Book Review

Cyber–Physical System Design With Sensor Networking Technologies

Scott Davidson

The book *Cyber-Physical System Design With Sensor Networking Technologies* edited by Sherali Zeadally and Nafaâ Jabeur consists of a collection of papers on cyber–physical systems (CPSs) and the wireless sensor networks (WSNs) used to transmit data and control to and from them. You have seen this subject in *IEEE Design&Test*. CPS might sound a bit exotic and of limited interest to the average engineer, but the first takeaway I got from this book is that CPS is already pervasive in our world and is becoming more so. This is a subject you should be interested in.

First, what are CPSs and WSNs? Each of the 13 chapters in this book contains a definition, and they are all slightly different. Here is one from the abstract in Chapter 1: "CPSs thus do some physical activity—perhaps turning on heat in a thermostat, or opening a valve to inject drugs in a medical CPS. Thus computing is a physical act"; and from Chapter 5: "The CPS is a system that can efficiently integrate both cyber and physical components by leveraging modern sensing, computing, and networking technologies."

Basically, a CPS is a system that does something in the real as opposed to the virtual world. A video game system where a bad guy punches your character is not a CPS. One where the bad guy punches you through some sort of wearable hardware is.

The definition of a WSN is slightly clearer. Again from Chapter 1: "A wireless ad hoc network is a decentralized type of wireless network, where communication does not rely on a preexisting infrastructure, such as routers in wired networks or access points in infrastructure-based wireless networks."

Consider connected automobiles. Each car is a sensor in that it measures speed among other things. It transmits its speed to nearby cars using an ad hoc network, since the set of nearby cars will be changing rapidly. And each car is also a CPS, since it will use the information from the ad hoc wireless network to do physical work, such as decelerating or even using the brakes, when it learns of congestion ahead. Many more examples appear in the book.

The domain of WSNs and CPSs ranges from nationwide power grids to forests where WSNs can detect fire and disease to a household and down to our bodies, in wireless body area networks described in Chapter 9.

The first two chapters of the book describe the fundamentals of WSN and CPS, quite well. I would have preferred if the sections redefining these would have been removed in each of the subsequent chapters.That would make the book more consistent and more readable.

Chapter 3 discusses the integration of CPS with WSNs. Many CPS devices will run on batteries and might be hard to access, so restricting power consumption is vital. The system must be adaptive in the sense that it can handle nodes going out of service, and still offer a given quality of service. A very large network of wireless sensors will generate massive amounts of data, so some measure of data analytics must be built into the network to filter the data before it reaches data repositories. We will see these issues being repeated later in the book. All in all, Chapter 3 offers a good overview of the problems that need to be solved.

Digital Object Identifier 10.1109/MDAT.2017.2655504
Date of publication: 4 May 2017.

Copublished by the IEEE CEDA, IEEE CASS, IEEE SSCS, and TTTC

Chapter 4 describes high-level CPS architectures, and how they meet the constraints described in previous chapters—which are described again. Some examples are given to demonstrate how different applications call for different architectures.

Security is a major threat to CPS networks, one which I do not think gets adequate coverage throughout this book. Chapter 5 covers security, using as an example two types of data injection attacks on the smart grid—falsifying demand data (such as creating more demand than truly exists) and falsifying supply data, for instance, decreasing the reported supply. This can impact the energy market place, causing spikes in prices, for instance, if the demand increases.

I am not buying it. How anyone benefits from this attack is not explained. Energy prices can certainly be manipulated—I personally enjoyed the fruits of Enron's manipulation of the California market. However, utilities have good models of energy demand on a day-by-day basis. A major spike in demand for no reason is not going to go unnoticed, so the effect of the attack would be short-lived. I am sure the same is true for supply. A decrease in supply would be investigated. Figure 5.6, which shows increased cost from an attack on supply data, is done assuming 30% of supply nodes are compromised—which seems like a lot to go unnoticed.

I wish a better example had been chosen to highlight this very real problem.

Chapter 11, on resilience, is also concerned with security and availability. Given that it is impossible to totally secure a widely dispersed network, how can we ensure that the network is still available after an attack? Security is a preattack concern, while resilience is a postattack concern. Some excellent real examples are given as to how lack of resilience can cause massive damage when a system is attacked. This chapter makes a convincing argument about why resilience is vital to consider even in lower end systems. This is an excellent contribution.

Chapters 6–8 give details on the factors that must be considered when constructing a WSN–CPS system. Chapter 6 covers data management. The difference between data management here and in a WSN-only system is that the CPS devices are mobile, they often have to react to events in a constrained period, and that it is often important to extract high level data in the network to reduce communication costs. Chapter 7, on routing, gives a good idea of the complexities involved in getting information from mobile sensors to a repository, given constraints of power, time, constant change of sensor location, and the certainty that some sensor relays will be out of service.

Chapter 8 discusses resource management, in the sense of determining the routing and communications jobs nodes in the WSN will do. How can we efficiently allocate resources bottom up, with each node deciding the role it will play? This is not a simple problem. If nodes do not take on relay tasks in order to conserve power, the bandwidth of the network as a whole will be diminished. If some nodes are too eager to relay, they might become congested and will have a short battery life. This chapter looks at some solutions from game theory. It is interesting, but more for the specialist in this area.

There are a lot of instances of these systems already deployed, and even more proposed. The rest of the book surveys the literature and presents many examples. Chapter 9 surveys approaches to mobile sensor networks, and Chapter 10 describes ways of building intelligence into the network. Although each of these chapters is reasonably well focused, there is still a lot of overlap between them and between the previous chapters.

Chapter 12 gives many case studies of potential CPS applications, and is the most accessible chapter, the most fascinating, and the scariest.

Why scariest? Consider the section on smart house systems. One such system learns when the occupants of a house use hot water, and controls the water heater to turn on when needed, saving energy and water.

However, consider the intelligent lighting system also described. This tracks the locations and activities of people in a house, and adjusts lighting to meet their needs—say reading versus watching television. Sounds good? But do we really want a database of our locations and activities in a system that can be and will be hacked.

Then we can get too far. Section 12.5.3 talks about road safety helpers, where the back camera of a smartphone is used to detect approaching vehicles to warn a pedestrian of danger. It is claimed that this will help protect a person engaged in a phone call while crossing a road. If the camera is pointed the right way. If the system can respond in time. If the person engaged in the call will respond in time to the warning. I think paying attention while crossing streets might be a better solution.

The CPS applications described here come from the literature, so we cannot blame the authors of this chapter for them, but I would have liked the survey to comment on privacy issues, and be a bit more critical of the more outlandish proposals—which I am glad were included.

The last chapter is an equally fascinating one on medical applications. Some applications are for an assisted-living scenario where sensors can detect emergency situations faster, especially as there are more elderly and fewer who can care for them. Again, there is scant discussion of privacy issues as medical data are assumed to be aggregated into central repositories. However, the scariest phrase I have seen in a technical book for ages is "augmented cognition" for dementia patients, which involves augmenting memory through tracking eye movement and communication through sentence fragments. Details are not given.

In sum, I got a lot more out of this book than I expected to. CPS systems are going to surround us soon. The writing is good and accessible in general, and while a nonexpert may want to skim some parts, there is a lot of interest for everyone. There is a lot of redundancy in terms of definitions and examples. I minded this reading from beginning to end, but a reader should be able to get value from looking at chapters individually. As a nonexpert I do not know if this is the best book in the area for a specialist, but it worked well for me.

■ Direct questions and comments about this department to Scott Davidson; Davidson.scott687@gmail.com.