base station. Finally, WSN are usually long-lived, and the sensor nodes may have limited mobility [32].

From a technological perspective, as shown in Fig. 1, a WSN is mainly composed of two types of devices: sensor nodes and base stations. The sensor nodes, also known as motes or simply nodes, are small and constrained devices equipped with hardware sensors, microcontrollers, transceivers and batteries. Hardware sensors are used to sense the physical features of the environment (e.g. temperature, humidity, radiation, vibration). Microcontrollers are highly constrained in both computational power and memory, but thanks to them nodes are capable of processing information on their own. Wireless transceivers enable nodes to collaborate towards a common goal, such as routing the information to a base station. Finally, most nodes are battery-powered thus, they can survive in their deployment field for more than a year if their internal operations are optimized [12].

The base station is a more powerful device that behaves as a *front-end* between the services provided by the sensor nodes and the users of the network. While it would seem that WSN are highly dependent on the existence of this base station, the architecture of the network is not centralized. The nodes operate in a decentralized fashion, managing themselves without accessing the base station. In fact, there are some specific networks, known as *unattended sensor networks*, where the base station is only available at certain moments in time. Still, the base station usually plays an important role on the overall behaviour of WSN. Normally, a base station collects all the information coming from the sensor nodes and stores it for later use. Also, it may issue control orders to the sensor nodes in order to change their behaviour.

The network architecture of a WSN can be organized in a completely distributed way (flat configuration), but it can also implement levels of hierarchy (hierarchical configurations). In flat configurations all the nodes contribute in the decision-making process and participate in internal protocols such as routing. Conversely, in hierarchical configurations the network is divided into clusters or group of nodes. Inside a cluster all organizational decisions, like data aggregation, are made by a single entity called cluster head. It should be noticed that it is also possible to have a combination of the two previous configurations into the same network; for instance, to avoid situations where the *spinal cord* of the network – the cluster heads – fails and the information must be routed to the base station.

Regarding the services offered by wireless sensor networks they can be classified into four major categories: monitoring, alerting, provisioning of information *on-demand* and actuating. Due to the computational capabilities of the sensor nodes, it is also possible to re-program the network during its lifetime, or even use it as a distributed computing platform under specific circumstances.

- *Monitoring:* Sensor nodes can continuously monitor certain features of their surroundings (e.g. measuring the ambient noise level) and timely send such information to the base station.
- *Alerting:* Sensor nodes can check whether certain physical circumstances (e.g. a fire) are occurring, alerting the users of the system when an alarm is triggered.
- *Information on-demand:* The network can be queried about the actual levels of a certain feature, providing information whenever the user needs it.
- *Actuating:* Sensor nodes can be able to change the behaviour of an external system (e.g. an irrigation system) according to the actual state of the context (e.g. humidity of the soil).

There have been many experimental applications (from environmental monitoring to smart environments) created by the research community that take advantage of the previously shown WSN services [9]. For example, sensor nodes are very useful in precision agriculture [35], where they can improve the quality of the crops through actively managed irrigation. Moreover, a specific application that has attracted the attention of the industrial community is nuclear power plant monitoring [4], where sensor nodes can provide real-time information of the radiation levels of both workers and physical structures of a nuclear power plant. We believe that potential markets for WSN are likely to be increased drastically in the next coming years mainly due to recent developments in the field. This prediction is based on the rapid adoption of WSN in the areas mentioned above during the last few years.

2.2. Security and trust

The emerging importance of sensor networks could be hindered by their inherent security problems. This technology is tightly associated to the physical world. Thus, the nodes are as accessible as the event they monitor. The wireless channel used in the communications can also be accessed by anyone. Also, the nodes are highly constrained in terms of computational power, memory, communication bandwidth and battery power. Consequently, any malicious adversary could launch a certain set of attacks that could render the network partially or totally useless.

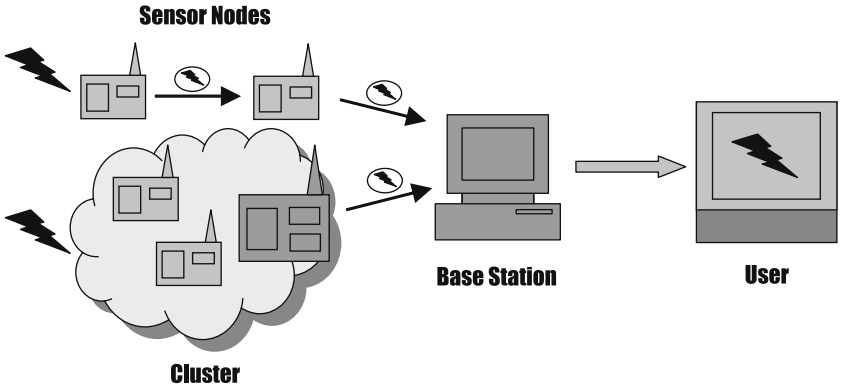

Fig. 1. An overview of the architecture of WSN.