Journal of Network and Computer Applications 34 (2011) 783–795

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Risk-based adaptive scheduling in randomly deployed video sensor networks for critical surveillance applications

Congduc Pham [a,*], Abdallah Makhoul [b,1], Rachid Saadi [c,1]

[a] University of Pau, LIUPPA Laboratory, Avenue de l'Université, BP1155, 64013 Pau Cedex, France
[b] University of Franche-Comté, LIFC Laboratory, France
[c] INRIA Rocquencourt, France

ARTICLE INFO

Article history:
Received 19 November 2009
Received in revised form
9 September 2010
Accepted 11 October 2010
Available online 16 October 2010

Keywords:
Sensor networks
Scheduling
Video surveillance
Critical applications

ABSTRACT

In randomly deployed visual wireless sensor networks for surveillance applications, the scheduling of sensor nodes can be seen from the risk perspective: different parts of the area of interest may have different risk levels according to the pattern of observed events such as the number of detected intrusions. In this paper, we propose a multiple-level activity model that uses behavior functions to define application classes and allows for adaptive scheduling based on the application criticality and on the availability of multiple cover sets per sensor node. The paper then describes how an adaptive scheduling model can be defined in order to dynamically schedule nodes by varying the capture speed according to nodes' environment. Simulation results are presented to validate the performance of the proposed approach in terms of percentage of active nodes, percentage of coverage and stealth time under intrusion scenarios.

1. Introduction

The monitoring capability of wireless sensor networks (WSN) makes them very suitable for large scale surveillance systems. A large number of applications related to environment (agriculture, water, forest, fire detection, etc.), military, buildings, health (elderly people, home monitoring, etc.), disaster relief, area and industrial monitoring have already been studied from the WSN perspective. Most of these applications have a high level of criticality and cannot be deployed with the current state of technology. Moreover, the purely scalar nature of traditional sensor nodes might be limiting for more complex applications such as object detection, surveillance, recognition, localization, and tracking. Therefore, in addition to traditional sensing network infrastructures, a wide range of emerging wireless sensor network applications can be strengthened by introducing a vision capability. In the domain of surveillance applications that are extremely mission-critical in nature, adding visual capabilities highlights news challenges.

This article focuses on wireless video sensor networks (WVSN) for mission-critical surveillance applications where sensors can be thrown in mass when needed for intrusion detection or disaster relief applications. The first concern in randomly deployed video sensors is that they will not land upside-down with the embedded camera turned towards the ground. This can actually be easily avoided by fitting the video sensor in a rocket-shaped case which will always touch ground in the right way as illustrated by Fig. 1 (left) (the figure shows an iMote2 with an IMB400 multimedia board, Crossbow, accessed 3/05/2010). Figure 1 (right) shows a simple video surveillance application we developed for the iMote2 with the IMB400 multimedia board that continuously takes pictures and displays both the current picture and the last picture.

The next thing to consider is that surveillance applications have very specific needs due to their inherently critical nature associated to security (He et al., 2004; Oh et al., 2006; Dousse et al., 2006; Zhu and Ni, 2008; Freitas et al., 2009). Early surveillance applications involving WSN have been applied to critical infrastructures such as production systems or oil/water pipeline systems (Stoianov et al., 2007; Albano et al., 2009). There have also been some propositions for intrusion detection applications but most of these early studies focused on coverage and energy optimizations without explicitly having the application's criticality in the control loop, which is the main concern in our work. For instance, with video sensors, the higher the capture rate, the better relevant events could be detected and identified. However, even in the case of very mission-critical applications, it is not realistic to consider that video nodes should always capture at their maximum rate when in active mode.

In high density randomly deployed sensor networks, sensor nodes can be redundant (nodes that monitor the same region) leading to overlaps among the monitored areas. Therefore, a

* Corresponding author. Tel.: +33 559407594.
E-mail addresses: congduc.pham@univ-pau.fr (C. Pham), abdallah.makhoul@iut-bm.univ-fcomte.fr (A. Makhoul), rachid.saadi@inria.fr (R. Saadi).

[1] Was with the LIUPPA laboratory at the time work was done on this article.

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.10.002