Sustainable Performance in Energy Harvesting - Wireless Sensor Networks

Xenofon Fafoutis
Dept. of Applied Mathematics
and Computer Science
Denmark Technical University
xefa@imm.dtu.dk

Alessio Di Mauro
Dept. of Applied Mathematics
and Computer Science
Denmark Technical University
adma@imm.dtu.dk

Nicola Dragoni
Dept. of Applied Mathematics
and Computer Science
Denmark Technical University
ndra@imm.dtu.dk

ABSTRACT

In this practical demo we illustrate the concept of "sustainable performance" in Energy-Harvesting Wireless Sensor Networks (EH-WSNs). In particular, for different classes of applications and under several energy harvesting scenarios, we show how it is possible to have sustainable performance when nodes in the network are powered by ambient energy.

Categories and Subject Descriptors

[**Computer systems organization**]: Embedded and cyber-physical systems; [**Networks**]: Network protocols

1. INTRODUCTION

Recent advancements in energy harvesting have led to the possibility of powering wireless embedded devices by small-scale ambient energy. Depending on the nature of the application, several environmental energy sources can be harvested, such as solar power or heat from radiators. In contrast to the limited amount of energy a battery can store, energy harvesting can potentially produce an infinite amount of energy. Therefore, the continuous operation of the system is only limited by hardware or software failures. As a result, the installation and maintenance costs of a network are significantly reduced. Furthermore, energy harvesting constitutes an environmental friendly means to power embedded devices, as it is an efficient driver to cut down wasted energy and battery wastes.

The system goal of Energy Harvesting - Wireless Sensor Networks (EH-WSNs) is fundamentally different from the one of traditional (battery-powered) WSNs (that is, to maximize network lifetime by minimizing energy consumption). Indeed, as long as the harvested energy is more than or equal to the energy consumed, energy does not constitute a limitation on the lifespan of the embedded device. Furthermore, any additional harvested energy can be used to improve the performance of the application. Thus, the system goal of EH-WSNs is twofold. Sustainable operation constitutes the primary goal, while application performance represents the secondary goal whenever the energy input allows it. In other words, we aim at achieving max sustainable performance.

In this demo we show some results on our ongoing research on realizing EH-WSNs. In our previous work, we introduced ODMAC [3], a MAC[1] protocol specifically designed for EH-WSNs. The MAC scheme plays a central part in the design of energy-efficient WSNs since it controls the duty cycle of each node and the radio component (which dominates the energy consumption of a node). In particular, our analytic results [2] and simulations [3] shows that ODMAC supports sustainable performance. The contribution of this demo is to illustrate these findings on a real EH-WSN test bed developed in our lab. In particular, for different classes of WSN applications (i.e., applications having different performance requirements) as well as under several energy harvesting scenarios, we show how ODMAC supports sustainable operation of nodes powered by ambient energy.

2. EH-WSN TEST BED

Hardware. The system has been implemented on Texas Instruments' eZ430-rf2500 sensor nodes. Each node consists of an MSP430 microcontroller and a CC2500 radio, operating on the 2.4 GHz band. In addition to batteries, the nodes can be powered by external energy harvesting boards. In particular, we use Cymbet's CBC-EVAL-10 and CBC-EVAL-9 energy harvester boards (Figure 1). The boards harvest energy from different sources and store it into embedded batteries ($100\mu A$ capacity). The energy harvester board can power the radio in active state for approximately $150 - 200$ ms every 10 seconds.

Firmware. Our aim is to have complete control of the system, mitigating mitigate the use of external libraries. As a result, the only external library we use is a Texas Instruments' Minimal Radio Frequency Interface (*MRFI*), which provides an interface for the radio transceiver. More explicitly, it allows for the actual communication between the microcontroller and the radio components, it provides fundamental primitives (*receive, transmit with/without clear channel assessment*) and it gives control over the powering of the radio module itself (*sleep, listen*). On the other hand additional overhead and unnecessary information are added to the exchanged frames. For this reason, this layer will be replaced and rewritten in the future to better suit our needs.

[1] Medium Access Control

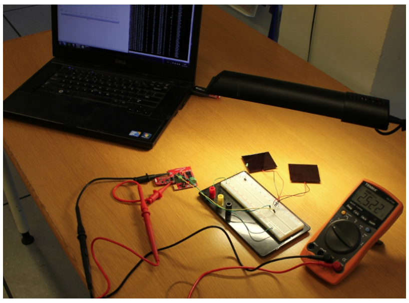

Figure 1: Ex. of Nodes in our EH-WSN Test-Bed

On Demand MAC Scheme. On top of MRFI we implemented ODMAC [3], a receiver-initiated Medium Access Control protocol we specifically designed for EH-WSNs. The key feature of ODMAC is the possibility for each node in the network to dynamically and independently choose its own duty-cycle in order to accommodate its energy constraints. Furthermore, ODMAC supports anycast routing, namely *opportunistic forwarding*. The idea is that each node, instead of waiting for the optimal relay, sends messages to the recipient that wakes up first (that is, to the first recipient that makes itself available for reception). This recipient must belong to a set of possible forwarders provided by the routing protocol. The main consequence from the adoption of ODMAC is that the sensor network is characterized by some important features, such as autonomous load balancing, reduced delay and reduced idle listening. These characteristics, in particular the former and the latter, become crucial from an energy consumption perspective.

Embedded Security. A security suite inspired by TinySec [4] has been designed and implemented at the MAC layer. In order to support sustainable performance, the suite provides four security modes, namely *no security, authentication, encryption, both.* The specific mode can be chosen on a per-message basis. Authentication of beacons (control messages) has also been implemented. Both confidentiality and authentication are provided through the same encryption primitive. The adopted algorithm is *Skipjack* [1], and other implementations are underway (e.g. AES, PRESENT) for further security analyses. Encryption is always performed by using secure modes of operation, specifically *Cipher-block Chaining* with *Cyphertext Stealing* to keep the message size unmodified. Since the suite works at the MAC layer, Message Authentication Codes and encryptions are verified and reconstructed at each hop. This requires more CPU intensive work, but allows for forged or malformed packet to be identified and discarded right away, thus saving transmissions of useless data and assuring greater energy savings. Key managements schemes and adaptive security (that take into account the energy harvesting rate of the nodes) are work-in-progress extensions of the current security layer.

3. DEMO

The purpose of this demo is to show how our EH-WSN prototype can run under several energy harvesting scenarios (i.e. varying the amount of salvageable energy) always adapting itself in order to maintain a sustainable operational state. As WNS applications are mission-specific, we run our sensor network in three scenarios characterizing different classes of WSN applications. Each class will favor a different performance metric.

Scenario 1: Delay Sensitive Applications. The focus of this class of applications is to minimize the end-to-end delay which is defined as the amount of time elapsed since a message generation until its reception, while maintaining the sustainability of the system. This scenario is characterized by a sender and an energy harvesting powered receiver. The beaconing period of the receiver controls the level of the delay. The specific measurement that we will evaluate is the delay of the messages generated by the sender node. The energy harvesting node has to find the right compromise between survivability and low delay. Minimal delay is crucial for surveillance type of applications, where an anomaly should be reported as soon as possible.

Scenario 2: Datalogging Applications. The focus of this class is to gather as many messages as possible for long-term monitoring or offline analysis. The optimal working point here would be the one that allows for the highest number of successful transmission, independent of the time it takes a specific message to travel across the network, while maintaining sustainability. Here we use a basic two nodes single-hop topology, with the sink on one side and an energy harvesting powered node on the other.

Scenario 3: Security Sensitive Applications. This class of applications handles data having significant security requirements. In this scenario we focus on the impact of the possible security extensions over the energy consumption. Depending on the specific application, different messages may have different security requirements. We will use the same topology of scenario 2 to measure the network's throughput, while cycling through all the security modes.

4. CONCLUSION

The use of energy harvesting technologies to power embedded wireless devices has changed the fundamental optimization goals of sensor networks. Instead of focusing on maximizing the limited lifetime of the nodes, energy harvesting can provide nodes with potentially infinite energy that can be used to prioritize the requirements dictated by the underlying application rather than merely prolonging the network's life. The key challenge is to optimize the performance of the application without compromising the sustainability of the system. In this practical demonstration, we show how ODMAC is able to support the aforementioned goal in three different scenarios, namely delay-sensitive, datalogging and security-sensitive WSN applications.

5. REFERENCES

[1] KIPJACK and KEA Algorithm Specifications 2.0, National Institute of Standards and Technology. Technical report, May 1998.

[2] X. Fafoutis and N. Dragoni. Adaptive Media Access Control for Energy Harvesting - Wireless Sensor Networks. In *Proceedings of INSS'12, IEEE.*

[3] X. Fafoutis and N. Dragoni. ODMAC: An On-Demand MAC Protocol for Energy Harvesting - Wireless Sensor Networks. In *Proceedings of PE-WASUN'11, ACM.*

[4] C. Karlof, N. Sastry, and D. Wagner. TinySec: a Link Layer Security Architecture for Wireless Sensor Networks. In *Proceedings of SenSys'04, ACM.*