Available online at www.sciencedirect.com
SCIENCE DIRECT®
Ad Hoc Networks 4 (2006) 447–486
Ad Hoc Networks
www.elsevier.com/locate/adhoc

Polygonal broadcast, secret maturity, and the firing sensors

Shlomi Dolev [a,*], Ted Herman [b], Limor Lahiani [a]

[a] Department of Computer Science, Ben-Gurion University, Beer-Sheva 84105, Israel
[b] Department of Computer Science, University of Iowa, Iowa City, IA 52242, United States

Received 16 May 2004
Available online 9 March 2005

Abstract

This work considers communication among sensors that are deployed in a geographic region. Each sensor is a computing device with severe resource limitations, low power, slow processing and small memory. The devices are distributed (uniformly) in the geographic region. In this work we present self-stabilizing broadcast, flooding and sense of direction procedures that fit the special characteristics of the system. Imaginary polygon tilings are presented as a general scheme for supporting communication in sensor networks. Broadcasting is a common way of communicating in ad hoc mobile networks such as sensor networks. We present broadcast procedures and show how they are used by a sensor for broadcasting globally and locally, achieving sense of direction and distributing secrets that activate the sensors simultaneously at a particular time without revealing the nature of the upcoming activity.

Keywords: Sensor network; Wireless network; Mobile ad hoc networks; Graph theory; Power control; Security and privacy; Broadcast; Flooding; Sense of direction; Self-stabilization

1. Introduction

There is a great interest and attention of industry and research communities in the capabilities of small computing devices, called *sensors*, that use wireless communication among themselves [1,16]. The applications for such devices in creating a global computing environment [14,15] may change our view on computers and computing.

The new special settings of such systems require careful examination, and rethinking concerning the methodologies and technologies used for coordination. Energy limitation is a concern in sensor networks. Message transmission is more

* Corresponding author. Tel.: +972 8 647 2715; fax: +972 8 647 7650.
E-mail addresses: dolev@cs.bgu.ac.il (S. Dolev), herman@cs.uiowa.edu (T. Herman), lahiani@cs.bgu.ac.il (L. Lahiani).

1570-8705/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2005.01.003

expensive, in energy terms, than message receiving e.g., [8]. Moreover, energy required for transmission can grow more than quadratically with the distance imposing locality of transmission [18]. In addition, since sensors must receive a broadcast message, the efficiency of the scheme is tuned up by the number of sensors that have to transmit the message (even in the cases in which the energy for transmitting and receiving a message is the same). One would like to broadcast a message while *ensuring that most of the sensors will not have to transmit messages*. In a sense, a backbone of the network should be constructed, such that local broadcasts of some radius r of the backbone sensors will ensure global coverage of the geographic region in which the sensors are located. The geographic coverage requirement is a consequence of the possibility for having passive sensors that only receive messages (perhaps while operating in a mode used to harvest more energy) such that other sensors are not aware of their existence. Moreover, rather than having a fixed backbone, there could be an ad-hoc defined backbone for each particular broadcast. The existence of several backbones, spanned by different set of representative sensors, distributes the energy usage in a balanced fashion among the sensors.

We present several schemes based on imaginary (virtual) partition of the plane into (all possible) regular polygons: triangles, squares and hexagons. We call this an imaginary tiling because no permanent tiling or clustering of the sensors is established. Each polygon in the tiling has a representative sensor which is responsible for local-broadcasting the message to all the sensors in its polygon region. The representative can be elected according to different parameters such as, relative location in the polygon, maximum available power, etc. The polygon representatives form the ad-hoc backbone: they are the only transmitting sensors of a broadcast/flood, whereas all the others are only receiving. The scheme abstracts the specific transmission radius of the devices, by allowing the length of a polygon edge to be a parameter.

Our broadcast schemes are extended to the case in which the sensors are not uniformly distributed. We use polygonal flooding in order to cope with empty or hardly populated areas. The polygonal flooding requires (an additional constant factor) more transmissions and storage of arriving messages in the sensors memory. Subsequently we turn to cases in which only portions of the network should be notified by presenting polygonal local broadcast and polygonal local flooding. We show that it is possible to send a message to a particular geographic relative location. The combination of polygonal send and polygonal local broadcast/flooding enables a remote broadcast to a particular region. We also demonstrate the way the imaginary tiling can be used to provide sense of direction. Sense of direction is useful in many applications; for instance, sensors could direct an audience to building exits. Our sense of direction schemes are based on polygonal (backbone) flooding.

At last we examine a specific application of the polygonal broadcast/flooding schemes. Namely, we study the case in which an initiator would like to activate the sensors simultaneously and securely. An adversary that can observe the entire activity of every sensor including the initiator (see, e.g., [5] for similar settings), immediately after the initiator starts the broadcast and until the sensors are actually activated. In other words, we would like the sensors not to know what is the command (or if there is a command at all) in the arriving message.

To achieve the above we propose to use puzzles in the form of public key, transmitted by a satellite, used by the initiator to encrypt the command (such a command is decided upon sensing an event or by user-request, is thereafter immediately eliminated from the initiator memory). Then the command is broadcast with the time the puzzle will be solved by the satellite. The command is decrypted and executed simultaneously, succeeding to cope with the inherent delay in the information flood from initiator to receivers. In addition, we allow the command itself to be encrypted by a (time) puzzle, in a way that a predefined period of computation time will be required by the sensors for decryption. In this way the end-to-end delay will be eliminated by the first (unidirectional satellite) scheme, while the flexibility in activation time will be tuned and controlled by the (sensor that is the) command initiator.