Available online at www.sciencedirect.com

SCIENCE DIRECT®

Computer Standards & Interfaces 28 (2005) 159–165

COMPUTER STANDARDS & INTERFACES

www.elsevier.com/locate/csi

Modeling, specification and verification of ad-hoc sensor networks using SPIN

Vladimir A. Oleshchuk

Department of Information and Communication Technology, Faculty of Engineering and Science, Agder University College, Grooseveien 36, N-4876 Grimstad, Norway

Available online 16 February 2005

Abstract

A sensor network is a set of sensor nodes that communicate by sending messages over wireless links either directly to destination node or indirectly over a sequence of intermediate nodes. Sensor networks are often formed by ad-hoc deployment and utilized for information gathering and processing. Reliable and correct behaviors of such sensor based infrastructures are critical for many applications. The goal of this paper is to demonstrate applicability of finite model-checking to analysis and verification of sensor networks specifications modeled as dynamically changing graphs where connections and disconnections are determined by the distance between nodes.

Keywords: Ad-hoc sensor networks; Finite model-checking; Linear temporal logic; Specification; Verification

1. Introduction

An ad-hoc sensor network [5,6] is a set of sensor nodes that communicate by sending messages over wireless links either directly to destination node or indirectly over a sequence of intermediate nodes. Sensor networks are often formed by ad-hoc deployment and utilized for information processing and gathering. Since by design, sensors are small inexpensive devices it can be expected that wireless networks of thousands or even millions of sensors will be widely deployed in the near future, and thus will influence many if not all aspects of our lives. As typical applications of sensor networks we can mention emergency response information gathering such as fire detection, medical monitoring of health conditions, logistics and inventory management [7,9].

These applications indicate that reliable and correct behavior of sensor network based infrastructure can be critical for life safety, decision making etc., and consequences of misbehavior can be catastrophic. Therefore development of reliable, stable and secure solutions that work provably correct even in unreliable and distrusted environment is extremely important. However, limited resources of sensor devices such as processing power, storage, bandwidth and energy make it impractical to use many known

E-mail address: vladimir.oleshchuk@hia.no.

0920-5489/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2005.01.017

algorithms and protocols since they were designed for more powerful devices. Mobility, ad-hoc deployment and size of sensor networks may demand using self-organization principles where dynamic on-the-fly reconfiguration is an essential part of network behavior. Therefore the new algorithms and protocols should be invented, specified and verified with respect to the new constraints and correctness requirements imposed by applications [10].

The goal of this paper is to demonstrate applicability of finite model-checking to analysis and verification of sensor networks. We assume that sensor networks are presented as dynamically changing graphs where connections and disconnections are determined by distance between nodes and their willingness to collaborate. In Section 2 we present assumptions about properties of sensor networks that are essential for building useful and realistic models. Section 3 gives short description of model-checking system SPIN which we use to model and study properties of sensor networks. In Section 4 we discuss main features of sensor network models and sketch how they can by specified in Promela. In Section 5 we describe correctness criteria and show how they can be expressed in linear temporal logic, and then verified in SPIN.

2. Assumption about sensor networks

Modeling and analysis of sensor networks require their formal specification. Since such networks can be rather complex we have to select properties of the real sensor network and environment we have to model, i.e., we need to make assumptions about what properties should be considered in order to adequately model network behavior and its environment.

In this paper we make following general assumptions about sensor networks. The only sensors that are within one another's transmission radius can directly communicate with each other. In the sensor networks, sensors can cooperate with each other to conduct join computational tasks based on the inputs they supply to each other and/or values supplied to the sensors by their environment (e.g. modeling gathering of environmental information such as temperature, humidity, location etc.). It is reasonable to assume that both communication links and sensors themselves are unreliable. We should also assume that computations within sensor networks occur among distrusted or only partly trusted participants. However, even when two networks of sensors distrust to each other they still may need to cooperate by exchanging some data to perform join computations [9].

The sensor network can be modeled as a dynamically changing, undirected graph with nodes representing sensors connected by edges showing that corresponding sensors can communicate directly. Based on our assumptions about sensor networks we can formulate following general requirements to any sensor network model.

(1) Nodes are mobile, distrusted, have unique identifiers within their communication radius. (All known algorithms assume a unique identifier within a whole network but it can be unfeasible for networks of thousands of nodes with dynamically changing configuration).
(2) Communication links are bidirectional and unreliable.
(3) Underlying protocols ensure that nodes are aware of the other nodes within their transmission radius and support establishment of communication between nodes that can communicate directly.

Under assumptions (1)–(3) behaviors of such highly-distributed networks can be rather complex and unpredictable. Therefore it is necessary to develop methods to analyze and study properties of such hundreds or even thousands sensors network if one wants to be able to design reliable sensor network based applications.

Traditionally, design of computer communication networks follows (often loosely) the International Organization for Standardization (ISO) Open System Interconnection (OSI) Reference Model as the basis for their protocol stack design. The OSI Reference Model specifies seven protocol layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. The following considerations relate sensor networks models we study in this paper to the OSI Reference Model.

Since communication media for sensor networks are broadcast in nature, there is a need for medium access control (MAC) that gives the method by which