Journal of Network and Computer Applications 34 (2011) 1225–1239

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

A survey on quality of service support in wireless sensor and actor networks: Requirements and challenges in the context of critical infrastructure protection

Jaime Chen *, Manuel Díaz, Luis Llopis, Bartolomé Rubio, José M. Troya

University of Málaga, Dpto. Lenguajes y ciencias de la Computación, Calle de Bulevard Louis Pasteur, s/n. 29071 Málaga, Spain

ARTICLE INFO

Article history:
Received 7 July 2010
Received in revised form
15 November 2010
Accepted 21 January 2011
Available online 31 January 2011

Keywords:
Quality of service
Wireless sensor and actor networks
Critical infrastructure protection
Real-time communication
Reliability
Communication protocol
Dependability

ABSTRACT

Wireless sensor and actor networks (WSANs) are likely to become a pervasive technology in the near future due to the special characteristics of these devices and to the great number of applications where it can be applied. One of these applications is the critical infrastructure protection (CIP). In fact, WSANs have actually been identified as having the potential to become an integral part of the CIP. However, in order to achieve that goal, WSANs need to provide a set of features which includes a robust QoS. Unfortunately QoS support mechanisms in WSANs are still largely undeveloped. This paper studies the state-of-the-art of QoS management in WSANs by exploring existing proposals, challenges and open issues in the field. Emphasis is put on QoS in the context of CIP by focusing on the QoS requirements and the needs of CIP applications. Existing middleware and protocols are surveyed and the challenges and open issues in the field are presented.

1. Introduction

WSANs have introduced an innovative way of monitoring and interacting with the environment (Akyildiz and Kasimoglu, 2004). Due to the flexible and interesting characteristics this technology has, WSANs are expected to be one of the most promising technologies in the near future. WSANs are composed of small devices with multiple on-board sensors which can communicate with each other through wireless links. By taking advantage of the large number of nodes which a WSAN is composed of, a high fault tolerance can be achieved and a scenario can be effectively monitored. Furthermore, scenarios can be controlled by means of actors, that is, resource rich devices that are capable of acting in the environment. WSANs flexibility is partly due to the lack of wiring and external power sources.

As WSAN technology evolves, new applications make use of it because of the inherent advantages it provides (Verdone et al., 2008). However, developing WSAN applications is not an easy task and intense research has been carried out to find new frameworks, tools, and middleware that provide higher level of abstraction with the aim of simplifying the task of the developers (Rubio et al., 2007; Mottola and Picco, to appear). The difficulties are caused by the intrinsic nature of these devices. Nodes in a WSAN are resource limited, non-reliable, dynamic devices. A WSAN constitutes a distributed system and as such all the difficulties of these kinds of systems apply to it.

As applications become more complex, the demands expected in the platform supporting them also increase. If the platform itself does not directly meet the requirements of the application, protocols and tools need to be used in order to manage the hardware with the aim of providing the required functionality. Intense research has been carried out in areas such as architecture, protocol design, energy conservation and locationing but Quality of Service (QoS) in WSANs is still a largely unexplored field of research (Chen and Varshney, 2004). In applications such as nuclear reactor control, battlefield surveillance or more generically in critical infrastructure protection (CIP), it is essential to guarantee certain levels of QoS.

Critical infrastructures as defined in the glossary of US Government (1997) are "Infrastructures which are so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security." The task of ensuring their availability and correct functioning under different scenarios including failures and attacks is therefore of utmost importance. Examples of critical systems are water supply, emergency systems, government services, electrical power or telecommunications. Proof of the growing interest in this field is that the number of initiatives dealing with

* Corresponding author. Tel.: +34 952 13 2865; fax: +34 952 13 1397.
E-mail addresses: hfc@lcc.uma.es (J. Chen), mdr@lcc.uma.es (M. Díaz), luisll@lcc.uma.es (L. Llopis), tolo@lcc.uma.es (B. Rubio), troya@lcc.uma.es (J.M. Troya).

1084-8045/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2011.01.008