EAI Endorsed Transactions on Ambient Systems

Research Article ICST.ORG

A simple network agreement-based approach for combining evidences in a heterogeneous sensor network

Raúl Eusebio-Grande[1], Angélica Muñoz-Meléndez[1,*]

[1]Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE), Mexico.

Abstract

In this research we investigate how the evidences provided by both static and mobile nodes that are part of a heterogenous sensor network can be combined to have trustworthy results. A solution relying on a network agreement-based approach was implemented and tested.

Received on 30 November 2015; accepted on 30 November 2015; published on 01 December 2015

Keywords: sensor network, static nodes, mobile nodes, confidence.

doi:10.4108/eai.1-12-2015.150710

1. Introduction

The design of sensor networks has been a very active field of research in recent years. This research has greatly benefited from the availability of all sort of devices and electronic components that integrate sensing, logging, processing, and communication capabilities.

However, most of the infrastructure developed so far is mainly oriented to support homogeneous sensor networks, i.e., networks comprising nodes equipped with essentially same features, in terms for instance of technical capabilities such as sensitivity, sampling rate, scope of communication, and so on.

The design of heterogeneous sensor networks, i.e., networks comprising nodes equipped with different capabilities, has been much less studied. Data collected through heterogeneous sensor networks is in principle more diverse and its fusion into consistent models is a challenging issue.

In this research we investigate how the evidences provided by both static and mobile nodes that are part of a heterogenous sensor network can be combined to have trustworthy results.

A sensor network prototype for acquiring environmental parameters, such as temperature, humidity, dust density, and noise in domestic scenarios has been designed. Static nodes are encapsulated within boxes with wireless connection to a network, whereas mobile nodes are encapsulated in hats that are worn by human users and transmit data to a server through smartphones.

In this network, nodes are not necessarily submitted to security threats or malfunction, as it is usually the case in the related work [1, 2]. In our case, the performance of sensors can be affected when they are set in mobile nodes and worn by people. A solution relying on an estimation of levels of confidence applying a network agreement-based approach was implemented and tested.

2. A heterogeneous sensor network prototype

The network comprises two static nodes, three mobile nodes and one server (see Figure 1) with the features described below.

- **Static node.** It is equipped with a sensor of temperature and humidity HIH-6130 from Honeywell, a microphone OPA344 from Texas Instruments, an optical dust sensor GP2Y1010AU0F from Sharp, an Arduino UNO electronic board, and a RN-XV WiFly module from Roving Networks. The dimensions of the module's base are $12cm \times 12cm$ and $5cm$ of height, and it has a weight of $180gr$. The module has a cable supply AC.

*Corresponding author. Email: munoz@inaoep.mx

- **Mobile node.** It is equipped with a sensor of temperature and humidity HIH-6130 from Honeywell, a microphone OPA344 from Texas Instruments, an Arduino Lilypad electronic board, and a RN-42 bluetooth communication module from Microchip. These components are arranged in a panel of $11cm \times 7.5cm$ that has a weight of $50gr$. The module is powered by a 3.7V LiPo battery.
  Mobile nodes function with smartphones. Three Sony Ericsson Xperia Arc S smartphones with a 1.4GHz processor and 512 Mb of RAM, running under Android 4.0 are used, one for each mobile module.

- **Server.** A desktop computer equipped with an Intel Core i7 processor with 8Gb of RAM, running under Ubuntu 12.04 LTS was used to collect data from all the modules.
  Due to storage limitations, static nodes transmit sensor data to the sever every 20 seconds. In mobile nodes, sensor data are transmitted from the Liliypad board to the smartphone every 20 seconds, and from the smartphone to the server on demand, usually at the end of a session or experiment. For both cases, data are transmitted using a TCP protocol.

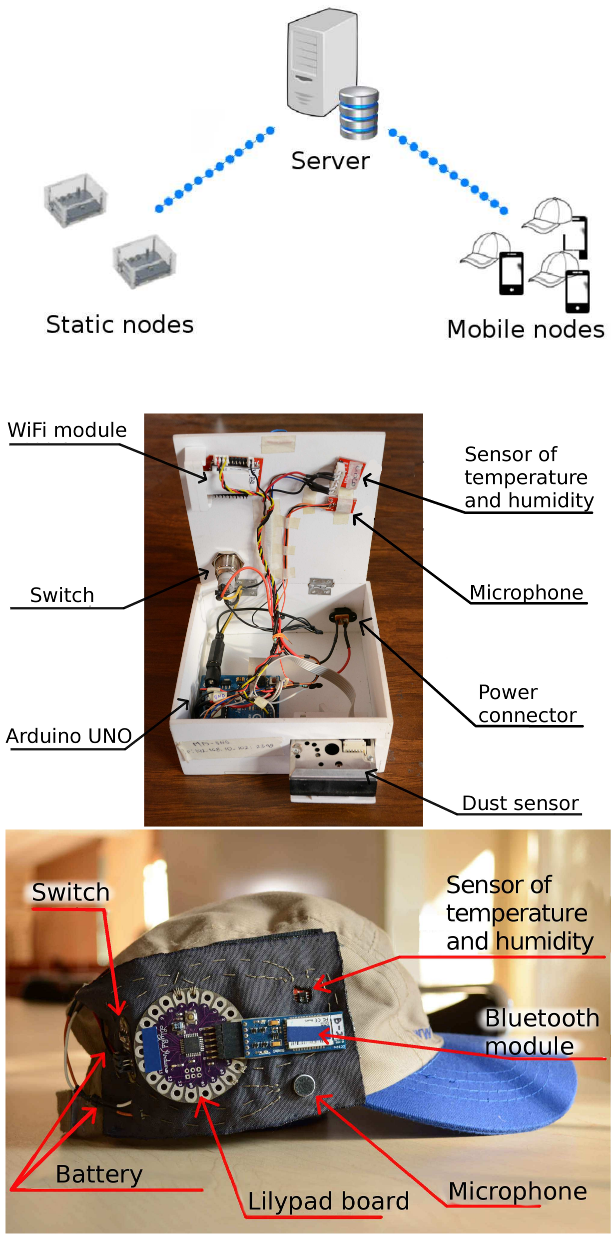

Figure 1. Architecture of the sensor network prototype (top), static node (middle), and mobile node (bottom)

5. Examples of combination of evidences

We have conducted a set of controlled experiments in order to determine the behaviour of the different nodes comprised in the network. Even though we are using similar sensors for monitoring a known environment, a considerable variability is expected in the sensors' readings according to their configuration, static or mobile.

In this research we focus on data about "noise" and "temperature" collected by a network comprising four nodes, two static and two dynamic nodes. For all the experiments described in this article, commercial sensors external to the network were used as ground truth. A sonometer GM1358 from Benchteck and a thermometer TER-100 from Steren were used for measuring references for, simultaneously, "noise" and "temperature".

Figure 2 shows the estimations of the network for the parameters "noise" measured in dBA (top) and "temperature" measured in Celsius degrees (bottom), with respect to the external references during 1 hour. During this time, the nodes were immobilised side-by-side on a desk. In this case, the server simply calculates an average value from raw evidences transmitted by all the nodes. The average root mean square (RMS) are of 2.50 for "noise" and 0.17 for "temperature", that indicate that estimations are, in stationary conditions, stable.

In the second experiment that lasted 2 hours, an explicit exchange of mobile nodes was introduced. A user worn the mobile node 1 during the first hour while the mobile node 2 remained immobilised on a table. Then the user worn the mobile node 2 during the second hour leaving the mobile node 1 on the table. Static nodes remained also on the mentioned table. During this experiment the user stayed in the vicinity of the area covered by the rest of nodes (within a radio of $2.5m$). The network estimations based on simple averages recorded during this experiment are shown in Figure 3.

In spite of the exchange of mobile nodes made during experiment 2, note that estimations of the network for the parameter "noise" remain reasonably closed to the ground truth values. However, the motion and the heat generated by the user wearing mobile nodes have a significant effect on the parameter "temperature" measured by mobile nodes, and in consequence, impact considerably the global estimation of the network. The average RMS of the network estimations for "noise" and "temperature" are, respectively, 3.03 and 1.46.

In order to provide more details about this experiment, in the top of Figure 4 the raw recordings of "temperature" scored by individual nodes of the network are plotted. The effect that mobile nodes worn by a user have on these recordings is remarkably visible at the beginning (first 10 minutes) and in the middle of the experiment (minutes 60-70).

For dealing with this situation, we have implemented a network agreement-based approach to merge data collected from a sensor network relying only on data. This agreement is calculated by the server over the values transmitted by individual nodes applying simple statistical measurements. Basically, when the location of nodes is within a radio of less than $6m$ we assume that the values recorded by nodes might be closed to each other, and we identify outliers as the values that are beyond the average of nodes' values ± a standard deviation, as summarised below.

- **First agreement**. Let be $v_t = (ev_1, ev_2, \ldots, ev_n)_t$ a vector of n readings of a given parameter from a sensor network collected at time t, and let be μ_t and σ_t the average and standard deviation of the values in v. If $\mu_t - \sigma_t \leq ev_i \leq \mu_t + \sigma_t$, then consider ev_i for the network estimation, otherwise ignore it.

- **Conservative agreement**. Let be $v_t = (ev_1, ev_2, \ldots, ev_n)_t$ a vector of n readings of a given parameter from a sensor network collected at time t, and let be μ_t and σ_t the average and standard deviation of the values in v. If $\mu_t - \sigma_t \leq ev_i \leq \mu_t + \sigma_t$ then consider ev_i for the network estimation, otherwise ignore it. If more than one value is considered for the network estimation, then prefer the one with less variation in the most recent subsequent readings.

The variations of our network agreement-based approach are illustrated in the bottom of Figure 4 for the readings of parameter "temperature". The RMS applying the first agreement criterio is 1.32 while the RMS applying the conservative agreement criterio is 0.93, considerable less than the error scored when applying a simple average combination of evidences.

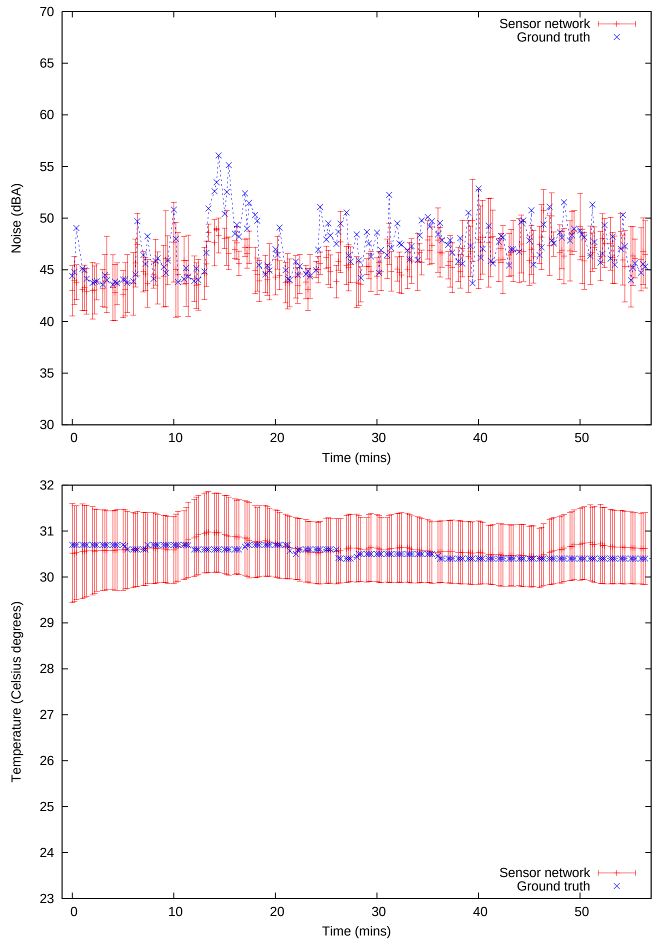

Figure 2. Average estimation of the sensor network for the parameters "noise" (top) and "temperature" (bottom), with respect to external references during 1 hour with all the nodes immobilised

4. Concluding remarks

This research aims at combining evidences collected by various heterogeneous nodes of a sensor network in flexible manners. The main idea of our network agreement-based approach is to identify outliers that might bias the result or measurements of the sensor network by calculating statistical measurements over samples of evidences.

A lot of work remain to be done in order to propose and refine methods for combining real-time data in consistent and useful knowledge of the phenomenon or environment measured by a sensor network.

In the near future, we plan to test our approach using sensor networks with more nodes in experiments lasting several hours and days.

References

[1] Ryutov T and Neuman C 2007, 'Trust based approach for improving data reliability in industrial sensor networks',

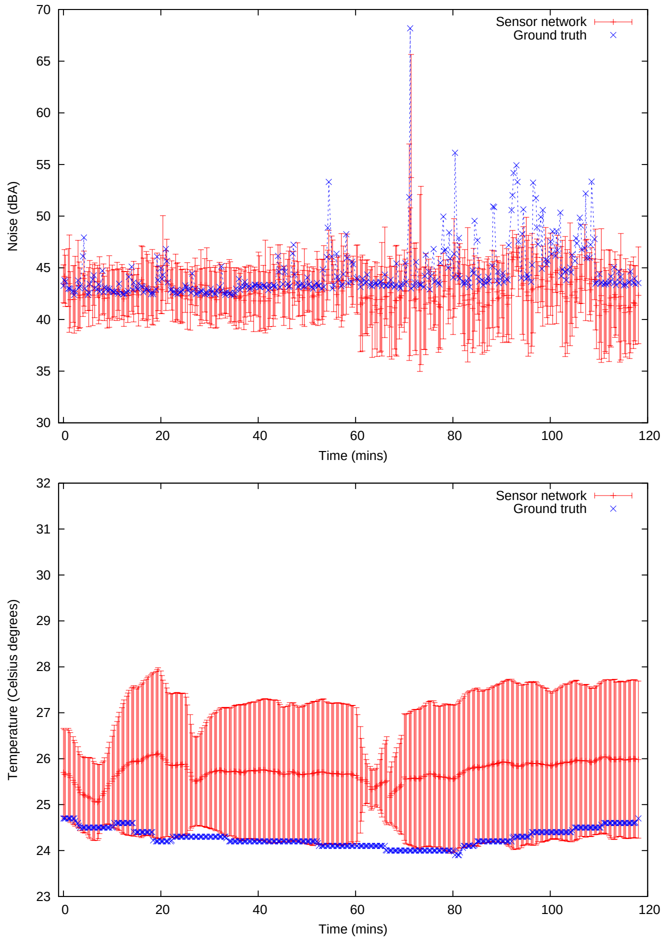

Figure 3. Average estimations of the sensor network for the parameters "noise" (top) and "temperature" (bottom), with respect to external references during 2 hours where mobile nodes were worn by a user

Book chapter, *Trust Management*, vol. 238, pp. 349-365. Springer, Boston.

[2] Han G, Jiang J, Shu L, Niu J and Chao H-C 2014, 'Management and applications of trust in Wireless Sensor Networks: A survey'. *Journal of Computer and System Sciences*, vol. 80, pp. 602-617.

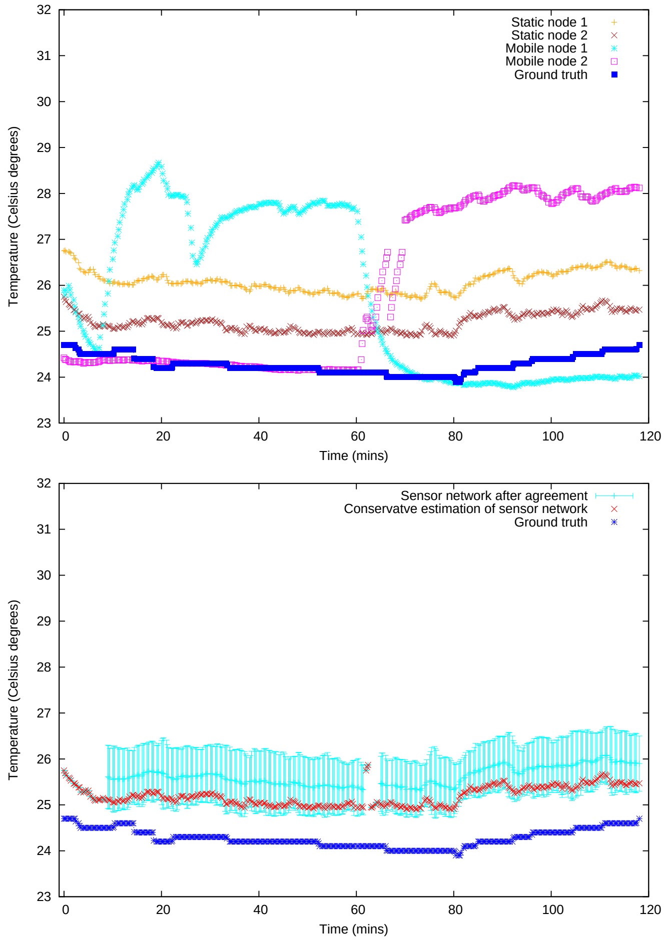

Figure 4. Individual recordings of the nodes of the sensor network for the parameter "temperature" (top) and revised estimations of "temperature" relying on two variations of our network agreement-based approach