Engaging with Ubiquity: Students, Sensors and Security

[1]Meriel Huggard, [2]Ciarán Mc Goldrick
Trinity College Dublin, Dublin, Ireland, Meriel.Huggard@tcd.ie [1];
Trinity College Dublin, Dublin, Ireland, Ciaran.McGoldrick@tcd.ie [2]

Abstract

Pervasive networking concepts, where many different wireless networking technologies are transparently integrated into everyday objects and activities, are increasingly prevalent in everyday situations. Looking to the future, it is foreseen that billions of small Internet-enabled, ubiquitous devices will provide digital intelligence and connectivity for almost every leisure, commercial and industrial product. Interconnectivity through the Internet will facilitate seamless interfacing and interactivity with many aspects of our lives; providing smart operations in both commercial and personal settings. Wireless Sensor Networks (WSN) are hailed as one of the key enabling technologies of this ubiquitous vision and such infrastructure is commonly realised using small, low power, low data rate, wireless devices with sensing and actuating capabilities.

In this paper we detail a practical laboratory task where final year undergraduate students design, implement and validate an inferred security wireless sensor access system. We evaluate the students' experience of working with the Sun Microsystems SunSPOTs and explore how their perception of both ubiquity and security evolves from inception to completion of the activity.

1. Introduction

Keystone courses aim to provide final year undergraduate students with a learning experience that not only draws on their existing knowledge but also encourages them to engage in the professional practice of self-directed learning that is more common in the workplace. It seems natural to seek to incorporate such experiences into the laboratory-based elements of courses, as they do not sit comfortably in more traditional lecture settings. The assigned laboratory tasks should encourage students to engage with problems that reflect those seen in the workplace; students must make decisions that take them from the initial planning stages of the project, through system design, specification and implementation, to the testing and formal presentation of their final solution. The practical project outlined in this paper seeks to engage students with such learning experiences on a final year module in Mobile Communications.

2. Challenges in Delivering Keystone Modules

Accreditation bodies [1] have long emphasised the importance of credible, practical skill building and concept reinforcement as fundamental underpinnings of modern Science and Engineering programmes. Realisation of such practices frequently necessitates the use of small group and peer learning modalities for practical delivery and assessment of student outputs. Whilst the pedagogical merits of such practices have been well documented in the literature [2], there is an inherent managerial tension between the competing requirements of the quality and quantifiable outputs of the educational experience, and the "affordability" of resourcing such activities. It is increasingly common for the academic and pedagogical goals and aspirations to be subjugated to the more immediately quantifiable "cost" of resourcing such "teaching" activities.

In such circumstances it is incumbent upon educators to strive to maximise the learning and educational outcomes for their student cohorts. In doing so they encounter a somewhat more insidious impediment – the motivation and goal orientation of the individual students. In general students seek a path to quantifiable academic achievement that maximises their likely outcome for any given input. Thus modern academics must design, deliver and evolve modules that challenge, convey and inform the frontiers of knowledge; that imbue practical skills and experience of relevance to enterprise and employers; and that appear both accessible and advantageous to student cohorts.

These principles helped inform the conceptualisation and design of a practical ubiquitous computing task as a core element of a final year undergraduate Wireless Communications module.

3. Ubiquity, Sensors and Security

The term Ubiquitous Computing means different things to different groupings, but most expressions of the concept will extend Weiser's [3] original articulation ("making many computers available throughout the physical environment, but making them effectively invisible to the user") to include wireless communication capabilities. Thus a "ubiquitous computing" device will fuse computing (programmability, processing, storage) capabilities with communication (discovery, transmission, reception, routing) competences.

A wholly modern realization of such devices and capabilities can be found in the field of Wireless Sensor Networking. Individual wireless sensor devices, generically known as nodes, satisfy the primary requirements for ubiquitous computing devices. Thus the use of Wireless Sensor Network (WSN) technologies as a primary hardware vehicle for the task advances our pedagogic goals and, moreover, it contributes to strategic institutional and national aspirations that teaching be "research-led" [4,5].

There are many different families of Wireless Sensors, most of whom have their own dedicated programming and interoperability metaphors. At the outset, the students were provided a wide variety of these wireless sensor nodes and platforms, asked to choose a platform they wished to use for the task and to identify their reasons for doing so. This mirrors the real-world scenario where a professional must identify the most appropriate technology for the task in hand and establish a case for its use.

The concept of "inferred security" denotes the activity of building or inferring trust from ongoing interactions with ubiquitous computing devices. In its simplest form devices about your person spontaneously interact with other devices in the surrounding environment on an on-going basis. The nature and circumstances of these interactions will tend to characterise the communicating entities. It is practicable to exploit information arising from these interactions to infer a measure of certainty as to the likely identity of the holder of the communicating device – thereby enabling basic security and authorization capabilities.

Cellular network Location Based Service (LBS) information [6] may form a subset of the data used to provide inferred security capabilities. Such an articulation is useful as it provides an accessible reference model for students in seeking to understand the broader security concept. Moreover it also serves to highlight the nature and scope of information being routinely gathered by State Agencies – thereby engendering valuable societal and ethical debate amongst the students.

4. Building on Prior Knowledge

To properly conceptualise and design their inferred security products the student cohort must understand the fundamentals of wireless communication systems; must be cognisant of the practical limitations of generic wireless sensor nodes; must have quantified the "practical" security level required for their service; and should have satisfied themselves as to the practicalities of an implementation on their chosen Wireless Sensor Networking platform.

As the task has multifaceted pedagogical objectives (none of which are explicitly programming related) we established the following requirements for the Wireless Sensor platforms used: i) the nodes should be programmable by the students using their existing language skills; ii) the nodes should be capable of autonomous operation; iii) the nodes should incorporate existing physical phenomena sensing capabilities; iv) the node platform should include some standard data routing and dissemination algorithms [7]; v) the nodes should be capable of straightforward interfacing to external devices; vi) the nodes should be capable of computing security and cryptographic primitives in "near" real time.

From a pedagogic perspective the task is established as a minimally specified problem domain exercise. The students have complete freedom with respect to the hardware employed, the security strategy and constructs exploited, and the language and implementation environment selected. The students are aware that they must quantify and articulate a cogent rationale for their choices and selections in interview at the end of the task.

The programmability (and ease thereof) of the Wireless Sensor devices was established as a key determinant of student selection of hardware platform. As the students had significant prior experience of programming through Java, they chose the Sun Microsystems/Oracle SunSPOT platform [8] as these devices are programmed through Java/J2ME. Moreover this language familiarity also had a significant bearing on their subsequent engagement with the task. The SunSPOT was one of the more capable Wireless Sensor nodes available so the enforced choice also satisfied the preestablished platform requirements.

4.1 The SunSPOT Platform

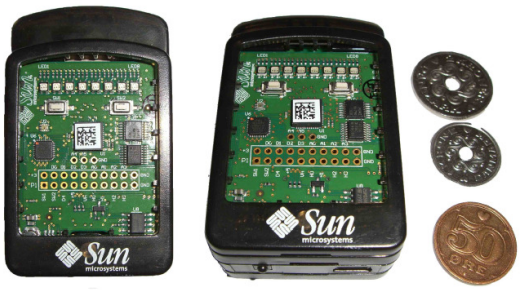

Figure 1: SunSPOT nodes, with some coins to provide scale [9]

The SunSPOT (Sun Small Programmable Object Technology) wireless sensor was developed by Sun Microsystem, now Oracle Labs (see Figure 1). The first SunSPOT model, known as rev.6, is the version employed in this task. It incorporates a 180 MHz 32-bit ARM920T microprocessor [8] with 512KB of RAM and 4MB of flash memory. The SunSPOT has 6 analog inputs readable by an onboard Analog/Digital Converter, 5 general purpose I/O pins and 4 high current output pins. The SunSPOT runs a Java ME (Micro Edition) virtual machine called Squawk which is capable of running Java bytecode on embedded devices. It is powered by a rechargeable 3.6V Lithium-Ion battery. Ad-hoc On-Demand Distance Vector Routing Protocol (AODV) is the routing protocol employed in the default SunSPOT configuration. AODV is a reactive protocol in that it establishes a route to destination only on-demand. AODV makes it

possible to transparently establish a dynamic, end-to-end, path for data transmission from a source node to a destination node, potentially via intermediate nodes [10].

The students have a number of years of pre-existing experience developing in Java, predominantly using the Eclipse Development Environment [11]. The availability of a free SunSPOT plugin [12] for the Eclipse platform allowed the students to leverage their existing familiarity with that software system to rapidly prototype code for the SunSPOT nodes.

5. The Laboratory Assignment

The aggregate task description provided to the students was as follows:

"*Sensor Inferred Security*: You'll have all heard and read about the concept of Ubiquitous, Ambient and/or Pervasive Computing. The basic concept is that everyday devices will have built-in wireless sensing and communications capabilities. It is expected that they will be used for personal body networks, health monitoring, etc. For this assignment you will design, implement and validate an inferred security wireless sensor access device.

The practical concept: You carry a wireless sensor (e.g SunSPOT) with you. Devices and structures within your everyday environment are equipped with their own SunSPOTs or functionally (from a Communications perspective) equivalent Wireless Sensors. They can interact with each other when within communications range.

The algorithm: You should document and clearly explain the algorithm/strategy/approach you are using, and why you believe it to be "best-of-breed"
The challenge: 1. When you arrive at your office door, a wireless sensor interfaced to the lock-mechanism should determine whether the lock opens using information received from your 'opener' node. 2. If your wireless sensor is lost or stolen, the stolen device should not open the office door.

Actuation: You will actuate the lock by enabling an "open" signal/output for three seconds. It is sufficient to demonstrate/simulate this in code, although an actual lock will be used on demo day.

A suggested strategy might be: i) use the wireless sensor (e.g SunSPOT) as the deployment platform; ii) produce a system demonstrator that can open an electric lock mechanism using *only* inferred information; iii) Your demonstrator must be created, tested and validated using the platform emulator BEFORE deploying on actual hardware for testing; iv) You should identify any requirements/assumptions required by your system; v) You must provide a short report, with source code, that describes who did what, how your system operates, how secure you believe your system to be, why, and provides us with feedback on your experiences."

5.1 The Implementation

To provide a "real world" practical demonstrator for the students to target, a magnetic door lock was interfaced to a SunSPOT using a Relay/Opto-Isolator circuit. This "actuator" SunSPOT sets an output pin "high" to actuate the magnetic lock mechanism and allow the door to be opened. The input required from the student developed security mechanism is limited to the activation of an output pin on the actuator SunSPOT.

To create a realistic simulation of a ubiquitous computing environment, a number of SunSPOT's were dispersed throughout an office environment, and an "opener" node was carried in a jacket pocket. The goal of the scenario is to emulate a deeply embedded ubiquitous environment where devices are integrated into everyday objects and embedded in clothing.

Whilst a variety of different solution paths were adopted by different groups, there was a commonality of challenge to be addressed by all. The initial goal was to establish programmatic control of the wireless communication function of the "opener" SunSPOT. Having done so students then sought to poll or otherwise establish the existence of (and communication with) nodes embedded in the surrounding environment. Thereafter each group proceeded to implement their inferred security strategies as they saw fit.

5.2 Security

The notion of Security has different meanings in different contexts. For instance a magnetic door lock controller requires less rigorous security capabilities than a bank safe. Thus the nature and capabilities of the security solution implemented should be both appropriate for, and proportionate to, the likely threat or compromise vectors. The student groups struggled somewhat with this distinction, with many expending considerable time and effort on "high" security algorithmic approaches, such as AES and Public/Private Key infrastructures. As communication with, and between, WSN nodes will be "best effort" using AODV, it is impractical for them to use key infrastructures as there may be no timely communication route to the server. Traditional key management and validation approaches are similarly impractical. For symmetric key cryptosystems the challenge of secure key dissemination and synchronization remains largely impractical in a WSN environment as routing practices presume regular eavesdropping and overhearing of adjacent communications. These activities were considered to be very useful in providing practical reinforcement of (hitherto) theoretical practicalities.

As time to complete the task was running out, the student cohort next considered the data they actually had available to them, and what they could credibly achieve with it, This proved to be the most quantifiably effective phase of the task, as most practical deliverables evolved from this activity. Amongst the information routinely exchanged between nodes engaged in communication activities are each node's unique identification number (nodeID). As the "opener" node moves around as part of an individual's regular daily activities, the node dynamically discovers and communicates with other nodes within its effective radio range. In doing so, the individual nodeID's get exchanged. It is possible to use this information, in combination with historical movement profiles, to "infer" a likelihood that the "opener" node is currently in the possession of the legitimate occupier of the "locked" office.

5.3 Proposed Technical Solutions

As might be expected the student solutions ranged from the straightforward through those that were technically robust and onwards to those that were also (potentially) fit for commercial purpose. The most straightforward solutions assembled a list of nodeID's for devices heard over a given time period; presented the list to the door management process and empowered it to determine whether to open the door. This solution has the attraction of relative simplicity of implementation on the "opener" node as a simple, fixed length loop buffer can be used to store heard nodeID's. An interim class of solution used one or more elements of "known" information e.g. password, in combination with the nodeID list. Synchronisation of the password information is achieved using a side-channel (e.g. Internet) and requires the "opener" node to acquire the next password from one or more pre-defined reference nodes. The most compelling implementations exploit the side channel concept to provide basic cryptographic key management and exchange behaviours. The "opener" node, or group of nodes, establishes an indexed key set at a trusted location e.g. home, car. The key generation information is available to the door, or doors, management processes via the side channel. The door queries the node for both its list of NodeID's and a specific sequence of keys from the indexed list. Once validated the door unlocks and updates a subset of the indexed keys stored on the opener node.
With the latter implementation an attacker must either compromise the backend control system or intercept all communication instances the "opener" engages in to ensure a successful attack.

6. Evaluation

When evaluating the success of this laboratory based assignment it was necessary to judge the quality of the learning and technical environment created from a number of perspectives - that of both individual students and groups of students, as well as that of the academic delivering the module. While independent surveys of courses and modules are carried out by the University's Quality Office at the request of individual instructors, these capture high level information on the students' experience of the module but fail to gather useful data on specific course elements. Hence it was necessary to carry out targeted evaluation exercises to gather qualitative and quantitative data on the students' experience of the WSN laboratory assignment. As part of their report on the assignment students were asked to provide feedback on their experiences. It was made clear to students that this feedback would be used to refine future presentations of this assignment and they were encouraged to be as constructive as possible in their comments.

6.1 Quantitative Evaluation

This laboratory assignment was the third continuous assessment (C.A.) exercise for the module undertaken by the student cohort and it came close to the end of the academic year. It is usually the case that as the academic year progresses the student's grades on C.A.'s decline. This can be attributed to a number of factors including (i) student fatigue as the semester progresses, (ii) the time available to work on the assignment is reduced as students have begun working towards the end of semester examinations and (iii) increased student workload as many academics delay setting assessment exercises until the students have a chance to assimilate material covered at the start of the academic year.

It was notable that students scored significantly higher on this assessment than on the previous two assignments. Two tailed paired t-tests were performed on the three data sets and the resultant p-values are given in Table 1. It can be seen that the difference in student performance on the WSN assignment is significantly different from that on Assignment 1 (at the 99.2104% level) and Assignment 2 (99.9482% level). This increase in student grades was attributed to their level of engagement with the assignment – indeed it was necessary to remind some of the students that the assignment was just one element of one module out of the five or six modules they were taking at that juncture in their final year. It was important to encourage the students to place the assignment in perspective as the amount of time they were spending on it seemed (proportionately) high.

Table 1: Two-tailed Paired t-test results for Student Performance on the Continuous Assessment Exercises

	p-value
CA1 vs CA2	0.782164
CA1 vs WSN Assignment	0.001896
CA2 vs WSN Assignment	0.000518

In addition to the more general survey carried out by the University Quality Office, targeted survey forms were completed by the students in order to collect feedback specific to the WSN laboratory element of the course. The answers were given using a five-level Likert [13] scale (1- Strongly disagree, 2 - Disagree, 3 - Neither agree nor disagree, 4 - Agree and 5- Strongly agree). The results show that students' satisfaction with the WSN laboratory assignment is very high.

Table 2: Students' Evaluation of Learning Outcomes

Question	*Average Score (1:Strongly Disagree to 5: Strongly Agree)*
The WSN laboratory task was interesting	4.08
Participating in the WSN lab was beneficial	4.17
The laboratory provided me with an opportunity to use my existing skills and knowledge	4.5
The laboratory contributed to my practical knowledge of wireless communications technologies	4.25
I was satisfied with the laboratory set-up (technologies and facilities available to me, assignment description, assignment assessment)	4.33

6.2 Qualitative Evaluation

The final reports from the students contained their reflections on their experience. Students were encouraged to provided constructive feedback that would help refine the learning experience for future student cohorts. Once the assignment had been completed and graded, student comments were collected as part of the targeted survey on the module.

The students' comments reflected a high level of satisfaction with the laboratory assignment. They commented favourably on the hands-on experience of real world technologies ("practical and relevant"). Others mentioned the freedom they were given throughout the course of the assignment ("plenty of choice") and the fact that they were made responsible for decisions on the most appropriate technology to use from amongst those provided for them ("We were allowed to decide which mote to use and given the chance to play with a few different types of mote before we made our decision"). Some students felt the laboratory should be given to them earlier in the academic year so that they could have more time to work on it ("more time needed to really get it working", "make it longer and get rid of (CA2)"). One or two groups felt a bit overwhelmed by the freedom given and found the assignment quite challenging ("no sample code given", "no relevant examples on the web"). They also expressed dissatisfaction with a perceived lack of direction and guidance ("don't keep saying `you decide'"). However they were repeatedly reminded that they should consider themselves in a professional setting where they are the people charged with planning and executing the project and that management focus will be on a final, validated solution to the problem.

7. Conclusion

A novel wireless sensor network laboratory that encourages students to engage with the concepts of ubiquity and security was presented. The lab formed part of a keystone course for final year undergraduates and builds on their prior learning by encouraging them to engage with a real world problem of the type they might experience as professionals in the workplace. The student reaction to the laboratory learning experience was very positive and they particularly enjoyed the practical, hands-on experience with state-of-the art wireless sensor networking technologies.

References

1. ABET, “Criteria for Accrediting Computing Programs, 2011-2012 Review Cycle”, http://www.abet.org/Linked%20Documents-UPDATE/Program%20Docs/abet-cac-criteria-2011-2012.pdf
2. Meriel Huggard and Ciaran Mc Goldrick, “Computer Experience - Enhancing Engineering Education”, *International Conference on Engineering Education*, Puerto Rico, USA, 23 - 28 July 2006, 2006, pp.T4C-21 - T4C-25
3. Mark Weiser, “The Future of Ubiquitous Computing on Campus”, *Communications of the ACM*, 1, 1998, pp.41-42
4. Trinity College Dublin, “Strategic Plan 2009-2014”, http://www.tcd.ie/about/content/pdf/tcd-strategic-plan-2009-2014-english.pdf
5. Irish Government, National Development Plan 2007-2013, http://www.ndp.ie
6. Meriel Huggard and Ciaran Mc Goldrick, “Practical Positioning Projects: Location Based Services in the Laboratory”, *Proceedings Frontiers in Education 35th Annual Conference, Frontiers in Education*, Indianapolis, Indiana, 19 - 22 October 2005, Institute of Electrical and Electronics Engineers, 2005, pp.S3F-1 - S3F-6
7. Ciaran Mc Goldrick, Michael Clear, Ricardo Simon Carbajo, Karsten Fritsche and Meriel Huggard, “TinyTorrents - Integrating Peer-to-Peer and Wireless Sensor Networks”, *Sixth International Conference on Wireless On-Demand Network Systems and Services, (WONS)*, Snowbird, Utah, 2-4 February 2009, Institute of Electrical and Electronics Engineers, 2009, pp.119-126
8. Oracle/Sun Microsystems, “Sun SPOT Theory of Operation”, http://www.sunspotworld.com/docs/index.html
9. Waqas Ahmed, Meriel Huggard and Ciarán Mc Goldrick, An application adaptive energy model for wireless sensor nodes, *Proceedings of the 6th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks (PE-WASUN'09)*, Tenerife Spain, 26-30 October 2009, Association of Computing Machinery, 2009, pp.147-150
10. Ricardo Simon Carbajo, Andrea Staino, Kevin P. Ryan, Biswajit Basu and Ciarán Mc Goldrick, “Characterisation of Wireless Sensor Platforms for Vibration Monitoring of Wind Turbine Blades”, *Irish Signals and Systems Conference*, Dublin, Ireland, 23-24 June 2011, To appear
11. Eclipse Foundation, “Eclipse Integrated Development Environment”, http://www.eclipse.org
12. Giacomo Ghidini, “Project Sun SPOT Eclipse Plugin”, http://crewman.uta.edu/sunspot-projects-crewman
13. Rensis Likert, “A Technique for the Measurement of Attitudes”, *Archives of Psychology*, 140, 1932, pp.1–55.