Machine-to-Machine Communications With In-Network Data Aggregation, Processing, and Actuation for Large-Scale Cyber-Physical Systems

Ivan Stojmenovic, *Fellow*, *IEEE*

***Abstract*—Machine-to-Machine (M2M) paradigm enables machines (sensors, actuators, robots, and smart meter readers) to communicate with each other with little or no human intervention. M2M is a key enabling technology for the cyber-physical systems (CPSs). This paper explores CPS beyond M2M concept and looks at futuristic applications. Our vision is CPS with distributed actuation and in-network processing. We describe few particular use cases that motivate the development of the M2M communication primitives tailored to large-scale CPS. M2M communications in literature were considered in limited extent so far. The existing work is based on small-scale M2M models and centralized solutions. Different sources discuss different primitives. Few existing decentralized solutions do not scale well. There is a need to design M2M communication primitives that will scale to thousands and trillions of M2M devices, without sacrificing solution quality. The main paradigm shift is to design localized algorithms, where CPS nodes make decisions based on local knowledge. Localized coordination and communication in networked robotics, for matching events and robots, were studied to illustrate new directions.**

***Index Terms*—Cyber-physical systems (CPSs), machine-to-machine (M2M) communications.**

I. Introduction

CYBER-PHYSICAL SYSTEMS (CPSs) feature a tight combination of, and coordination between, the system's computational and physical elements and integration of computer- and information-centric physical and engineered systems. An important class of CPS is called *Internet of Things (IoT)*, which is a network that can *interconnect* ordinary physical objects with identified *addresses*, based on the traditional information carriers *including* internet and telecommunication network. Therefore, internet is not mandatory in IoT. Further, interconnection and addresses are not required in CPS. From the definition, one could mathematically conclude that IoT is a subset of CPS. Arguably, control technologies in non-networked embedded systems applications are examples of CPSs that arenot IoTs.

Recently, the Sensor Web concept came into foreground, aiming at combining distributed sensing with the ubiquitous connectivity and accessibility of the web, therefore, facilitating the close interaction of digital world with physical world. Toward merging the information-centric character and node-centric physical world connectivity, well-defined analytical models, methodologies, and experimental validations are required on how to build such systems capable of coping with the entire chain of operations and orchestrating the various parts together in a flexible, efficient, and economic way.

Another definition views CPSs as integrations of computation, communication, and control processes. Wireless sensor networks are traditionally used only for monitoring the environment. Actors (or actuators) are elements that can act on themselves, sensors, or the environment, and could be static (e.g., water sprinkler) or mobile (robots). Control processes aim at the performance of actors. CPSs are related to the embedded systems and control theory. Single robot, space shuttle, etc., are CPSs and may be handled by control theory approaches (e.g., equation solvers).

CPS and IoT concepts recently established themselves as one of the hottest research areas worldwide. Although their names appear new, the concepts were envisioned in 1926 by Nikola Tesla (the father of wireless communication, demonstrated radio remote-controlled submarine in 1898), who envisioned "tele-automation" research. "When wireless is perfectly applied, the whole earth will be converted into a huge *brain*, which in fact it is . . . and the instruments through which we shall be able to do this will be amazingly *simple* compared with our present telephone. A men will be able to carry one in his vest pocket."

Research advances in CPS promise to transform our world with new relationships between computer-based control and communication systems, engineered systems, and physical reality. Building on the concepts of embedded systems in which software programs and computers are embedded in devices for reasons other than computation alone (toys, cars, medical devices, scientific instruments, and machinery), the goal of researchers in CPS is to integrate the abstractions and precision of software and networking with the dynamics, uncertainty, and noise in the physical environment. Using the emerging knowledge, principles, and methods of CPS, we will be able to develop new generations of intelligent medical devices and systems, "smart" highways, buildings, factories, and agricultural systems, as well as defence and robotic systems.

Machine-to-Machine (M2M) communications well describe most existing CPSs. M2M uses a *device* (such as a sensor or meter) to capture an *event* (such as temperature, inventory level, etc.), which is relayed through a *network* (wireless, wired or

Manuscript received November 04, 2013; revised February 18, 2014; accepted March 10, 2014. Date of publication March 13, 2014; date of current version May 09, 2014. This work was supported by NSERC Discovery Grant and NSERC Collaborative Research Development *Robot-assisted deployment and maintenance of wireless sensor networks for area and event monitoring* (CRDPJ445199-12; 2013–2015).

The author is with the SEECS, University of Ottawa, Ottawa, ON K1N 6N5, Canada. He is also with King Abdulaziz University, Jeddah 22254, Saudi Arabia and also with Deakin University, Melbourne VIC 3125, Australia (e-mail: Stojmenovic@gmail.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JIOT.2014.2311693

Fig. 1. Networked control systems.

hybrid) to an *application* (software program) that translates the captured event into meaningful information, which can trigger an *actuation*.

Actor (or actuator) can act on the environment, itself (e.g., controlled movement, turn, video recording), and networks' elements, e.g., sensors. They can be static (e.g., traffic lights) or mobile (e.g., robots). They can be considered as the combined cyber-physical elements. Future CPSs might feature large number of actors that seamlessly integrate cyber and physical components.

M2M examples include telemetry, industrial, automation, and supervisory control and data acquisition (SCADA) (in power grids) applications. Modern M2M communications expanded beyond one-to-one connection into a system of networks that transmits to personal devices. This is facilitated by the expansion of IP networks across the world which has lessened the amount of power and time necessary for communication. New connections between consumers and producers are supported by this M2M concept of CPS. Existing M2M concepts incorporate a *central point* for gathering information, making decision, and acting. The information may be gathered via, e.g., wireless sensor network by single-hop or multi-hop communication, to a base station (BS). M2Ms are finding increased application in diverse areas such as environmental, health care, automotive, military, business, and logistics, and they are the key component of various embedded systems. Imagine, e.g., structures, from buildings to bridges, that can recognize the need and call for their own site-specific maintenance, or self-help systems that can assist and protect the elderly, infirm, or disabled, automatically switching OFF hotplates, reporting accidents, ensuring food is fresh and the pantry restocked, and maintaining medication schedules; cots that monitor sleeping babies; highways that manage traffic flow; forests that alert rangers to fires and "report" on the well-being of their inhabitants. Outcomes of this sort are only some of the potential results of developments in the CPS discipline with assisted M2M communications.

Networked control systems have a controller connected to a physical system (e.g., plant) via a network [12] (see Fig. 1). One of the fundamental characteristics of today's CPSs is that the network is only a mediator between computing and physical entities. We are interested in new challenges and new methods in conjunction to control theory. Although control theory handles actions of a single actuator, the coordination and wireless communication among increasing number of cyber and/or physical elements requires a new layer and methods. In our vision, network elements are not merely communicators, but also potential decision makers and actuators.

Large-scale CPS (see Fig. 2 for an illustration of the core idea) has challenges in three directions that represent the top-level tasks for each application:

1) *interconnection* and *data exchange* among heterogeneous network elements, with global network convergence and local regional autonomy, and presence of weak-state interconnection, and weak ability nodes [e.g., sensors, radio frequency identification (RFID)];
2) intensive *information processing*, using uncertain sensory data, multi source and type data fusion, authorization and privacy protection, interaction and adaptation;
3) comprehensive intelligent *service*, including delivery, adapting software design, service adaptation, and modeling.

Networked computing at multiple scales plays a crucial rule in CPSs as such systems use computation and communication deeply embedded in and interacting with physical processes to drive the cyber-physical coupling. CPSs with networked computing are also termed *cyber-physical networking systems* (CPNSs). Research issues and challenges include finding innovative ideas and promising cutting-edge solutions (methodologies, techniques, and approaches) on diverse CPNS-related topics. The goal is to understand the broad, novel scope of CPNSs and grasp new thinking, challenges, and approaches underlying the issues, methodologies, modeling, theory, protocols, systems, architectures, implementations, and emerging CPNS technologies. Further issues in distributed and large-scale CPNSs include resource management, security, privacy, trust, scalability, and reliability issues, design, and cross-layer optimizations. Technologies and methodologies applied in CPS include ambient intelligence, context-awareness, data mining, embedded system and software, evolutionary computation, modeling environments and human behavior, social networks, big data, and ubiquitous computing.

Is there any existing large-scale CPS? Commercial applications tend to be based on simple scenarios. One such example is preventing bulls from fighting in a farm [27]. Bulls are nodes in network, carrying collars with sensing and actuation capabilities. Actuation are stimuli when two bulls come near each other.

CPSs find direct applicability in a wide range of areas and disciplines, including (but not limited to) the following.

1) *Smart Grid Technologies*: Aiming at facilitating intelligent monitoring and control of reliable, secure, and efficient delivery of electricity to consumers using digital communications.
2) *Wireless Sensing, Monitoring,and Networking*: To enable distributed monitoring systems of numerous smart sensors and actuators, mobile devices, RFIDs, (ground, aerial, and aquatic), robots, etc., which revolutionize a variety of application areas with unprecedented density, fidelity, and scalability of environment instrumentation.
3) *Vehicular Cyber-Physical and Intelligent Transportation Systems*: Integrating computing, communication, and storage capabilities with monitoring and control of vehicles to deal with the grand challenges of safe, green, and efficient transportation, e.g., distributed traffic control systems.
4) *Smart Living Technologies*: Smart city (e.g., increasing security, comfort and convenience, and green energy), intelligent park and space, healthcare systems, smart cameras, etc.

Preliminary conference version of this paper appeared in [23].

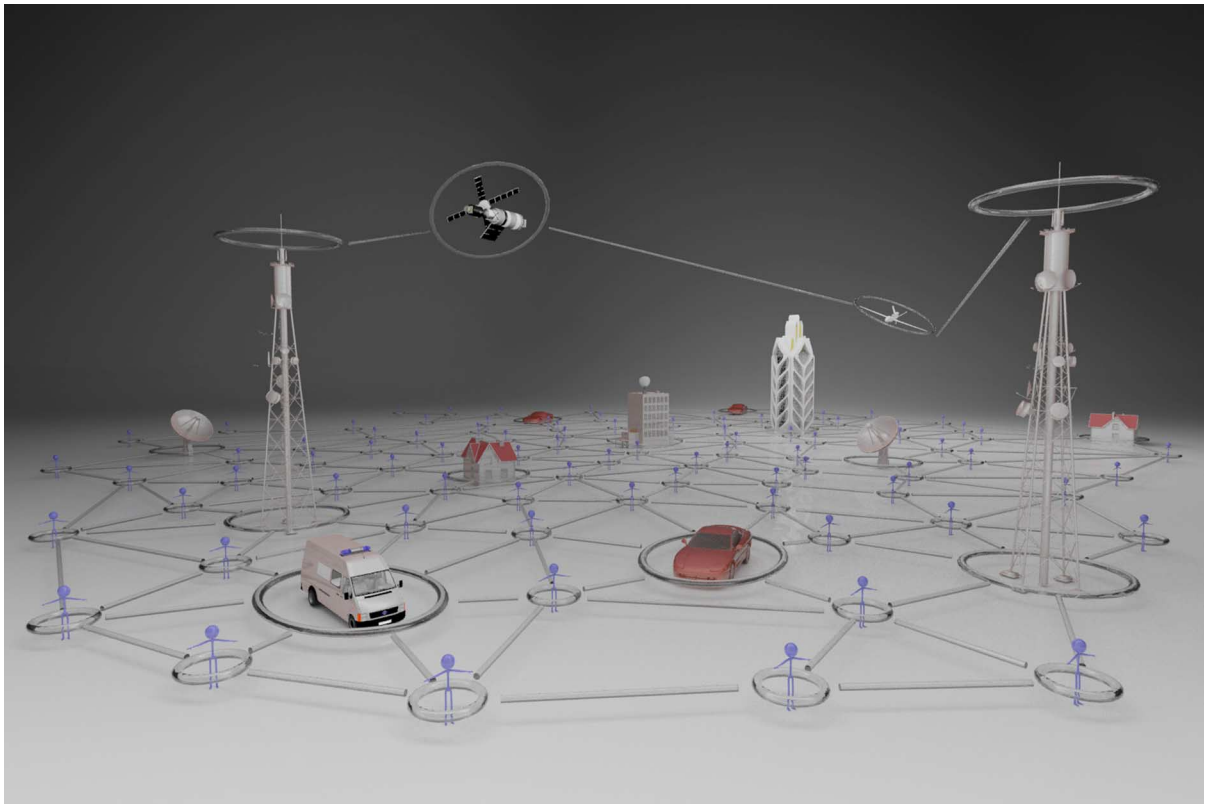

Fig. 2. Large scale CPS supported by M2M communications among participating interconnected 'things' (wearable devices on human, vehicles, buildings) equipped by sensors, RFID tags, processors and wireless antennas for communication assisted by base stations, satellites, cellular towers, airplanes etc.).

II. Literature Review

Several European Union projects attempt to define M2M and IoT. European Telecommunications Standards Institute (ETSI) M2M and IoT-A proposed several architectures and standards. BETaaS (www.betaas.eu) proposed to replace cloud as the resident for M2M applications by "local cloud" of gateways, the later being the devices that provide smart things with connectivity to the internet (e.g., smart phones, home routers, and road-side units). This enables applications that are limited in time and space, require simple and repetitive interactions, and respond in consistent manner.

It is important to envision certain CPS environments and derive our objectives as their fundamental enabling operations. For instance, one comprehensive vision of a high-level hierarchical CPS system architecture, when the number of devices explodes, is described in [29]. The service is provided by a server which could be assisted by a cloud. The top-level interface is provided by mobile operator. Some sensor devices can be directly connected to it. "Indirect" sensor devices are connected to gateways by a personal area network (Zigbee, WiFi, and Bluetooth), or are grouped around aggregation points connected to gateways by local area networks (WiFi or wired). Gateways are connected into peer-to-peer network. Key features for air interface optimization include mass device transmission (handling near simultaneous transmission attempts from an extremely large number of devices), high reliability in emergency situations, or scenarios where privacy is extremely important (e.g., healthcare and remote payment), enhanced access priority (to communicate "alarms" in a variety of use cases), extremely low-power consumption, small burst transmission, low-mobility support, unusual events (e.g., changed device location or damage), addressing, group control and addressing, periodic traffic, time-tolerant traffic, one-way data traffic, extremely low latency, and infrequent traffic.

Booysen *et al.* [2] elaborated on a generic large-scale M2M communications architecture for vehicular networks as CPS. M2M communication consists of multiple interconnected gateways. Data collectors (e.g., temperature sensors, location sensors, or heart rate monitors) collect information from multiple sensing locations and report to one of the gateways. Data collectors of the same type are connected to small networks (e.g., body area networks, Zigbee, and Bluetooth) called subnets. In a fully distributed network, all nodes (e.g., various computers on a home Wi-Fi network) are connected as peers and share data. One of the nodes (e.g., a router's Wi-Fi module) acts as a super-peer that has the ability to connect through some gateway [e.g., a router's asymmetric digital subscriber line (ADSL) connection] to the internet. In a cooperative network, none of the nodes (e.g., body area sensors) communicate directly with each other, but rather via the gateway (e.g., a cellular phone). The collected data are then aggregated at possibly multiple layers of aggregation points. At each aggregation layer, the aggregation function can reduce the amount of data retransmitted. This can be achieved, e.g., through filtering data based on relevance or by extracting

higher-level information from aggregated data. Data aggregation is used to allow M2M devices to have low cost, consume little power, and have a limited operating area. This is required to enable a system of billions devices. Storage and postprocessing services and applications may be enabled by cloud computing paradigm.

Zhao *et al.* [31] proposed a system architecture for gathering sensory data from mobile vehicles and processing at the central server. A packet can either be delivered via multihop transmissions in the vehicular ad-hoc networks (VANET) or via 3G. Intermittent connectivity may cause delay in multihop vehicle-to-vehicle communication, which is otherwise preferred because there is budget constraint on the overall 3G traffic. This is an intrinsic tradeoff between delivery ratio and delivery delay when using the 3G. It is challenging to decide which set of packets should be selected for 3G transmissions and when to deliver them via 3G. Zhao *et al.* [31] described a centralized integer linear programming-based solution which does not scale for this potentially large-scale network with plethora of road side units and 3G access points.

One of modeling dimensions in CPSs is interdependency between cyber and physical systems. As a typical emerging application of CPS, smart power grid is composed of interdependent power grid and communication/control networks. The latter one contains relay nodes for communication and operation centers to control power grid. Failure in one network might cause cascading failures in the other. A k-to-n interdependence model for smart grid is studied in [9]. Each relay node and operation center is supported by only one power station, while each power station is monitored and controlled by k operation centers. Each operation center controls n power stations. The system controlling cost is proportional to k. Survival ratio (fraction of functioning parts) is calculated using percolation theory and generating functions. A threshold exists for the proportion of faulty nodes, beyond which the system collapses. Smart grid with higher controlling cost has a sharper transition, and thus is more robust.

Security and privacy in CPS was mostly studied in the context of smart grids (e.g., [11] and [13]) and M2M communications [17]. The main security issues are authentication at different levels of gateways as well as at the smart meters installed in the consumer's home. Each smart meter and smart appliance has an IP address. A malicious user can either tamper with its own smart meter, report false readings, or spoof IP addresses. Several public key infrastructure (PKI)-based solutions, including device attestation and certificate management, have been proposed in [20]. Some authentication techniques, using Diffie–Hellman key exchange, have been discussed in [5]. Smart meters encrypt the data and forward them to the aggregator node, e.g., a home-area network (HAN) gateway. HAN then decrypts the data, aggregates the results, and passes them forward. A homomorphic function takes as input the encrypted data from the smart meters and produces an encryption of the aggregated result [18]. The aggregator node cannot decrypt the readings from the smart meter and tamper with them. This ensures the privacy of the data collected by smart meters, but does not guarantee that the aggregator node transmits the correct report to the other gateways. Privacy issue deals with hiding details (e.g., what appliance was used at what time) while allowing correct summary information for accurate charging. In [4], a third party key escrow policy using several pseudonyms instead of unique identifier is proposed.

Cooperation and selfish behavior of CPS nodes was studied in [28], which describes a reputation-based credit incentive mechanism with reputation-formed payment risk. Combined with a forwarding cost model, neighboring and intermediate nodes achieve a Nash equilibrium in the noncooperation game, which economically provides a rational decision on the allocation of forwarding tasks for transmitters under an optimal reward.

Intrusion in smart grids can be detected using either a signature-based method in which the patterns of behavior are observed and checked against an already existing database of possible misbehaviors or using an anomaly-based method in which an observed behavior is compared with expected behavior to check if there is a deviation [1]. Berthier *et al.* [1] proposed intrusion detection to be carried out in different stages. At the appliance (sensor) level, the routing operations are verified and the packet payload is checked. At the home networks, the smart meters can check the readings with the meter logs and report if anomaly is detected. At the access points, the traffic load is checked and compared with the expected values.

Data aggregation in CPS was mostly studied in the context of smart grid. In [22], data aggregation for smart grid application is carried by concentrators that are located in neighborhood area networks. They serve as cluster-heads, and receive individual measurements from M2M devices (smart meters), sum them up, and transmit the sum to the BS, which aggregates all received data.

In [6], gateway collects sensed data from the monitoring area, which is divided into sensing regions. CPS node senses a subset of sensed data, and may transmit all of them in a single transmission. Gateway creates a transmission schedule for each CPS node, and the goal is to minimize the total number of transmission units assigned to them (during a cycle). For each type of data, at least one transmission unit should be received during the corresponding cycle. This integer linear programming (ILP) formulation is solved by a centralized algorithm. The algorithm does not minimize the activity times or maximize the lifetimes of CPS nodes, and does not consider possible message collisions.

CPS access stabilization was considered for CPS with cellular systems for enabling communications. 3GPP standard developed access class barring (ACB) for individual stabilization in each BS. The purpose of stabilization is to control expected number of simultaneous accesses to a common radio resource to be one. This is achieved by broadcasting the probability p for accessing channel by CPS devices associated with the BS. Lien *et al.* [16] consider supporting trillions of CPS devices and proposes global stabilization and access load sharing. Through the interface among BSs (such as the X2 interface in long-term evolution (LTE)-Advanced), direct communications and thus cooperation among BSs are available. They want to balance the number of associated CPS devices among them over iterations, starting from the initial attachment of each M2M to one of BSs. Taleb and Kunz [25] addressed issues relevant to

subscription, network congestion, and overload control, and suggested handling a bulk of similar signaling messages from M2M devices in a single shot. To minimize signal and latency, hybrid contention and schedule-based schemes are proposed in [8] and [14], incorporating the merits of low-complexity random access and high performance centralized access at higher loads.

A cloud-based architecture was proposed in [26]. A machine swarm of sensors is connected (wireless single hop or multihop) to data aggregators (some of them could be robots). Wireless infrastructure (e.g., 3GPP-type cellular systems or IEEE 802-type wide/local area networks) connects data aggregators to gateways, which in turn access cloud server that enables and maintains variety of services. Effective M2M communications would be the foundation of operation of wireless robotics to benefit human life. With cloud-based architecture, Tseng *et al.* [26] innovatively demonstrates in-network computation to significantly alleviate the requirement of communication bandwidth for multihop networking, to achieve spectrum-efficient M2M communications.

Vehicular social networking architecture is an opportunistic network consisting of vehicular ad hoc network, with many cars additionally equipped with mobile phones and other on board mobile devices. Interaction with other cars and service providers (e.g., cloud) via wireless links may provide new services in this potentially large-scale CPS.

III. Novel Concepts and Directions

Still in its infancy, CPS is emerging as the potential creator of a seamless interface for superior M2M communication, as well as communication between computer systems and the physical world. Our vision is CPS with *distributed actuation* and *in-network processing*. We describe few particular use cases that motivate the development of the M2M communication primitives tailored to the large-scale CPSs.

We may consider a generic sensor–actuator model, where sensors provide input, whereas certain input triggers certain action, controlled by a single sensor or a network of sensors. An example is decentralized smart building control with wireless sensors deployed to measure temperature, humidity, or levels of various gases in the building atmosphere. Furthermore, the sensors will be able to exchange information (e.g., all sensors in a floor) and *coordinate* to combine their readings and arrive at reliable measurements, and use distributed decision making and activation to react to data. The system components may then work together to lower the temperature, inject fresh air or open windows. Air conditioners can remove moisture from the air or increase the humidity. Sensors can also trace and react to movements (e.g., by turning light ON and OFF). BSs could be assigned at each floor and could collaborate on higher level of actuation. Combined with other technologies, networked buildings can maintain their fabric, external and internal environments, to conserve energy, water, and other resources.

Existing large-scale wireless ad hoc sensor network deployments lack actuation and coordination among sensors. For example, the largest deployment (to the best of our knowledge), GreeOrbs [15] has over 5000 sensors in Wuxi and Lin'an. The expansion toward smart city applications, including pollution control and forest fire monitoring, with in-network data collection and processing, is envisioned.

A border surveillance system may consist of large number of fixed sensor networks equipped with cameras that can rotate and serve as actuators. They can preprocess captured images, and coordinate data gathering and distributed processing. The information can be consolidated at unmanned ground or aerial vehicles which can act as mobile sensors and actuators, to handle intrusions.

In a campus environment, student and professors, equipped with mobile phones, can report automatically their location, unusual events (e.g., falling on ice) to several BSs. The gathered information can serve to monitor class attendance, heating and cooling decisions, distribute advertisements, guide students in evacuation scenarios, etc.

M2M communications were considered in limited extent so far. The existing work is based on small-scale M2M models and centralized solutions. Different sources discuss different primitives (normally only one primitive), and there is no coherent view on the list of basic communication modules. Few existing decentralized solutions do not scale well.

The most original concept and research direction argued here is to aim at scalable architectures, and *design M2M communication primitives that will scale* to thousands and trillions of M2M devices, without sacrificing solution quality. For small-scale networks, it should match the performance of existing centralized solutions, while providing seamless transition toward data communication primitives that will absorb various parameters through a simplified design. For instance, the movement speed as parameter would be avoided in favor of solution that will transition itself smoothly from static, to moderately mobile, to highly mobile scenarios, with different nodes having different mobility patterns [24].

M2M communication aspects include modeling, interdependency, topology control, dissemination, data aggregation, reporting mechanisms for monitoring, cooperative access, security, and privacy. M2M primitives should address mobility, intermittent connectivity, wireless channel collisions, QoS for different messages and levels of urgency, and event distance dependent requirements.

A unique *model* of a generic CPS appears to be infeasible due to specifics of actuation and physical world reaction. The challenge is to identify common ingredients and components of CPS present in variety of scenarios, model and investigate them, and combine and apply them to certain categories of CPS and corresponding concrete systems. One example is modeling the interconnection and inter-dependency between cyber and physical systems, or CPS network elements. The solutions to the other objectives are model dependent. We propose a component-wise approach, to design new model ingredients for various other CPS dimensions. Modeling dimensions could include participating networks, gateways, communication channels, mobility, and cyber-physical dependencies.

For instance, the network of participating cyber nodes could be flat (e.g., wireless sensor networks), or a two-tier architecture of sensor nodes modeled as the unit disk graph, and data aggregators [7] modeled as the small world graph. In [26], data aggregators are connected to a cloud as the third layer. The cloud layer

might be "networked." In the fog computing concept [3], users are served by computing nodes close to the network edge (e.g., road side units in vehicular networks) to reduce latency and communication overhead, with periodic updates from the remote cloud. There are other options for the participating networks component. Each of them could be considered along mobility dimension, with static or mobile sensors and data aggregators, possibly even cloud (e.g., police car with cloud services).

Our decentralized vision of CPS requires new modeling for system behavior, interconnection, and communication. These aspects, or dimensions, can define a taxonomy of models, in a component modeling approach, where certain options from each dimension are combined into a more specific class of CPSs.

As an example of novel solutions tailored to large-scale CPSs, we propose here *a localized cooperative access stabilization algorithm.* M2M devices will collaborate in addition to gateways, and both will limit their collaboration to local neighborhood. This approach will provide ultimate scalability of the solution. Access probabilities of each M2M node should be tuned according to its local environment, because different nodes may access different number of gateways, and gateways may be associated with different number of M2M nodes. Suppose that k nearby gateways estimate the number of their corresponding (overlapping) sensors as $n_1, n_2, \ldots, n_k$, respectively, and a particular sensor is able to communicate to all of them, and expected to compete with others for access in the same slot. This sensor will then transmit with probability $1/(n_1 + \cdots + n_k)$, to maximize the chance to have exactly one transmission in the slot.

Some CPS may feature human as physical systems. An example is online social network serving as a cloud, with mobile access from human, and human actions as result of interaction. Mobile social networks feature spontaneous (opportunistic) networks, or creating self-configurable mobile ad hoc social networks. Some CPSs have human in the loop. Human could be equipped with wireless body area sensor network, cameras, sensors, actuators (e.g., robot arms) in the environment, and embedded system for centralized or distributed inference engine for control and assistance (e.g., restoring fundamental autonomy).

IV. Networked Robotics

Traditional view of robot network in literature was restricted to centralized control from one of the robots or a central server and a team of up to five robots. Recently, a large-scale robot network was envisioned [21] along with novel approach to the communication and coordination among robots. Time and mobility constraints gear toward selecting robots in the vicinity of an event. Therefore, in a large-scale network, one can expect that robots physically close to an event should coordinate to decide about response. This hints toward the design of *localized* algorithms, where robot information and communication is restricted to its neighborhood; a network wide consultation may considerably delay response while not improving significantly on the service quality.

The novel communication and coordination paradigm can be illustrated on an example from [21] (see Fig. 3). For simplicity, assume that the distance to the event is the only criterion for

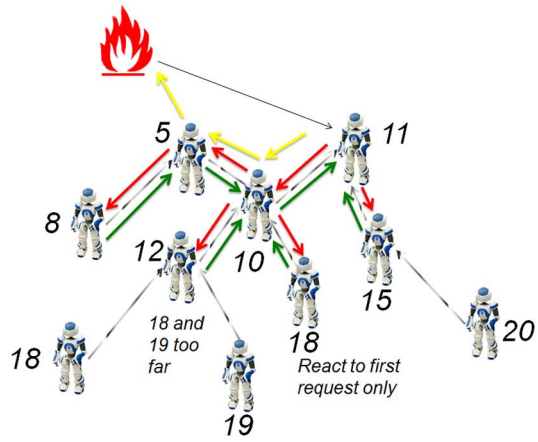

Fig. 3. Robot at distance 11 carries an auction (red arrows for contacting, green arrow for bids) to select the closest responder, the robot at distance 5 (yellow arrows).

selecting responding robot. A fire event has been reported to one of the robots (at distance 11). This robot starts an auction to detect the closest robot to the event, by consulting its neighbors at distances 15, 10, and 5 (red arrows). Robot at distance 15 estimates that its neighbor at distance 20, and all other robots potentially connected to it, would not be selected as best responders, and does not consult it. Instead, it responds back (green arrows) with itself as the best service provider. Robot at distance 10 consults its neighbors at distances 12 and 18. Neighbor at distance 12 finds its neighboring robots at distances 18 and 19 not competitive, and does not consult them. Instead, it offers itself back as best offer. Neighbor at distance 5 consults its neighbor at distance 8, and offers itself back to robot at distance 10, which in turn respond to auctioneer robot with best offer. Auctioneer robot then asks the "winner" at distance 5 (yellow arrows) to attend the event.

Given a set of events and a set of robots, the dispatch problem is to allocate one robot for each event to visit it. Each robot may be allowed to visit only one event (matching dispatch), or several events in a sequence (sequence dispatch). In a distributed setting, each event is discovered by a sensor and reported to a robot. Lukic and Stojmenovic [19] proposed pairwise distance-based matching algorithm to eliminate long edges by pairwise exchanges between matching pairs. The sequence dispatch algorithm iteratively finds the closest event-robot pair, includes the event in dispatch schedule of the selected robot and updates its position accordingly. When event-robot distances are multiplied by robot resistance (inverse of the remaining energy), the corresponding energy-balanced variants are obtained. Localized algorithms [19] are based on information mesh infrastructure, and local auctions within the robot network for obtaining the optimal dispatch schedule for each robot.

Robot movements are generally decided by virtual forces such as attraction toward an event, attracting or repelling from nearby robots or repelling from a boundary. The movement is in the direction of vector sum of all applied forces. The challenge is to decide the magnitude of these forces to achieve local responsiveness while converging toward desirable global behavior. Example applications include flying robocopter team for area mapping or sensor dropping (partially guided by already dropped sensors), collaborative diffusion profiling with aquatic sensing by a team of

robotic fishes [30], and robot deployment in disaster areas, areas with hard morphology and areas with moving hotspots, to enable other users on the ground with wireless connections.

References

[1] R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements, and architectural directions," in *Proc. 1st IEEE Int. Conf. IEEE Smart Grid Commun.,* 2010, pp. 350–355.

[2] M. J. Booysen, J. S. Gilmore, S. Zeadally, and G. J. van Rooyen, "Machine-to-Machine (M2M) communications in vehicular networks," *KSII Trans. Internet Inf. Syst.*, vol. 6, no. 2, pp. 529–546, 2012.

[3] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proc. ACM 1st Edition MCC Workshop Mobile Cloud Comput.,* Aug. 2012, pp. 13–16.

[4] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. IEEE Int. Conf. Smart Grid Commun.,* 2010, pp. 238–243.

[5] Z. M. Fadlullah, M. F. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward intelligent M2M communications in smart grid," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 60–65, Apr. 2011.

[6] H. L. Fu, H. C. Chen, P. Lin, and Y. Fang, "Energy-efficient reporting mechanisms for multi-type real-time monitoring in M2M communications networks," in *Proc. IEEE Conf. Comput. Commun.* (INFOCOM), 2012, pp. 136–144.

[7] L. Gu, S. C. Lin, and K. C. Chen, "Small-world networks empowered large machine-to-machine communications," in *IEEE Wireless Commun. Netw. Conf.* (WCNC), Apr. 2013, pp. 1558–1563.

[8] A. G. Gotsis, A. S. Lioumpas, and A. Alexiou, "M2M scheduling over LTE," *IEEE Veh. Technol. Mag.*, vol. 7, no. 3, pp. 34–39, Sep. 2012.

[9] Z. Huang, C. Wang, M. Stojmenovic, and A. Nayak, "Balancing system survivability and cost of smart grid via modeling cascading failures," *IEEE Trans. Emergent Topics Comput.*, vol. 1, no. 1, pp. 45–46, Jun. 2013.

[10] Y. Jan and L. Jóźwiak, "Scalable communication architectures for massively parallel hardware multi-processors," *J. Parallel Distrib. Comput.*, vol. 72, no. 11, pp. 1450–1463, 2012.

[11] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010.

[12] K. D. Kim and P. R. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, special centennial issue, pp. 1287–1308, May 2012.

[13] D. Li, Z. Aung, J. R. Williams, and A. Sanchez, "No peeking: privacy-preserving demand response system in smart grids," *Int. J. Parallel Emerg. Distrib. Syst.*, vol. 29, no. 3, pp. 290–315, 2014.

[14] S. Y. Lien, K. C. Chen, and Y. Lin, "Toward ubiquitous massive accesses in 3GPP machine-to-machine communications," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 66–74, Apr. 2011.

[15] Y. Liu, Y. He, M. Li, J. Wang, K. Liu, and X. Li, "Does wireless sensor network scale? A measurement study on GreenOrbs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 10, pp. 1983–1993, Oct. 2013.

[16] S. Y. Lien, T. H. Liau, C. Y. Kao, and K. C. Chen, "Cooperative access class barring for machine-to-machine communications," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 27–32, Jan. 2012.

[17] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 28–35, Apr. 2011.

[18] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proc. IEEE Smart Grid Commun.,* 2010, pp. 327–332.

[19] M. Lukic and I. Stojmenovic, "Energy-balanced matching and sequence dispatch of robots to events: Pairwise exchanges and sensor assisted robot coordination," in *Proc. IEEE Int. Conf. Mobile Ad-hoc Sens. Syst.* (MASS), Hangzhou, China, 2013, pp. 249–253.

[20] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grids*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[21] I. Mezei, V. Malbaša, and I. Stojmenovic, "Robot to robot: Communication aspects of coordination in robot wireless networks," *IEEE Robot. Autom. Mag.*, vol. 17, no. 4, pp. 63–69, Dec. 2010.

[22] D. Niyato, X. Lu, and W. Ping, "Machine-to-machine communications for home energy management system in smart grid," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 53–59, Apr. 2011.

[23] I. Stojmenovic, "Large scale cyber-physical systems: Distributed actuation, in-network processing and machine-to-machine communications," in *Proc. EUROMICRO/IEEE Workshop Embedded Cyber Phys. Syst.* (ECyPS'13); 2nd Mediterranean Conf. Embedded Comput. (MECO), Budva, Montenegro, Jun. 19, 2013, pp. 21–24.

[24] I. Stojmenovic, A. A. Khan, and N. Zaguia, "Broadcasting with seamless transition from static to highly mobile wireless ad hoc, sensor and vehicular networks," *Int. J. Parallel Emergent Distrib. Syst.*, vol. 27, no. 3, pp. 225–234, 2012.

[25] T. Taleb and A. Kunz, "Machine type communications in 3GPP networks," *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 178–184, Mar. 2012.

[26] F. M. Tseng, C. H. Lin, and K. C. Chen, "In-network computations of machine-to-machine communications for wireless robotics," *Wireless Pers. Commun.*, vol. 70, pp. 1097–1119, 2013.

[27] T. Wark, C. Crossman, W. Hu, Y. Guo, P. Valencia, P. Sikka, and A. Fisher, "The design and evaluation of a mobile sensor/actuator network for autonomous animal control," in *Proc. 6th ACM Int. Conf. Inf. Process. Sens. Netw.,* Apr. 2007, pp. 206–215.

[28] X. Wang, Y. Cai, and Z. Li, "A novel hybrid incentive mechanism for node cooperation in mobile cyber-physical systems," *Int. J. Parallel, Emerg. Distrib. Syst.*, vol. 29, no. 3, pp. 316–336, 2014.

[29] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson, "M2M: From mobile to embedded internet," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 36–43, Apr. 2011.

[30] Y. Wang, R. Tan, G. Xing, J. Wang, and X. Tan, "Accuracy-aware aquatic diffusion process profiling using robotic sensor networks," in *Proc. 11th ACM Int. Conf. Inf. Process. Sens. Netw.,* Apr. 2012, pp. 281–292.

[31] Q. Zhao, Y. Zhu, C. Chen, H. Zhu, and B. Li, "When 3G meets VANET: 3G-assisted data delivery in VANETs," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3575–3584, Oct. 2013.

Ivan Stojmenovic (A'98–M'04–M'05–F'08) received the Ph.D. degree in mathematics from the University of Zagreb, Zagreb, Croatia, in 1985.

He is a Full Professor with the University of Ottawa, Ontario, Canada. He held or holds regular and Visiting Positions in Saudi Arabia (Distinguished Adjunct Professor with the King Abdulaziz University, Jeddah), China (Tsinghua University, DUT, Beihang), Serbia, Japan, USA, Canada, France, Mexico, Spain, U.K. (as Chair in Applied Computing with the University of Birmingham), Hong Kong, Brazil, Taiwan, and Australia. He published over 300 different papers, and edited 7 books on wireless, ad hoc, sensor and actuator networks, and applied algorithms with Wiley. From 2010 to 2013, he was the Editor-in-Chief of IEEE Transactions on Parallel and Distributed Systems and is Founder and Editor-in-Chief of three journals. He is an Associate Editor-in-Chief of *Tsinghua Journal of Science and Technology*, steering committee member of IEEE Transactions on Emerging Topics in Computing, and editor of *IEEE Network*, IEEE Transactions on Cloud Computing, IEEE Transactions on Computers, ACM *Wireless Networks*, and some other journals. He is on Thomson Reuters list of Highly Cited Researchers (from 2013; <300 computer scientist), has h-index 60, top h-index in Canada for mathematics and statistics, and >15 000 citations.

Dr. Stojmenovic received five Best Paper Awards and the Fast Breaking Paper for October 2003, by *Thomson ISI ESI.* He received the Royal Society Research Merit Award, U.K., in 2006, and Humboldt Research Award, Germany, in 2012. He is a Tsinghua 1000 Plan Distinguished Professor in 2012–2015. He is a Fellow of the Canadian Academy of Engineering since 2012, and a Member of the Academia Europaea (The Academy of Europe) from 2012 (Section: Informatics). From 2010 to 2011, he was an IEEE CS Distinguished Visitor and received 2012 Distinguished Service award from *IEEE ComSoc Communications Software TC*. He received Excellence in Research Award of the University of Ottawa 2009. He chaired and/or organized >60 workshops and conferences, and served in >200 program committees. He was a Program Co-Chair at IEEE PIMRC 2008, IEEE AINA-07, and IEEE MASS-04&07, and founded several workshop series, and is/was Workshop Chair at IEEE ICDCS 2013, IEEE INFOCOM 2011, IEEE MASS-09, and ACM Mobihoc-07&08.