

# Poster Abstract: Run Time Assurance of Application-level Requirements in Wireless Sensor Networks

Jingyuan Li, Yafeng Wu, Krasimira Kapitanova, John A. Stankovic, Kamin Whitehouse, and Sang H. Son  
Department of Computer Science  
University of Virginia

{jl3sz, yw5s, krasi, stankovic, whitehouse, son}@virginia.edu

## Abstract

The current rapid development and deployment of wireless sensor networks (WSNs) and their application in mission critical systems are exacerbating the need for high confidence WSNs. Achieving high confidence WSNs will require new assurance technologies. Most current solutions deal with faults and reliability and not with application level semantics and associated assurances. We propose the use of a novel WSN design and assurance mechanism, run time assurance (RTA), to guarantee that important application-level requirements are met in mission critical applications.

## Categories and Subject Descriptors

C.2 [Computer-Communication Networks]: Distributed Systems; D.2.1 [Software Engineering]: Requirements /Specifications; D.2.4 [Software Engineering]: Software /Program Verification

## General Terms

Design, Software, Assurance

## Keywords

Wireless Sensor Networks, Run Time Assurance, Application Semantics, Petri Net, Virtual Event

## 1 Introduction

A common vision of the future is one where our everyday environments are replete with wireless sensing devices networked to form complicated systems of systems. These systems will need to exist for many years, and operate in the context of real world communication, sensing, and failure realities. Many of the systems will be unattended (at least for large periods of time) and often performing very important tasks. The current rapid development and deployment of WSNs and their application in mission critical systems are exacerbating the need for high confidence WSNs.

Achieving high confidence WSNs will require new assurance technologies both off-line and on-line. For off-line solutions we expect to utilize formal methods and new analysis techniques. However, even when the off-line solutions are effective, there will still be a great need for run time assurance technologies because these systems operate in the noisy,

error-prone physical world. Most of the current on-line solutions deal with faults and reliability and not with application level semantics and associated assurances.

Given the limited insights of the system's run time operability provided by current WSNs, and the highly desirable assurance requirements to allow users to capture run time failures at the application level, we propose a comprehensive and general framework to allow designers to build WSNs with RTA support. Our framework includes: a requirement specification language based on SNEDL [1], an extended Petri net [2] model, that is specifically designed to demonstrate the critical functionality of the system; a TinyOS based programming architecture that formalizes the implementation of the system's application level behaviors according to the SNEDL model; three run time mechanisms used for generating assurance tests according to the RTA requirements specifications and collecting information once the system fails.

The main intellectual contribution of this work is determining how to specify and support at run time a collection of solutions that enable WSNs to improve confidence and demonstrate application operability. The broad impact of this work can be extensive since there is a proliferation of WSNs being deployed or contemplated for critical applications such as fire fighting, pollution control, disaster response, tracking, military surveillance, and medical assistance. To the best of our knowledge, this is the first work that addresses the confidence issue of WSNs at the application semantics level and provides comprehensive solutions for RTA.

## 2 Proposed Solution

The proposed solution is composed of three major pieces: a formal requirement specification language used to define the application-level requirements, a TinyOS based programming framework that assists designers in implementing applications according to the RTA requirements specification, and a set of novel RTA mechanisms.

### 2.1 Formal Requirements Specification

We use SNEDL to formally describe the application level requirements of a WSN system. SNEDL is the first event specification language to support key features of WSNs. As a description language, it is an extension of Petri nets. A SNEDL Petri net integrates features from color, time, and stochastic Petri nets to tackle problems in specification and

