J Internet Serv Appl (2012) 3:41–49
DOI 10.1007/s13174-011-0057-4

SI: FOME - THE FUTURE OF MIDDLEWARE

Resilient dependable cyber-physical systems: a middleware perspective

Grit Denker · Nikil Dutt · Sharad Mehrotra · Mark-Oliver Stehr · Carolyn Talcott · Nalini Venkatasubramanian

Received: 24 November 2011 / Accepted: 30 December 2011 / Published online: 28 January 2012

Abstract In this paper, we address the role of middleware in enabling robust and resilient cyber-physical systems (CPSs) of the future. In particular, we will focus on how adaptation services can be used to improve dependability in instrumented cyber-physical systems based on the principles of "computational reflection." CPS environments incorporate a variety of sensing and actuation devices in a distributed architecture; such a deployment is used to create a digital representation of the evolving physical world and its processes for use by a broad range of applications. CPS applications, in particular, mission critical tasks, must execute dependably despite disruptions caused by failures and limitations in sensing, communications, and computation. This paper discusses a range of applications, their reliability needs, and potential dependability holes that can cause performance degradation and application failures. In particular, we distinguish between the notion of infrastructure and information dependability and illustrate the need to formally model and reason about a range of CPS applications and their dependability needs. Formal methods based tools can help us design meaningful cross-layer adaptation techniques at different system layers of the CPS environment and thereby achieve end-to-end dependability at both the infrastructure and information levels.

Keywords Cyber-physical spaces · Formal models · Reliability techniques · Reflection · Infrastructure resilience · Information dependability

G. Denker · N. Dutt · S. Mehrotra · M.-O. Stehr · C. Talcott · N. Venkatasubramanian (✉)
Department of Computer Science, University of California, Irvine, USA & SRI International, Menlo Park, USA
e-mail: nalini@ics.uci.edu

G. Denker
e-mail: denker@csl.sri.com

N. Dutt
e-mail: dutt@ics.uci.edu

S. Mehrotra
e-mail: sharad@ics.uci.edu

M.-O. Stehr
e-mail: stehr@csl.sri.com

C. Talcott
e-mail: clt@csl.sri.com

1 Introduction

Recent advances in embedded computing, networking, and stream data management technologies have made it feasible to create Cyber-physical Systems (CPS) that can sense and affect their environment in different ways and with different levels of sophistication. A common definition of a cyber-physical system is one that "*integrates computing and communication capabilities with the monitoring and/or control of entities in the physical world dependably, safely, securely, efficiently, and in real-time*." Such systems provide complex, situation-aware, and often safety- or mission-critical ecosystems and services. Examples of such CPS ecosystems include engineering systems such as intelligent transportation systems (air and ground), smart power grids, structural monitoring and control of civil infrastructures such as bridges and dams; medical/healthcare systems (for assisted living, patient monitoring in hospitals, automated laboratories); smart spaces (buildings with surveillance and microclimate control); smart agriculture; flexible manufacturing systems (with self assembling structures); systems and processes used in defense, homeland security and emergency response (ad hoc ground/airborne combat teams, intelligent firefighting, etc.). In the medical domain, for example, the

CPS ecosystem must bring together information from numerous devices that capture diverse physiological factors—such as heart rate, temperature, or oximetry—for diagnosis, treatment and care; many of these devices are typically designed for isolated use; the composition of these devices to design perpetual life assistants for busy, older or disabled people and location-independent access to world-class medicine is a grand challenge. In the area of intelligent transportation, advances are being made to achieve safe and efficient transportation at the level of individual vehicles (e.g., the CMU urban autonomous vehicle that drives with other vehicles, lanes, and intersections [1]), and enable significantly reduced traffic congestion and delays (e.g., the Cartel project [37] uses location of mobile phones and custom-built on-board telematics devices to enable traffic mitigation and road condition monitoring. Smart and Secure Power Grids are exploring how to change the process of power generation and distribution, orchestrate power usage to realize more sustainable societies with blackout-free electricity generation/distribution and net-zero-energy buildings.

Unlike pure sensor networks, CPSs can perform physical actions and are usually characterized by (distributed) control loops through which the environment provides essential feedback. Unlike traditional Sensor/actor networks, node and communication capabilities of emerging CPS ecosystems can vary significantly. For instance, in addition to resource-constrained embedded sensor/actuator nodes, devices carried by humans (e.g., PDAs), energy-rich nodes attached to vehicles (e.g., laptops), resource-constrained UAVs, as well as nodes with continuous Internet connectivity (e.g., ground stations and computationally powerful grid nodes) can all be part of the same CPS ecosystem.

We highlight key observations (derived from real world experiences in developing and deploying CPS systems) that indicate a paradigm shift in the future generation of cyber-physical systems. The *first* of these is a move from a device-centric view of CPS to an information-centric view. We argue that a broader, information-centric perspective is essential in upcoming CPS applications where *sensemaking* of the captured information is used to drive decision-making and control. In our expanded view, we observe that CPS applications today exhibit two levels of operation:

(a) a lower level hybrid control loop that enables automated actuation and management of networks of embedded devices, e.g., automated brake control in vehicular CPS;
(b) a higher level information centric loop, used to make slightly longer term decisions (by a human operator sometimes) that actuates new behavior. Such a "logical actuation" of the underlying system can exploit additional knowledge—third party information sources, historical and prior data, domain expertise, etc.

The latter aspect is gaining importance and presents many interesting opportunities for middleware-driven orchestration of CPS. For example, knowledge of how a building fire is propagating (extracted from multiple sensory feeds) can enable better deployment of firefighter resources. A *second* interesting observation is that in many of the above CPSs, there is an increased use of a human-in-the-loop (in lieu of the completely automated approach), where CPS systems provide situational awareness to humans who are decision makers. For example, power grid systems have humans that control usage; operators that control distribution and even control generation (reselling of power generated by solar panels back to the grid). Similarly, healthcare applications involve patients, doctors, nurses; individuals—all of which can impact how information is obtained and processed. Transportation systems have drivers with behaviors that control low-level braking behavior in cars; or user travel patterns that create congestion. Emergency response systems are inherently a human-oriented process where individuals in response agencies, onsite first responders, and citizens make decisions that can save lives and property. Such systems are especially interesting since they are complex heterogeneous networked systems with humans and (autonomous) agents in the loop—this brings about sociotechnical issues in the deployed cyber-physical systems. A *third* observation is that the information used in CPS environments is increasingly multimodal in nature with diverse data types (small sensor readings, images, video, audio/speech, text, and social media). Information may be structured (e.g., relational tables), unstructured (free form text) or semistructured (spatiotemporally tagged event data). This trend presents both an opportunity (due to the rich nature of the information) and challenge (added complexity due to volume of data and real-time processing needs).

In this paper, we discuss a specific example of an information-centric, human-oriented CPS that will benefit from the expanded view described above—i.e., that of an instrumented cyber-physical space (ICPS). It is possible today to build smart spaces that integrate a variety of sensing and actuation devices to create a digital representation of the evolving physical world that can then be exploited by applications for a variety of purposes. Such instrumented Cyber-physical spaces (ICPS) are technologically cutting-edge and exemplary of highly instrumented spaces of the future; Fig. 1 illustrates an example of such an ICPS. ICPSs are being explored, in both academia and industry, in a variety of application contexts including critical infrastructure monitoring and surveillance, maritime and port security, at-home patient monitoring and assisted living, and incident site situational awareness for improved emergency response. Many of these applications are mission critical (e.g., command and control, medical triaging, incident command systems for first responders) and involve decision making by

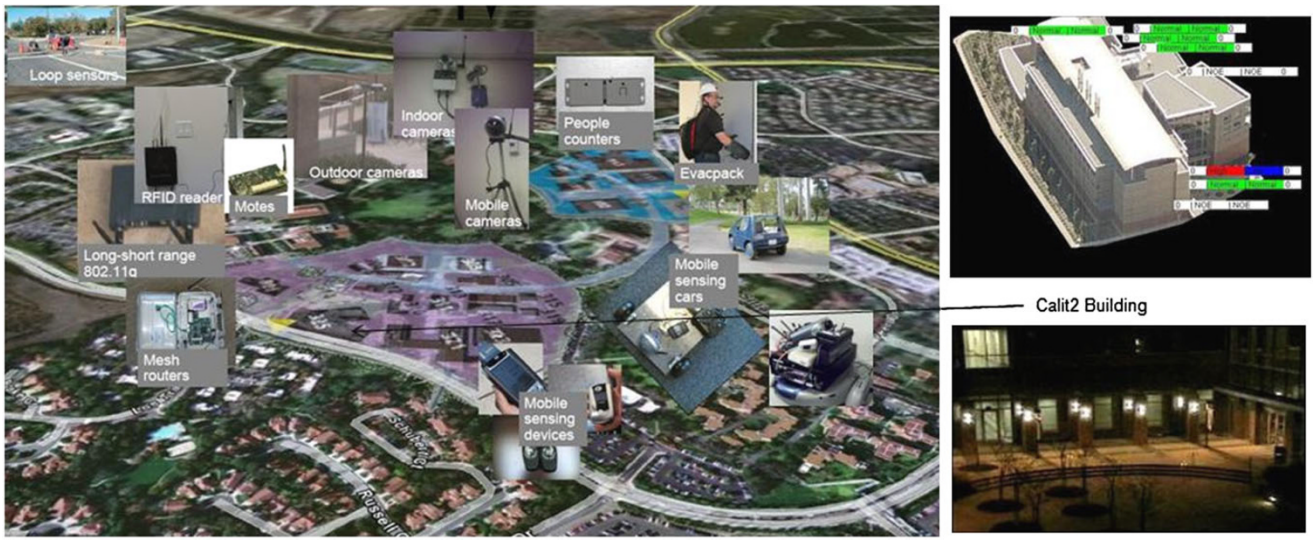

Fig. 1 Responsphere—an instrumented cyber-physical space at UC Irvine

humans who, through situational awareness systems, observe dynamically changing environments and respond to critical events. Indeed, the larger deployments exemplify a societal scale CPS system with a broad range of users and devices.

1.1 Challenges in designing and deploying cyber-physical systems

The dynamic, heterogeneous, and large scale nature of CPS systems create interesting challenges in their real world deployment. The first issue is that of *architectural configuration and management*—there is a need to determine the degree of decentralization and hierarchical control in the overall networked CPS environment based on its scale and connectivity characteristics. *Interoperability* poses a critical challenge in CPS systems at multiple levels—(a) Sensor and platform heterogeneity that arises due to the varying sensing, computational, and storage capabilities of diverse devices; (b) network heterogeneity due the diverse communication media that interconnect devices to application servers (e.g., wired Ethernet, WiFi, cellular, MANETS); application interoperability where information from the same underlying physical infrastructure is simultaneously repurposed for multiple applications (e.g., surveillance, social networking).

Implementation of the information centric approach to achieve system wide objectives (discussed earlier) poses significant challenges. Enabling the transition from sensing to sensemaking implies the need for programming information centric applications on a heterogeneous infrastructure of devices/networks. This in turn requires the development of abstractions that translate device-level features into those required by applications. In addition to the real-time, resource-limited, reactive aspects of traditional embedded systems, information centric CPSs must embody a situation awareness that reflects the overall distributed system and its environment. Local situation awareness of a network node is not sufficient. Each node must maintain a model of its local, directly observable situation together with models about the rest of the network. Furthermore, different nodes may have different degrees of awareness according to their capabilities. Asynchronous actions must achieve a desired overall coherent effect. An advantage of multiple distributed nodes is that resources can be pooled and limitations can be partially overcome by cooperation. To realize the potential benefits of pooling resources (energy, CPU cycles, memory, bandwidth, sensors/actuators), it is necessary for the different processes/layers on each node to adapt resource usage (setting parameters, choosing policies) to achieve system-wide objectives, not just local goals.

A dynamic CPS environment needs to be open in the sense that nodes may come and go. In fact, a system may assemble "on the fly" for a given purpose. Mission-critical systems may be scaled up or down depending on mission requirements. This points to the need for management frameworks that exhibit *agility and flexibility* and reduce deployment, integration, testing time. Another factor that is gaining importance in recent deployments is the *sustainability* of the CPS ecosystems that are being created. The battery-operated nature of the wireless devices in these infrastructures creates issues of maintenance; it also raises issues as to the energy/environmental costs vs. the benefits of having such infrastructures in the first place. The design of self-sustaining, green low carbon footprint CPSs is a topic of recent research. Other topics include the ability to set up instant CPSs rapidly where little capability exists, and ensuring the *privacy* of individuals embedded in cyber-physical spaces that are being monitored and adapted.

While there are several challenges in building CPSs, the remainder of this paper focuses on the issue of dependability and resilience in CPS systems. Section 2 motivates the need for resilience in CPS and describes the different forms of dependability in a CPS system (infrastructure and information dependability) through a motivating application. Section 3 discusses challenges in the modeling of dependability characteristics in CPS systems and uses formal methods to model and reason about dependability needs in CPS applications. Section 4 presents potential techniques and promising solutions to may enable improved infrastructure/information dependability. We conclude in Sect. 5 with potential research directions.

2 Resilience/dependability in CPS

This paper focuses on the prime issue of CPS resilience—that ensures dependable operation of the system despite small changes in ambient conditions or large perturbations (extreme events, crises) to the underlying infrastructure. Dependability, as defined by the IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance, refers to the trustworthiness of computing systems that allows reliance to be justifiably placed on the services it delivers. Resilience is a closely related concept [22] and refers to "the ability to recover from or adjust easily to or change;" in other words, "the persistence of dependability when facing changes." In particular, mission-critical applications require the underlying systems to be dependable despite disruptions in the infrastructure that cause failures in sensing, communications, and computation. Dependability constitutes a variety of nonfunctional requirements including availability, reliability, maintainability, safety, and integrity. In the context of CPS, dependability can broadly be classified at two interdependent levels that, combined, can provide a trustworthy platform for building applications.

- *Infrastructure dependability*—how dependable are the underlying infrastructure components (e.g., sensors, networks, actuators, computing/storage elements, software environments) in the presence of diverse failures that may lead to disruptions, and
- *Information dependability*—how dependable is the information generated by the underlying infrastructure given errors/uncertainty in information input (e.g., sensor readings) and data analysis mechanisms.

Several key aspects of dependability must be considered to enable resilience in CPS environments. First, dependability is an end-to-end system property—disruptions at any level of the system (hardware, OS, network, software) can hinder application needs—examples include packet drops at the network layer due to congestion, and bit flips in the architectural layer due to soft errors. Second, the underlying system is inherently dynamic—to support dependability, a structured approach to realizing adaptability is essential, especially when the CPS is long-lived and must operate under unpredictable situations. Third, designing for both adaptability and dependability requires the ability to reason about system evolution and determine whether adaptations performed meet the dependability needs. One of the key issues in the deployment of large scale CPSs today is a lack of understanding of the resilience properties of these systems. Fourth, an CPS environment contains heterogeneous sensing components that generate torrents of multimodal data delivered over heterogeneous networks (wired, wireless). Also, resource limitations exist at multiple levels, making it difficult to capture, deliver, and process information on-the-fly. The challenge lies in developing a management infrastructure that can detect, and cost-effectively handle environment changes while meeting dependability needs.

We argue for a principled approach to developing a management framework for dependable CPS. Closed loop control where sensor-driven observations cause dynamic adaptations to CPS devices is a driving philosophy in multiple CPS applications, e.g., building energy management [33] and healthare [24]. Recent CPS projects such as CYPRESS [13] and fractionated CPS (http://ncps.csl.sri.com/) explore an "observe-analyze-adapt" architecture, i.e., a reflective approach, in which a CPS has a model of itself, its objectives, and its effects on the environment; the CPS achieves dependability objectives through adaptation using runtime application of formal analysis methods. Such a framework enables researchers to explore a range of cross-layer dependability techniques ranging from networking and messaging technologies to adaptive information fusion.

The ability to monitor and adapt has far reaching outcomes in other domains as well. For example, a home health monitoring scenario will consist of RFID-enabled smart pillboxes, video cameras for determining the patient's location, and on-patient body area networks consisting of polar straps for heart rate, oximetry for respiratory conditions, accelerometers to determine position and ambulatory behavior, galvanized skin response sensors, and so on. A building automation application can be developed where information from sensors (cameras, motion detectors) can be used to determine building occupancy and consequently control the lights, elevators, and HVAC systems. Infrastructure and information reliability issues arise in all these scenarios; all require reliable detection of critical events from multiple sensors and the consequent triggering of actions to initiate appropriate response is crucial in all cases. Through the design of suitable adaptation knobs/techniques, applications can achieve reliability and gracefully deal with infrastructure failures.

2.1 A driving scenario

To illustrate how adaptability can help realize dependability in mission-critical applications, consider the normal functioning of a high-rise campus building instrumented with sensors for a surveillance related application—the surveillance scenario morphs into a situational awareness CPS application, called SAFIRE [34] when there is a fire in the building. Several calls are received at the 9-1-1 call center reporting a fire in a chemistry laboratory located in a high-rise building on a university campus. While fire and hazmat resources are en route to the scene, the CPS application unlocks access to resources pertaining to the particular location and type of incident that otherwise would not be available under normal circumstances. These could include (a) detailed floor plans of the relevant building, (b) an up-to-date inventory of hazardous materials obtained live via a campus chemical inventory database (c) connection to the building surveillance cameras allowing video feeds to be observed from inside the building. These resources and contextual information are made available to the incident commander and other first responders via networked terminals installed in the fire apparatus and command vehicles [34]. Fire personnel may place or carry additional sensing and networking equipment to augment the information capture capabilities at the incident site. Another CPS client application, a firefighting assistant, is initiated to provide a communications infrastructure that can dynamically configure itself according to need, make use of resources as available.

Over the past 2 years, our team has conducted experiments in a controlled instrumented campus environments (UCI Responsphere, www.responsphere.org) and more realistic structural fire drills (including live burns held in conjunction with first responder partners in different test sites in Orange County, California). The following observations were made [14]: (1) In CPS applications such as assisted firefighting, failures will happen; *there is no time to diagnose the problem on the spot, much less to reconfigure computers, swap/recharge batteries, or change cables*. Failures are aggravated by the presence of hazards such as fire. (2) *Current network mechanisms are sensitive to noise*. Experiments using WiFi infrastructure networks for transmitting multimodal speech and video data demonstrated a significant drop in information quality even with limited network noise; exploiting ad hoc communication is beneficial even when infrastructure may be available. (3) *Network topology and its degree of stability impacts reliability*. Mobility further reduces reliability and increases convergence time. To enable infrastructure dependability, the system will dynamically prioritize information captured by sensors in the impacted area (e.g., camera feeds showing entrapped victims) to flow through available networks. To illustrate information dependability, consider in the same scenario, a temperature and gas sensor feed that shows an anomalous reading (e.g., heightened temperature and CO levels). In this scenario, the ICPS provided critical information needed to respond to the hazard (e.g., the presence of water-reactive chemicals in substantial quantities). It provided a means to utilize observational capabilities of the building infrastructure (locations of alarm panels and cameras), automatically incorporating new components when they become available. In the following sections, we discuss two key directions for further work (a) cross-layer modeling of the CPS environment and evolving state; (b) resilience techniques for infrastructure and information dependability.

3 Modeling CPS systems and dependability needs

The physical resources and infrastructures in a CPS span multiple scales (e.g., sensors capturing real-time events at the hardware layer, to networked communication for dissemination of critical information from event sources to multiple destinations). A key challenge in managing the disparate abstractions in the logical, physical, and temporal dimensions is the consistent cross-layer modeling of information flow across these abstractions. A modeling framework is required that can capture the layered CPS architecture and application needs, analyze current system state, detect violation of end-to-end dependability requirements, and reason about the validity of adaptations. To determine the best strategies for adaptation, a system that can carry out gedanken experiments to predict the outcomes under different policies or parameter settings is best suited (e.g., reflective route planning for DTNs [36]). To enable such gedanken experiments, a system must have a representation of and reason about itself. This can be achieved through executable models of the system that have well-described state and behavior in a framework with well-defined reasoning principles. Such formal executable models can then be used for reasoning and analysis, and relating dependability constraints (e.g., accuracy of measurement or expected timeliness of data delivery) to component parameters. The verification and validation of CPS is notoriously difficult and conventional techniques are too expensive; factoring out the minimal functionality common to CPS is a first step toward making verification feasible, because the cost of verification can be amortized over many instantiations of the common framework. This is far from enough, however, because mission-specific properties and performance metrics will require verification, also, and the mission-specific software will typically be much more complex than the minimal framework. Furthermore, conventional verification cannot enable rapid deployment at acceptable cost.

The use of formal methods to ensure safety and dependability in CPS is a topic of much interest [3, 23, 24] in CPS

domains including transportation, healthcare, and avionics. For example, the CYPRESS [13] and NCPS[1] projects are exploring the use of the Maude rewriting logic language and environment [11, 26] for developing the formal models of CPS. Rewriting logic is well suited to model concurrent systems; techniques have been developed to treat time [28] and probabilistic features [20]. Modeling and analysis in a formal framework, such as Maude, can then be used to prototype ideas, develop techniques to analyze design decisions, and inform observation/adaptation decisions.

As a sample use case of the formal model, let us consider the dependability of the CPS communication infrastructure which consists of diverse technologies [12] such as wired Ethernet, WiFi, cellular, Zigbee, mobile ad hoc (MANETs), mesh, and personal area networks (PANs). Various failures can lead to message delays or latencies in the combined wired/wireless networks, and thus impede the flow of information to CPS applications. In general, verifying optimized operation or fault tolerance over a general space of network architectures is an intractable problem. By analyzing and verifying selected points in the network architecture space, the network structure can be varied to provide protection mechanisms against faults. For example, one may choose standard or high-integrity network components (that provide additional protection using self-checking pairs); techniques for path and system redundancy can be incorporated to provide protection against failures. Equipped with a formal specification of the network components, network architectural choices and input traffic, analysis tools can be developed for fault and performance analysis. For example, in a camera surveillance scenario, we can analyze the communication network to predict the likelihood that there is no surveillance data for an area. Similarly, considering different camera collection schedules may provide more (or less) surveillance, resulting in more (or less) frames in the network. Such analysis will help generate improved failure models and devise strategies to couple such models into the larger CPS framework.

4 Techniques to support resilience in CPS

Sensors, devices, communication medium, and the application context are subject to constant changes or failures in dynamic environments. For example, devices can be turned on and off, or moved from one place to another; networks may be congested and packets are dropped; the target (e.g., monitored person) may move from one building to another. At the information level, sensed information may be imprecise and the dynamics of the event may require different information to be captured. We discuss techniques at the infrastructure and information level to handle such changes.

[1] http://ncps.csl.sri.com/.

4.1 Infrastructure resilience techniques

To illustrate issues at the infrastructure-level, let us consider the specific case of enabling communication infrastructure dependability in CPS. In the context of multiaccess networks, techniques have been developed for network handoff [27, 32] power management [19] and monitoring [4], and QoS support [30]; enabling techniques for specific combinations of networks (cellular/ad hoc [8, 25], cellular/Wi-Fi [29], Bluetooth/Wi-Fi [2]) have been explored. Many of the proposed techniques are at the network and lower layers; adaptability to unexpected failures and surge demands is difficult to orchestrate at these lower layers. A middleware driven approach to managing communication over diverse network technologies can help leverage the components' network capabilities seamlessly in a quality sensitive manner. Recent work has developed techniques where nodes can communication decisions locally, using available knowledge of network status and taking into account tolerance parameters (timing, accuracy, reliability) [31, 36]. What is new and challenging is using these ideas to deal with the overall CPS multinetwork infrastructure.

Exploiting multiple access networks: One approach to enhance communication reliability is by combining the capabilities of multiple access networks to form reliable connected networks. The first step toward this is to be able to structure a complex network of networks and design a management system that captures and maintains network state information efficiently in a logically centralized DB. Such a multinetwork management system must be able to scale to large number of devices and deal with the dynamic aspects induced by mobility. Intelligent exploitation of hierarchy and clustering can help structure a network architecture, techniques for "intelligent gateway placement" are required to connect networks (e.g., cellular backhaul to a on-site wireless mesh network [39]) and enable smooth flow of information. The underlying state collection mechanisms must minimize the overhead of state capture (number of messages, power consumption) while meeting time, frequency, or accuracy requirements. The multinetwork environment must also include techniques for exploiting concurrency across the multiple networks—joint routing [15] of CPS data across multiple access networks using adaptive access selection [5, 6, 21], content fragmentation, bandwidth aggregation [9], and network coding [17], thereby leveraging the bandwidth/resource provided by multiple networks to attain communication performance that cannot be achieved by any single network alone. The challenge is to effectively exploit path/access diversity while considering the content specifics, user priorities, and information timeliness/reliability needs.

Exploiting mobility in disconnected networks: In CPS scenarios with high mobility and sparse deployment, main-

taining continuous connectivity between nodes is a challenge. The ability to exploit nodes that move around as potential "mules" to relay data "bundles" to specific gateways (similar in spirit to delay tolerant networks [7]) is useful in such scenarios. Communication criteria may involve reliability (aim to deliver as many bundles as possible to their destinations), storage efficiency (reduced storage consumption on mobile nodes), transmission efficiency (fewer number of transmissions), and timeliness (reduced latency incurred before bundles reach their destinations). In a CPS environment (e.g., fire situational awareness), mobile sensing may be event-driven; where the trajectory of the mobile node is not fixed, but dictated by the evolution of events in the space. Often, higher resolution data is required from the event region and unequal sensing needs in the space (due to the event) may cause buffer overflow at the sensor. The challenge then is to design mobile capture techniques that sense as frequently as needed (via quality-aware sensing); upload data as quickly as possible (time-efficient); ensure no buffer overflows; and provide this despite network disruptions.

4.2 Information resilience techniques

Information reliability in the CPS environment is a semantic concept—it refers to reliability of the observed information (as opposed to reliability of individual devices involved in capturing or communicating the information). Information obtained in an ICPS may be erroneous due to inherent imprecision of the sensing devices, dynamics of the event being captured and limitations of the underlying sensing and communication infrastructure. Approaches need to be designed to support robustness to changes in sensing needs at the semantic level in order to enhance confidence in the sensing outcome under dynamic changes. We describe below two potential approaches to improve dependability of information from sensors.

Sensor fusion to realize dependability requirements: The ability to observe and extract information using sensors may vary across the physical space of the CPS system; exploiting this knowledge to fuse information from multiple sensors to provide an aggregate estimate of the sensed values can result in increased confidence in the result, i.e., improved information reliability. For example, consider an extensible localization framework that enables seamless fusion of multiple localization technologies (e.g., GPS, GSM, Wi-Fi, ultrasound, ultra-wideband (UWB), inertial sensors, and IR) that differ in availability, operational costs, infrastructure requirements, levels of accuracy and efforts needed to calibrate, and use the technology [10, 16, 18, 35]. What is required is a generic approach whereby diverse sensing technologies can be fused together to meet the diverse needs of the ICPS applications in a cost-effective manner. How exactly to design and deploy fusion pipelines to meet information accuracy needs remains a challenge.

Cooperative sensor actuation and event disambiguation: The CPS event processing engine is required to react to events quickly, e.g., notification about an unauthorized individual's entry in a surveillance scenario is much more valuable seconds after entry as opposed to minutes after he has already left the premises. This requires applying complex processing operators on high volume data; information extraction tasks such as person identification from multimedia surveillance data is difficult in resource-constrained environments where I/O storage limitations, transmission delay, bandwidth restrictions, and packet losses may prevent the capture of high quality data. The ability to exploit semantics (of content, deployment, application, users) can help in enhancing information quality in the presence of such resource limitations. Recent work on camera networks suggests that a probabilistic model based on extracted semantics can predict where events of interest will occur and dedicate scarce resources accordingly [38]; this will help meet compute limitations without sacrificing event detection accuracy. However, the ability to increase dependability of one event may come at the cost of increased uncertainty about other activities that the sensor could have captured. For example, activating zoom capabilities to collect high-resolution facial images will imply temporary loss of "pan" capability which can capture potential events (albeit at lower resolutions) elsewhere in the coverage area of the camera sensor. While custom techniques can be designed, addressing information uncertainty with large numbers of devices is challenging.

5 Concluding remarks

In this paper, we presented the need for dependability in the future generation of societal scale cyber-physical systems. We argued for adaptability as a key enabler in building dependable CPS systems and illustrated how a reflective "observe-analyze-adapt" methodology can provide a basis for structured adaptation. The approach described in this paper represents a paradigm shift in the area of monitoring, orchestration, and control of real-world dynamic cyber-physical systems using an information-centric approach (instead of a device-centric approach). Formal methods based specification and reasoning can provide a platform to perform what-if analysis and support consistent integration of the components into a larger framework.

Deploying Human-Oriented CPS raises additional issues of sustainability and security; these are particularly interesting since they can at times conflict with dependability needs. Today, sustainable infrastructures are self-managing; green; and energy-aware through the use of various energy-harvesting technologies that leverage renewable sources of natural and artificial energy (solar, wind, geothermal, kinetic). While the use of these novel approaches

enables sustainability, they bring with them new levels of (un)predictability—the dependable operation of a smart building is now connected to the availability of solar and wind power for instance. Societal scale CPSs also require the involvement of humans both as information providers (humans-as-sensors) and consumers (humans-as-decision-makers). This raises questions of trust in the service provider who maintains and analyzes the data and privacy of individuals who are embedded in the instrumented space. The question of what exactly "privacy" means in these settings and how to express it merits further exploration. Whether the required privacy needs (once specified) can be enforced is debatable—especially in the presence of external inference channels (public and background knowledge). While privacy techniques aim to hide information and disclose as little as possible—resilience techniques attempt to do the opposite, gather rich information for increased confidence in the event. The next generation of societal scale cyber-physical systems requires designing a system-of-systems approach where societal entities, cyber entities, and physical devices cooperate toward a set of common goals will eventually lead to the blurring of distinctions between the "cyberphysical" and "sociotechnical" worlds.

Acknowledgements This material is based upon work supported by the National Science Foundation under Award Numbers 1063596, 1059436.

References

1. Azimi SR, Bhatia G, Rajkumar R et al (2011) Vehicular networks for collision avoidance at intersections. In: SAE 2011 world congress and exhibition
2. Ananthanarayanan G, Stoica I (2009) Blue-Fi: enhancing Wi-Fi performance using bluetooth signals. In: Proceeding of MobiSys
3. Bak S, Manamcheri K, Mitra S, Caccamo M (2011) Sandboxing controllers for cyber-physical systems. In: 2nd ACM/IEEE ICCPS
4. Bailey MD (2006) A scalable hybrid network monitoring architecture for measuring, characterizing, and tracking Internet threat dynamics. PhD thesis, University of Michigan
5. Bellavista P, Corradi A, Giannelli C (2011) A unifying perspective on context-aware evaluation and management of heterogeneous wireless connectivity. IEEE Commun Surv Tutor 13(3):337–357
6. Bonnin JM, Lassoued I, Hamouda ZB (2009) Automatic multi-interface management through profile handling. Mob Netw Appl 14
7. Camp T, Boleng J, Davies V (2002) A survey of mobility models for ad hoc network research. Wirel Commun Mob Comput 2(5)
8. Chandra R, Bahl P (2004) MultiNet: connecting to multiple IEEE 802.11 networks using a single wireless card. In: Proceeding of INFOCOM
9. Chebrolu K, Rao R (2006) Bandwidth aggregation for real-time applications in heterogeneous wireless networks. IEEE Trans Mob Comput 5(4)
10. Chen B, Tong L, Varshney P (2006) Channel aware distributed detection in wireless sensor networks. IEEE Signal Process Mag 23(4):16–25
11. Clavel M, Duran F, Eker S, Lincoln P, Oliet NM, Meseguer J, Talcott C (2007) All about Maude: a high-performance logical framework. LNCS, vol 4350
12. Cook DJ, Das SK (2007) How smart are our environments? An updated look at the state of the art source. In: Proceeding of pervasive and mobile computing
13. CYPRESS project: http://www.ics.uci.edu/~dsm/cypress/index.html
14. Davison C, Massaguer D et al (2010) Practical experiences in enabling and ensuring quality sensing in emergency response applications. In: IEEE PerNEM
15. Erramilli V, Crovella M, Chaintreau A, Diot C (2008) Delegation forwarding. In: MobiHoc
16. Gastpar M, Vetterli M, Dragotti PL (2006) Sensing reality and communicating bits: a dangerous liaison. IEEE Signal Process Mag 23(4):70–83
17. Ho T, Lun DS (2008) Network coding: an introduction. Cambridge University Press, Cambridge
18. Ihler AT, Fisher JW III, Moses RL, Willsky AS (2005) Nonparametric belief propagation for self-localization of sensor networks. IEEE J Sel Areas Commun 23(4)
19. Jones CE, Sivalingam KM, Agrawal P, Chen JC (2001) A survey of energy efficient network protocols for wireless networks. Wirel Netw 7
20. Kim M, Stehr M, Talcott C, Dutt N, Venkatasubramanian N (2007) A probabilistic formal analysis approach to cross layer optimization in distributed embedded systems. In: 9th IFIP FMOODS'07
21. Koundourakis G, Axiotis DI, Argyropoulos M, Theologou M (2008) A network-centric approach for access and interface selection in heterogeneous wireless environments. Int J Commun Syst 21(5)
22. Laprie J-C (2008) From dependability to resilience. DSN'08 Fast Abstracts
23. LaViers A, Egerstedt M, Chen Y, Belta C (2011) Automatic generation of balletic motions. In: IEEE/ACM ICCPS
24. Lee I, Pappa GJ et al (2006) High-confidence medical device software and systems. IEEE Comput 39(4)
25. Luo H, Ramjee R, Sinha P, Li L, Lu S (2003) UCAN: a unified cellular and ad-hoc network architecture. In: MobiCOM
26. Meseguer J (1992) Conditional rewriting logic as a unified model of concurrency. Theor Comput Sci 96(1):73–155
27. Mohanty S, Akyildiz IF (2007) Performance analysis of handoff techniques based on mobile IP, TCP-migrate, and SIP. IEEE Trans Mob Comput 6(7)
28. Ölveczky PC, Meseguer J (2007) Semantics and pragmatics of real-time Maude. In: Higher-order and symbolic computation, vol 20
29. Pang J, Greenstein B, Kaminsky M, McCoy D, Seshan S (2009) Wifi-reports: improving wireless network selection with collaboration. In: MobySis2009
30. Pras A, Meent R, Mandjes M (2005) QoS in hybrid networks. In: Lecture notes in computer science
31. Ramdhany R, Grace P, Coulson G et al (2009) MANETKit: supporting the dynamic deployment and reconfiguration of ad-hoc routing protocols. In: ACM middleware
32. Rappaport S (1991) The multiple-call hand-off problem in high-capacity cellular communications systems. IEEE Trans Veh Technol
33. Rowe A, Berges M, Rajkumar R (2010) Contactless sensing of appliance state transitions. In: ACM BuildSys
34. SAFIRE project. http://www.ics.uci.edu/~projects/cert/safire.html
35. Sczyslo S, Schroeder J, Galler S, Kaiser T (2008) Hybrid localization using UWB and inertial sensors. In: IEEE international conference on ultra-wideband
36. Stehr M, Talcott C (2008) Planning and learning algorithms for routing in disruption-tolerant networks. In: MILCOM

37. Thiagarajan A, Ravindranath L et al (2009) VTrack: accurate, energy-aware road traffic delay estimation using mobile phones. In: ACM SenSys
38. Vaisenberg R, Mehrotra S et al (2009) Exploiting semantics for scheduling data collection from sensors on real-time to maximize event detection. In: MMCN
39. Xing B, Deshpande M et al (2010) Gateway designation for timely communications in instant mesh networks. In: IEEE pervasive wireless networks