Performance Optimization of WSNs using External Information

Gabriel Martins Dias

Department of Information and Communication Technologies, Universitat Pompeu Fabra, Barcelona, Spain.
Email: gabriel.martins@upf.edu

Abstract—The goal of this work is to describe a self-management system that correlates data sensed by different Wireless Sensor Networks (WSNs) and adjusts the number of active nodes in each network to provide an appropriate amount of measurements. The architecture considers the factors that make the external data relevant to the local network, such as the distance between covered areas, the relation between the types of sensed data and the reliability of the measurements. As a result, the operation of each network will be tuned to trade-off the accuracy of the measurements and the power consumption.

Keywords-Information Sharing; Wireless Sensor Networks; Autonomic Computing, Performance Optimization;

I. Introduction

Different types of WSNs may be deployed in similar areas in order to measure semantically linked data, for example, temperature and humidity. Therefore, these data could be combined to enhance the accuracy of different WSNs without increasing their measurement rate and keeping their levels of energy consumption low.

According to [1], most WSN applications for fire detection use a fusion of sensed data, such as temperature and CO_2 levels. This is usually mapped using functions that provide a trustful correlation between different types of parameters. Tests done in [2] show that a WSN for fire detection that uses ionization and photoelectric sensors might increase its accuracy up to 45% if the temperature was also considered in the detection algorithm. Additionally, the amount of data collected by a WSN can be tuned if the network has information from external sources about the probability that the event it is monitoring exists. In case of a low probability, the amount of data to collect can be reduced, hence saving the sensors' batteries.

In [3], some examples of collaborative WSNs are described. Those networks either use collaboration methods as (internal) solutions for some problems of WSNs, such as coverage, localization, energy conservation, and security, or they cooperatively monitor and control objects (i.e. providing information to other systems). This work is meant to provide the missing link between both definitions: how to reduce the problems of WSNs, such as coverage and energy conservation, by cooperatively monitoring the environment.

So far, no work has considered using data collected by external WSNs in order to improve the performance of internal WSNs. As a side note, there are some challenges when considering to achieve an effective collaboration between WSNs that were not built to work together, because they may not cover exactly the same area, the data sensed by their neighbors may not be tightly coupled to their own type of monitored data, or simply because they are under different ownership. To handle these problems, it is necessary to weight the relevance of the data received from external WSNs as well as consider possible malicious behavior.

The main goal of this work is to maximize the lifetime of WSNs without compromising the quality of the measurements taken. To achieve this, the proposed system will be capable of self-configuring its networks at runtime according to the changes in the environment, detected by the internal or external WSNs.

II. Architectural Components

In [4], an architecture for WSN collaboration is presented. A new type of node, called an Enhanced Gateway (EG), is used as the contact point between the internal WSNs and the other EGs. They are directly connected to the respective WSN sink nodes and maintain an overlay connection to other EGs in order to exchange information about their networks and measured data. The same role is played by a manager in the autonomic systems (described in [5]), which must perform monitor, analyze, plan and execute functions in order to configure its networks according to the environmental changes. Figure 1 shows the basic workflow.

A. Monitor

After receiving new data either from internal or external WSNs, the EG must filter it in order to remove noise and errors by performing syntactic and semantic validations over the measurements. At this point, the WSN application goals (e.g. fire detection) must be considered in order to scale how relevant the data can be that is received from other WSNs. The filtered data will be used to find a relationship between different sensed data types.

B. Analyze

Every change in the environment must be analyzed in order to know what the probability is of having an event of interest, for example, a forest fire. The inference can be made either using pattern-matching or threshold-based algorithms.

Approaches that use manually-set thresholds require prior knowledge of the domain and the relationship between the
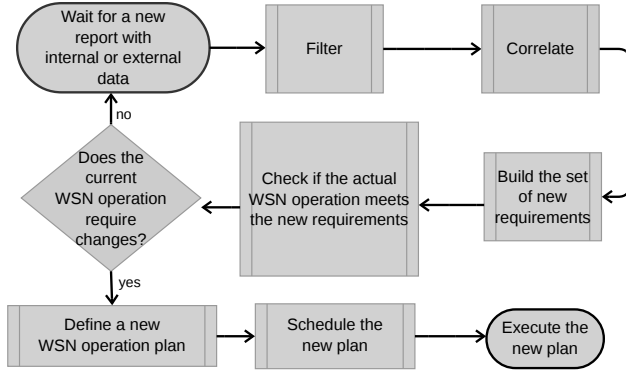
Figure 1.   Flowchart of an Enhanced Gateway (EG)

III. PERFORMANCE EVALUATION PLAN

Our first planned step is to simulate multiple WSNs that share and use their measured data to optimize their own operation. For example, temperature monitoring and fire detection. For that, the components described in Section II will be implemented in the simulator, starting with a data correlation algorithm and the definition of how to quantify the quality of the measurements done in the WSNs. After this step, it will be possible to compare the energy consumption of the WSNs when collaboration is used versus the opposite case. A second step is to evaluate the proposed architecture in a test-bed, which will proof the suitability of the proposed approach in real world scenarios.

IV. EXPECTED OUTCOMES

The main expected outcome of this work is an implementation of an autonomic system that provides a scalable and self-managed solution for WSNs management.

The challenge is to build an architecture that will reduce the energy consumption of the WSNs based on the knowledge acquired from historical data. Additionally, the new method will use collaboration models and explore the WSNs as sources of knowledge to achieve this goal.

Other expected outcomes are a generic approach for correlating data from different sources by applying pattern-matching or threshold-based algorithms, and metrics for measuring and evaluating the quality of measurements based on the application types.

V. ACKNOWLEDGEMENT

different types of sensed data. In addition, each EG must keep information about the trust of the networks that are collaborating with it. The trust value may consider discrepancy to its own data, the distance between the networks and also the errors observed in past measurements. Artificial Intelligence techniques can be used to build a learning system that adjusts the trust value after evaluating each new measurement input. On the other hand, pattern-matching approaches require less external configuration and can build predictions based on historical data.

C. Plan & Schedule

By checking the probability of having an event of interest, the EG will determine whether changes must be made in the network behavior. The new plan will depend on the type of the application deployed, which can be event-driven, monitoring or hybrid. Event-driven applications (e.g. decentralized fire detection) require no delay, quick transmissions and reliability. Monitoring applications (e.g. temperature and humidity) do continuous transmissions to the sink and tolerate packet losses as well as small delays between consecutive transmissions. Finally, hybrid applications (e.g. centralized fire detection) combine both types.

For example, if the network was operating with a low number of nodes transmitting measurement reports at a low rate, it might not manage to make an early detection of a new critical event such as a fire. According to the evaluation done, a request for changing the current set of active nodes and the time between consecutive reports will be issued.

In the end, the EG will compute the best combination of active nodes and the time interval between consecutive reports in case of continuous transmissions. The new plan must be a trade-off between the power consumption and the quality of measurements, which scaling may consider multiple parameters, such as the number of active nodes, the time interval between consecutive transmissions, network coverage, latency, packet loss rate, bandwidth used to report an event and information throughput at the sink.

REFERENCES

[1] M. Bahrepour, N. Meratnia, and P. Havinga, "Automatic fire detection: A survey from wireless sensor network perspective," December 2008.

[2] M. Bahrepour, B. Zwaag, N. Meratnia, and P. Havinga, "Fire data analysis and feature reduction using computational intelligence methods," in *Advances in Intelligent Decision Technologies*, vol. 4 of *Smart Innovation, Systems and Technologies*, pp. 289–298, Springer Berlin Heidelberg, 2010.

[3] W. Li, J. Bao, and W. Shen, "Collaborative wireless sensor networks: A survey," in *Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on*, pp. 2614–2619, 2011.

[4] S. Pal, S. Oechsner, B. Bellalta, and M. Oliver, "Performance Optimization of Multiple Interconnected Heterogeneous Sensor Networks via Collaborative Information Sharing," *arXiv preprint arXiv:1203.6316*, 2012.

[5] "An architectural blueprint for autonomic computing,", fourth ed. Computing IBMA, June 2006.