2016 IEEE First International Conference on Internet-of-Things Design and Implementation

A Layered Protocol Architecture for Scalable Innovation and Identification of Network Economic Synergies in the Internet of Things

Tilman Wolf
Department of Electrical and Computer Engineering
University of Massachusetts
Amherst, MA, USA
wolf@ecs.umass.edu

Anna Nagurney
Department of Operations and Information Management
University of Massachusetts
Amherst, MA, USA
nagurney@isenberg.umass.edu

***Abstract*—Many solutions to important societal problems relating to the environment, health care, transportation, etc. seek to utilize the promises of the Internet of Things (IoT), where sensing, computation, and actuation merge the physical world with the computational world. To date, many such solutions have focused on a single problem domain and require dedicated sensor and actuator infrastructure. This vertical integration makes the development of innovative, novel solutions costly and difficult to deploy. An architectural approach to addressing this challenge is to enable horizontal integration, where sensors and actuators from different applications can interconnect with any computational IoT application. In order to isolate complexities and to support heterogeneous systems and software, it is necessary to provide clear abstractions. We present such abstractions in the form of a layered protocol architecture that describes the necessary interfaces. Beyond technical challenges for horizontal integration, this paper also addresses network economic considerations since the various entities owning and operating sensors and actuators need suitable economic motivation to participate in such an approach. We believe that this work provides a conceptual foundation for future, scalable IoT solutions.**

***Keywords*-cyber-physical system, protocols, protocol stack, abstractions, incentives, economics**

I. Introduction

The Internet of Things (IoT) represent the technical foundation to solve some of the most important emerging societal and environmental problems. By combining sensing and response actions in the physical domain with processing and communication functionality in the computational domain, IoT systems can provide novel solutions in the areas of health care, transportation, energy, disaster response, manufacturing, defense, etc. It can be expected that IoT systems—more general, loosely-coupled, vastly more interconnected and richer variants of cyber-physical systems (CPS)—will become ubiquitously deployed in the coming decade as users demand more "smart" solutions in their environment.

One of the key challenges in IoT systems is the need for developing a common infrastructure on which innovative solutions (i.e., "applications") can be deployed. Current IoT/CPS architectures are dominated by vertically integrated "stovepipe" or "silo" designs where the three main functions, sensing, computation, and response, are customized for a single application domain. Developing custom IoT solutions for individual application scenarios is not a scalable and economically feasible approach to achieve large-scale deployment and use. Vertical integration also inhibits innovation since the realization of any new IoT application requires deployment of expensive infrastructure. A better approach is to seek horizontal integration in IoT systems such that sensing information can be shared across different application uses, multiple computational applications can coexist, and responses can be controlled by different entities.

While horizontal integration is beneficial, it requires careful design of suitable abstractions that enable interoperability across many domains. In this paper, we describe a layered protocols stack for the Internet of Things, which enables the efficient development of diverse applications on infrastructure that can be shared and reused. This architecture lays the foundations for a novel approach for large-scale deployment of innovative new solutions in IoT systems.

As we discuss in the context of our IoT stack, there are particular challenges around the question of how to accommodate different "contexts" in horizontal integration, i.e., how to accommodate interconnections between IoT components that make different assumptions in terms of security and privacy, economics, governance, etc. We introduce the idea of "exchanges" to bridge across such boundaries. Additionally, we present network economic models that show how horizontal integration can lead to synergies that provide incentives for entities to participate in IoT deployments.

The remainder of the paper is organized as follows. Section II introduces related work, and Section III discusses limitations of current approaches to realizing the Internet of Things. Our layered protocol architecture and its abstractions are presented in Section IV. We introduce the idea of IoT exchanges in Section V. Section VI discusses the economic issues that arise within IoT and how synergies can be exploited in horizontally integrated IoT architectures. Section VII discusses the potential impact of this architecture. Section VIII summarizes and concludes this paper.

978-1-4673-9948-7/16 $31.00 © 2016 IEEE
DOI 10.1109/IoTDI.2015.27

II. Related Work

Our aim for developing a layered protocol architecture is motivated by the vast success that the specification of a layered protocol architecture has seen in data communication networks. The TCP/IP protocol suite [1] in the context of the layered Open Systems Interconnection (OSI) protocol stack [2] has driven the large-scale deployment of the Internet and its ability to interconnect a large number of heterogeneous devices. A similar success of large-scale interconnectivity has been achieved in web services, where the World-Wide Web interconnected web content through a common Hypertext Transfer Protocol (HTTP) [3].

Architectures for the Internet of Things have been discussed in [4]–[6]. In [6], smart components are proposed to interact with each other and custom "workflows" are used as abstractions. Interaction types between components are considered in [5]. The importance of a cloud infrastructure to provide interconnectivity between components has been acknowledged in [4]. Neither work, however, provides a clear architectural structure, such as our proposed layered protocol stack, that can be applied to any type and scale of IoT system.

The World Wide Web Consortium (W3C) maintains a interest group on the Web of Things [7]. The stated goals of this interest group, "standardisation to enable open markets of applications and services based upon the Internet of Things (IoT) and the Web of data," align closely with our vision. The interest group has focused on standardization efforts (which our work can leverage) for specific areas, such as description of IoT components, interfaces, discovery and provisioning, and security, privacy, and resilience. Our work differs in that we aim to develop an encompassing architecture that provides a framework to think about these specific problems.

Cyber-physical systems have similar challenges as we describe in our work on IoT. Cyber-physical systems [8] present a number of interesting technical design challenges [9]–[12]. Numerous CPS solutions based on stovepipe architectures have been deployed. Example applications include energy [13], transportation [14], health care [15], and many more. However, CPS are often concerned with very tight real-time constraints (e.g., industrial automation, control in automobiles or aircraft). In such environments, horizontal integration may not be desirable due to performance constraints, lack of trust, etc. Thus, our work views the Internet of Things as a more general solution that encompasses traditional CPS in the lower layers, where real-time control is possible.

We may be able to leverage some results from the CPS domain for our work in IoT. The technical requirements for CPS have been discussed in [16]. Specialized CPS extensions to programming languages (e.g., [17]) and real-time operating systems (e.g., [18]) have been proposed. Security issues in cyber-physical systems have been explored in various contexts (e.g., control systems [19], [20]) and are an important aspect of any CPS. In the context of CPS architectures, composition in CPS has been discussed in related work (e.g., [21]).

Our own work has alluded to some of the ideas described in this paper with a stronger focus on developing economic incentives for horizontal integration [22]. The marketplace idea has been explored in the narrow context of networking [23]–[25]. This work has shown the importance of considering economic motivation of participating entities in order to drive innovation [23], [24], and thus we pursue a similar approach in this paper. Efficient searching in the large space of offerings in a marketplace has been described in [26]. Automated sensor verification in an environment of untrusted operators has been explored in [27].

The economic background for our work has been explored (cf. [28]) as network design under oligopolistic competition, in a supply chain context, which captures which facilities should be constructed and at which level the products should be produced, stored, and distributed to different demand markets. Also, potential synergies associated with horizontal integration of existing such networks have been quantified (see [29]). Earlier, [30] constructed a synergy measure to assess possible synergies associated with horizontal integration but using a system-optimization approach in which a single decision-maker, as in the case of a merger or acquisition, seeks to quantify the potential cost reductions due to such a potential integration. Of course, depending on the scenario, and this is one of the strengths of our framework, there may be a single decision-maker who wishes to minimize the total cost associated with a horizontal integration, while satisfying the demands for the information-based product at the various demand points. In addition, we can consider multicriteria decision-making, since distinct criteria may be relevant in different scenarios (see [31] for risk reduction synergy metrics and [32] for environmental and cost synergy metrics associated with horizontal network integration).

III. Limitations of Current IoT Architectures

Before presenting our proposed IoT stack in Section IV, we briefly review the operation of IoT systems and shortcomings of existing IoT architectures.

IoT systems perform three basic functions: (1) sensing characteristics of the physical world, (2) performing computation based on sensor input and other data sources, (3) generating response actions in the physical world through actuation. The basic principles of operation are illustrated in Figure 1.

Current IoT systems accomplish these three tasks by using custom solutions for sensing, computation, and actuation. This approach is typically pursued since the application domains of IoT systems vary considerably and custom solutions can be optimized for particular constraints (e.g.,

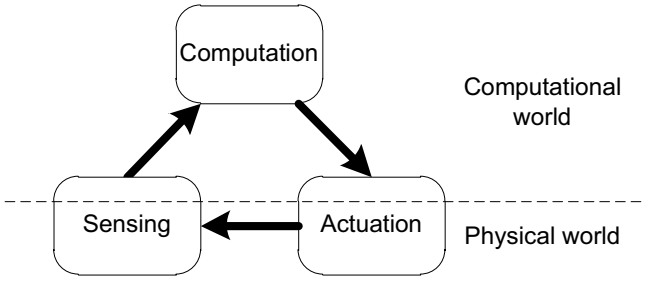


Figure 1. Principles of operation in IoT systems.

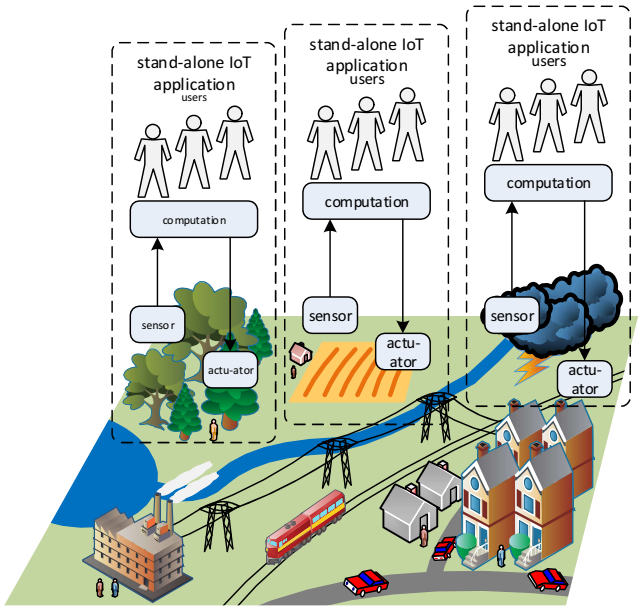
power and processing constraints, economic constraints, environmental constraints). As a result of customized IoT solutions, current IoT architectures are vertically integrated and operate independently of each other. This state-of-the-art is illustrated in Figure 2(a).

The main limitation of vertical integration in IoT is that new applications require a complete new top-to-bottom solution. For large-scale deployments, this approach is prohibitively expensive and thus limits overall system scalability. Specifically, we see the following shortcomings of current vertically integrated IoT:

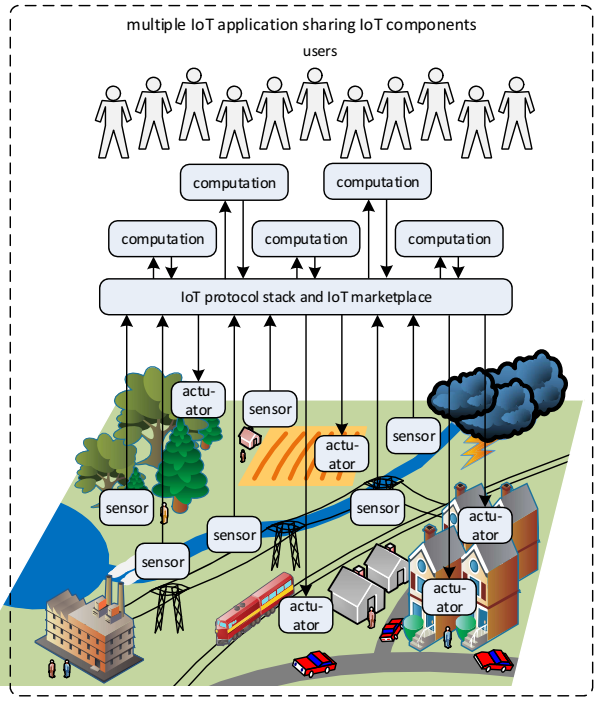
- Design complexity: Vertical integration requires that a system design considers all technical aspects from sensors to computation and actuators. While being able to design the entire system from scratch may reduce some complexities (e.g., no need for standardized interfaces), it still presents a major challenge when expertise is limited to only some of the system components.
- System cost: Deploying vertically integrated IoT applications is very costly since all sensors and actuators need to be installed in the physical world.
- Limited economy of scale: The system cost in vertically integrated IoT systems limits the deployment size and pervasiveness of an application. Infrastructure investments made by other IoT application deployments cannot be leveraged.
- Limited innovation: The cost and complexity of an IoT system inhibits innovation since new ideas and applications cannot easily be implemented.

The most critical shortcoming of vertical integration is that it limits innovation and ubiquitous deployments of IoT since individual application solutions require substantial investments in physical infrastructure. In the horizontally integrated approach that we present in Section IV, this obstacle is overcome by allowing different IoT application deployments to share access to existing IoT components.

Of course, owners of IoT resources (sensor data, computation, actuator access) need sufficient incentives to share. While the Internet has been successful in establishing a large-scale shared infrastructure without a clear underlying economic model, much of its resources (link bandwidth, computation time) are less tangible. In the IoT context, sensors and actuators have a clearly associated cost and assuming in-kind sharing is not likely to lead to a successful global IoT infrastructure. Therefore, we discuss the economic models underlying our proposed architecture in Section VI.



(a) Vertical integration of IoT architectures.



(b) Proposed horizontal integration of IoT architectures.

Figure 2. Comparison of IoT architectures.

IV. A Protocol Stack for Horizontal Integration in IoT Architecture

Our approach to horizontal integration in IoT is driven by the same ideas that made the Internet so successful: layering to hide complexity and well-defined interfaces to enable interoperability. The novel aspect of our work that focuses on IoT is that the scope of these abstractions not only encompass data communication, but also functionality on embedded devices (sensors and actuators) and computing infrastructure.

A. IoT Protocol Stack

Our foundation for a scalable, horizontally integrated Internet of Things lies in the design of an IoT stack that provides abstractions (1) to isolate complexities within each layer and (2) to enable instantiation of diverse IoT applications with diverse IoT components. The idea of abstractions and abstraction layers has been used successfully in many engineered IT systems, including networks and operating systems. The main challenge in IoT is that we need to develop an abstraction stack that ranges from small, simple sensor devices to large-scale control loops and optimization mechanisms.

Our proposed IoT stack is illustrated in Figure 3 and contains the seven layers that are described in the following (bottom-to-top).

1) Physical Layer: This layer represents the operation of sensors and actuators that interact with the physical world. This layer also encompasses the phenomena that occur in the physical world that cause feedback from actuators to sensors.

Upward data flow to device layer: raw sensor information; actuator status.

Downward data flow from device layer: raw actuator control; sensor configuration.

2) Device Layer: This layer translates the sensor and actuator interactions into common formats that can be exchanged via the interconnection layer. This layer also implements functions that enable efficient operation of IoT devices (e.g., sleeping to save battery).

Upward data flow to interconnection layer: sensor information in standard format.

Downward data flow from interconnection layer: actuator control in standard format.

3) Interconnection Layer: This layer provides communication and networking among IoT devices as well as the computational components of the IoT stack. This communication can be implemented on top of the global Internet or dedicated local or global networks.

Upward data flow to information stream layer: sensor information from one or more nodes in a sensor network.

Downward data flow from information stream layer: control instructions to one or more nodes in an actuator network.

4) Information Stream Layer: This layer implements the conversion of multiple data sources into a single, coherent stream of information. Format conversion, sensor data verification, extrapolation of missing data, etc. are implemented.

Upward data flow to control layer: aggregated information stream from sensors of IoT system.

Downward data flow from control layer: aggregated control decisions for actuators in IoT system.

5) Control Layer: This layer provides the functionality to implement different control mechanisms that tie together sensor inputs and actuator actions in an Internet of Things application.

Upward data flow to context layer: available control options to adapt IoT system behavior (e.g., "knobs" of IoT system).

Downward data flow from context layer: description of desired behavior of IoT system (e.g., "set point" of IoT system).

Note that there are additional control loops in other layers of the system. For example, the device layer may use a local control ("embedded control loop" in Figure 3) for an actuator using a local sensor (e.g., for positioning a steerable antenna) or the interconnection layer may use control loop to determine the rate of transmission between devices (e.g., flow control in TCP). However, some of these control loops, such as a networking control loop, are not specific to the IoT application domain and are not shown here.

6) Context Layer: This layer determines the goals and constraints of the IoT system. Example contexts are system optimization (e.g., maximizing performance), policy adherence (e.g., ensuring that privacy meet HIPAA policies), monetization (e.g., maximizing profits), etc. The implementation of the context layer may be local or remote (e.g., cloud data center that enables complex optimizations).

Upward data flow to user layer: available options for user input.

Downward data flow from user layer: user preferences.

7) User Layer:: This layer reflects interactions with a user (or user application). Interactions of this type include decisions that cannot be made by the IoT system automatically (e.g., objective of system operation (e.g., performance vs. efficiency), decisions relating to money, security, privacy, etc.), requests for user preferences, etc.

B. Example: Layering for Home Automation System

We envision that we can apply this layered architecture for Internet of Things to practically any use domain and application. To illustrate what such an IoT stack adaptation looks like for a specific environment consider the follow example of home automation:

- Physical Layer: Sensors that detect indoor and outdoor temperature, occupancy sensors, light switches, etc.; actuators to control heat, air conditioning, lights, shades, etc.

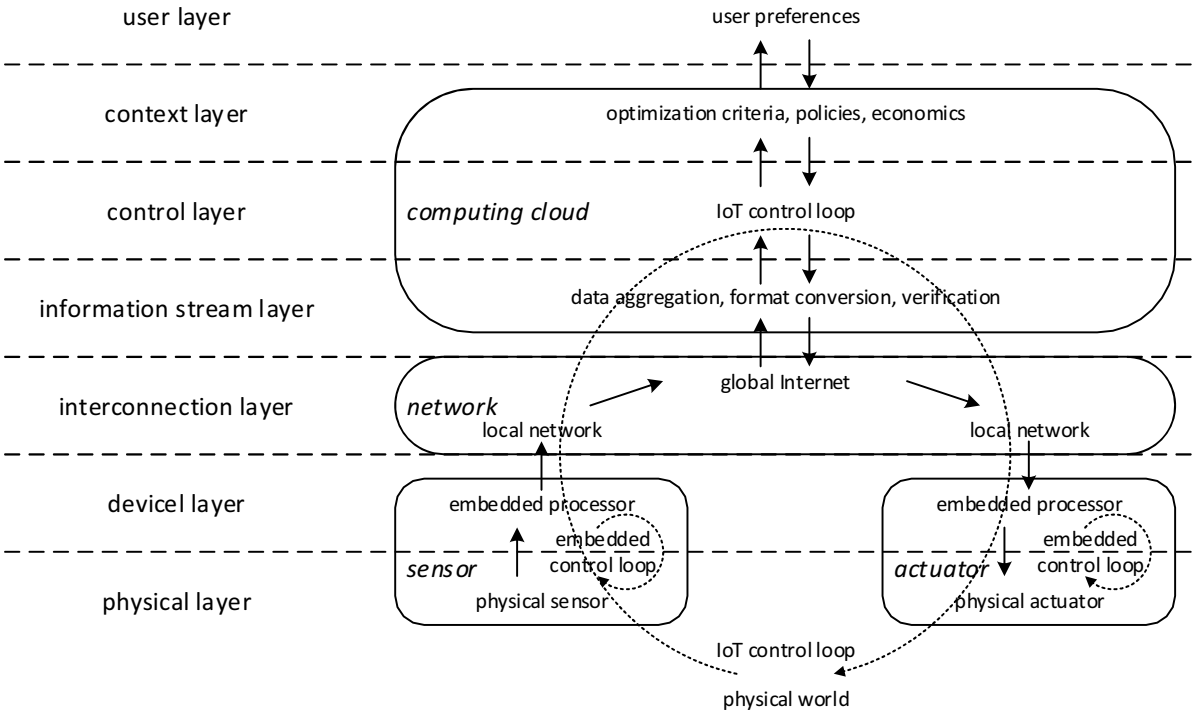


Figure 3. Proposed protocol stack for Internet of Things. Upward arrows indicate data flow, downward arrows indicate control flow, circles indicate control loops.

- Device Layer: Embedded systems that read sensor data and represent them in digital format and that drive analog inputs to actuators.
- Interconnection Layer: X10, ZigBee, UPB, or WiFi Network to exchange sensor data and actuator commands between devices.
- Information Stream Layer: A coherent stream of multiple (spatially and temporally diverse) sensor readings, such as temperature of one room over time, or control commands to one or more devices; additional information streams can include current price of electricity in a spot market, local weather forecasts, etc.
- Control Layer: A control mechanism to turn on air conditioner based on room temperature and spot price of electricity information streams given a target provided by the context layer.
- Context Layer: An optimization mechanism that minimizes energy consumption based on available information and control options. Long-term forecasts (e.g., based on weather forecasts, behavior patterns of user) are used to determine suitable control settings.
- User Layer: User input of acceptable tradeoffs between comfort (temperature range for rooms) and cost (willingness to spend money on running air conditioner).

Horizontal integration can then be achieved when components at different layers can be used by multiple IoT systems and applications. For example, an occupancy sensor may be also used by home security application, the temperature information stream may be used (after anonymization) to assess energy use in an area to enable forecasting and planning for utilities, a traffic management application may provide additional information streams or control settings based on user location and traffic predictions (e.g., later arrival to unoccupied home due to traffic), a healthcare application may override control settings based on medical policies (e.g., giving preference to healthier but possibly more expensive indoor temperatures), etc.

Using this structured IoT stack architecture, it is possible to interconnect the various IoT components to enable rapid development and deployment of novel applications that can address a wide range of applications across all domains of daily life, industry, and government.

C. Realization of Layered IoT Architecture

To realize the proposed architecture in practice a number of implementation issues need to be addressed.

1) Interfaces: Data does flow both upward and downward in this layered architecture. For example, sensor information flows in general upward, control commands flow downward. In each layer, information may be stored and/or processed to adapt it to the needs of the interface presented to the layer above or below.

The interfaces between layers provide the abstractions that can be used to access services in the layers below. For some

interfaces, well-established technologies can be used (e.g., sockets for interconnection layer [33]). For other layers, new interfaces need to be defined. Some work in the IoT community is pursuing this effort (e.g., W3C WoT working group [7]), albeit without an underlying, clearly defined, layered architecture. Similarly, abstractions for information streams have been explored in the context of web services and sensor networks [34].

2) Systems and Resource Management: Figure 3 shows the devices and systems that are involved in this layered IoT architecture. Sensors and actuators are embedded devices that implement the physical and device layer. The network that provides the interconnection layer can be a local network, a private network with regional or global reach, or the public Internet. The top four layers, information stream layer, control layer, context layer, and user layer, require substantial compute infrastructure and thus can be implemented in a private or public cloud. As data traverses the protocol stack upwards, real-time constraints decrease. Thus, remote, distributed, shared systems can be more easily used in higher layers.

One of the key characteristics of this architecture is that the IoT stack allows a *many-to-many relationship between all components* (as long as they adhere to layering). For example, an information stream can feed into multiple control components and a control component can send commands into multiple information streams. While information streams from sensors can typically be shared among many entities (assuming proper access control mechanisms if necessary), sharing actuators that operate in the physical world may be more difficult. For example, different control operations to a thermostat or a movable surveillance camera may make no sense. Thus, multiplexing control operations in the downward direction of the protocol stacks requires mechanisms to avoid conflicts and components needed to handle potentially conflicting commands.

V. Exchanges to Realize Contexts

The Internet of Things is characterized by large-scale diversity in terms of devices and application uses. This diversity results in significant challenges in two dimensions:

- How to interconnect components to enable correct operation at a technical level: The use of standardized interfaces can enable sensors, actuators, and computational resources to interconnect and use common protocols.
- How to interconnect components to enable correct operation in the context of intent, policies, economics, privacy, security, compliance, etc.: The ability to connect, communicate, and control at a technical level needs to be balanced with other criteria. We call these "contexts," where such criteria can be applied. For example, an economic context ensures that connections between components happen (only) when there is a suitable economic contract in place for access to these components (similar to contracts for services in a network [25]).

For interconnections that require adaptations in context, we propose the use of "exchanges."

A. IoT Exchanges

An exchange is a computational entity that can take in data and control information and adapt it to the context(s) that it provides. Figure 4 shows an example with a privacy exchange, which removes personal identifiable information from sensor streams and performs aggregation with other sensors, and a marketplace exchange, which ensures that economic interactions (e.g., payments) are conducted between data and control providers and users.

The figure shows three applications: A traffic management application reads GPS location information from users' cars, but the privacy exchange ensures that individual users cannot be identified. Similarly, the privacy exchange aggregates information from multiple temperature sensors to provide an input to a weather forecasting application, again protecting user's personal information. In the marketplace exchange, payments for sensor data or access to actuators are implemented. The power grid control application may pay a user money to allow control of an energy-consuming washing machine, where temporal load shifting can reduce peak demands on the grid infrastructure. The input to this power grid control could be the output from another application (i.e., weather forecasting), for which payments are exchanged.

As can be extrapolated from this example, many scenarios of interconnections via such exchanges are possible. The properties that are ensured by such exchanges can be vastly different, ranging from policy compliance in data (e.g., HIPAA) to verification of sensor data for validity (e.g., [27]). Since these exchange points can be reached from anywhere through a global network infrastructure (unlike network exchange points, which require physical proximity [35], [36]), any entity can utilize any exchange, and possibly use multiple at the same time.

B. Economic Exchange: IoT Marketplace

One example for a type of exchange for IoT is an "IoT marketplace." This marketplace provides the infrastructure necessary to advertise, search, and find IoT sensors, actuators, and computation. In addition, such a marketplace can also provide key features relating to trust, security, and economics.

The main goal of the IoT marketplace is to "connect" the right instances of IoT components. That is, we want to make sure that an application (i.e., computation component) has access to the necessary inputs (i.e., sensor data) and outputs (i.e., actuators in the physical world). The IoT marketplace provides the platform on which entities can offer and obtain such sensor information, computation services, and action responses. It is possible to integrate economic exchanges

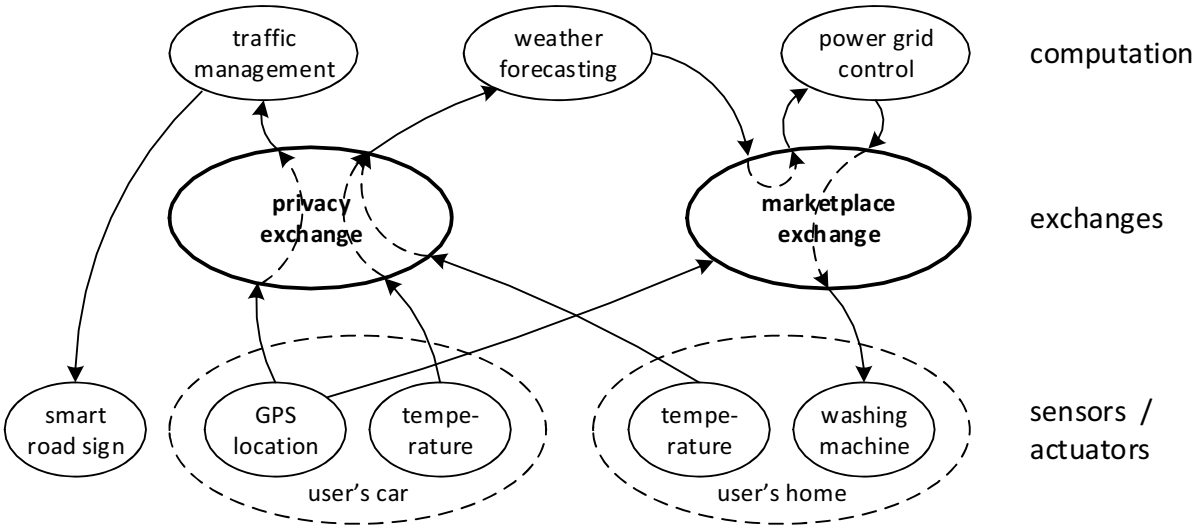


Figure 4. Exchange points can implement contexts for connections between entities.

into this framework, allowing operators of sensors, actuators, and computational solutions to charge money for using these components. By providing all entities with the power of choice (i.e., choice among different sensor inputs, choice among different computation solutions, choice among different action responses), competition is created and economic forces can drive selection and innovation as we discuss in the following section.

VI. Economic Interactions to Drive Innovation

In order to support a marketplace in the most transparent and effective manner, we propose a framework to identify network economic synergies associated with horizontal integration. We focus on cost minimization for societal benefit and value creation. We, subsequently, note that the framework may also be adapted to capture profit-maximizing behavior of different operators, as discussed in the context of the IoT marketplace. The network economic synergy perspective captures the types of connections that can be possible through horizontal links representing transactions and associated data transfer.

A. Network Economic Synergies

As discussed before, each application, prior to horizontal integration, would consist of sensing, computation, and actuation, which are economic activities, as depicted in Figure 5 in the case of two applications. In addition, there is data transfer from sensing to computation and from computation to actuation, an activity, which ends with the users. We assume that the costs associated with these economic activities are on the links and these depend on various factors, including the volume of data being transmitted.

We assume that, in vertically integrated applications, each economic network in Figure 5 is separately optimized so as to minimize the total (generalized) cost. The total cost associated with this solution is denoted by TC^0.

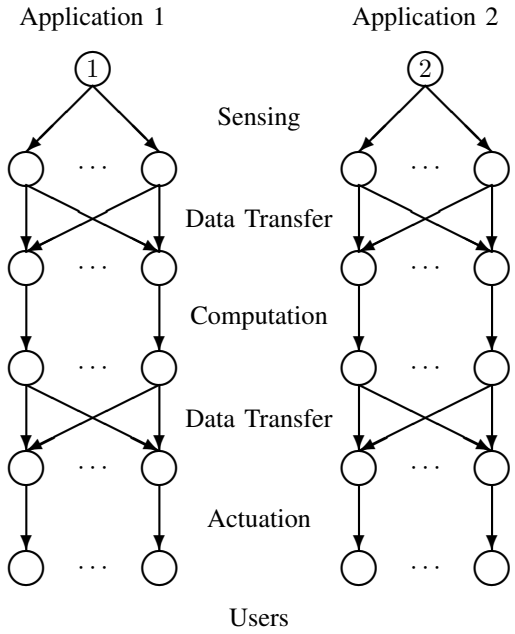


Figure 5. Case 0: Vertically Integrated Applications

We now consider partial horizontal integrations, as depicted in Figures 6 and 7, and then a complete horizontal integration, as depicted in Figure 8. Note that the horizontal integrations include an additional supernode 0 to reflect the integration with the links emanating to nodes 1 and 2 reflecting the cost of the integration at that level. In the economic network of Figure 6, the users can avail themselves of data obtained by the sensors in their original

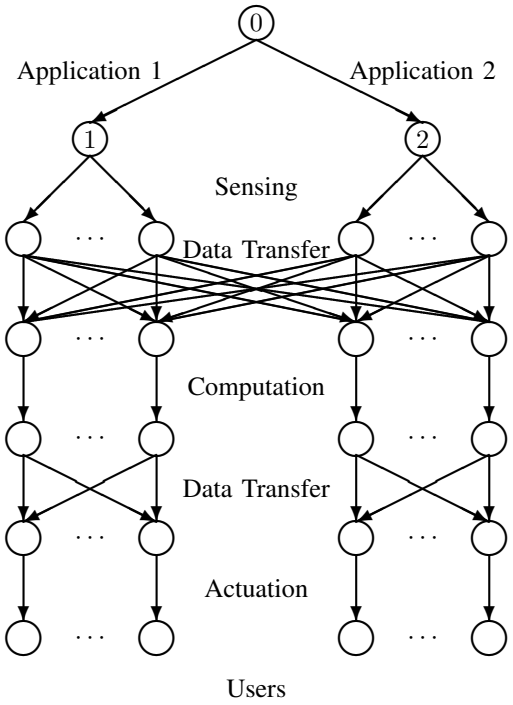


Figure 6. Case 1 Horizontal Integration: Sharing of Sensor Resources

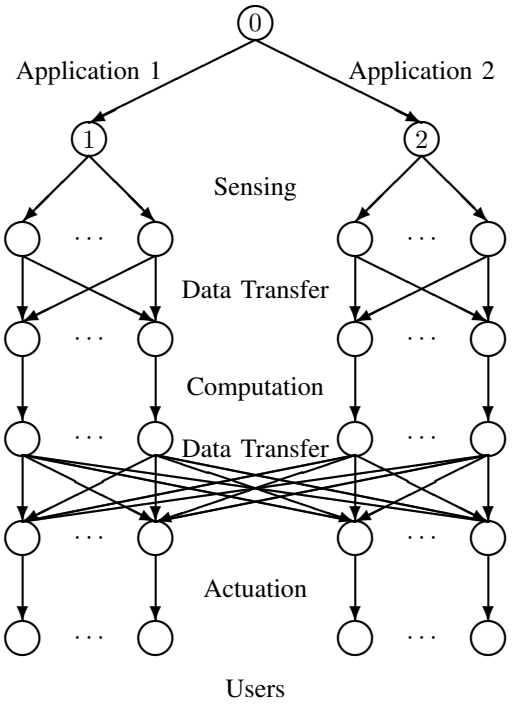


Figure 7. Case 2: Separate Sensing and Computation but Integration for Actuation

application as well as the other one. However, the computation activities still take place at their original, respective computational facilities. The new links associated with this horizontal integration have associated costs. The system-optimized solution in this integration corresponds to the total cost TC^1.

In the next horizontal integration figure, depicted in Figure 7, the sensing and computation are done using the original application resources but then transferred to the actuation activities to the users. The corresponding minimum total cost associated with such a horizontal integration is TC^2.

Finally, Figure 8 is the complete horizontal integration for the two applications, in which the users can benefit from data obtained by sensors in either or both application; the same for the computations. Here the minimum total cost is given by TC^3.

B. Synergy

We now provide a measure for quantifying the strategic advantage associated with the above cases of horizontal integration.

The measure that we utilize to capture the gains associated with a horizontal integration Case i; $i = 1, 2, 3$, corresponding to Figures 6, 7, and 8, respectively, is as follows:

$$\mathcal{S}^i = \left[\frac{TC^0 - TC^i}{TC^0}\right] \times 100\%, \qquad (1)$$

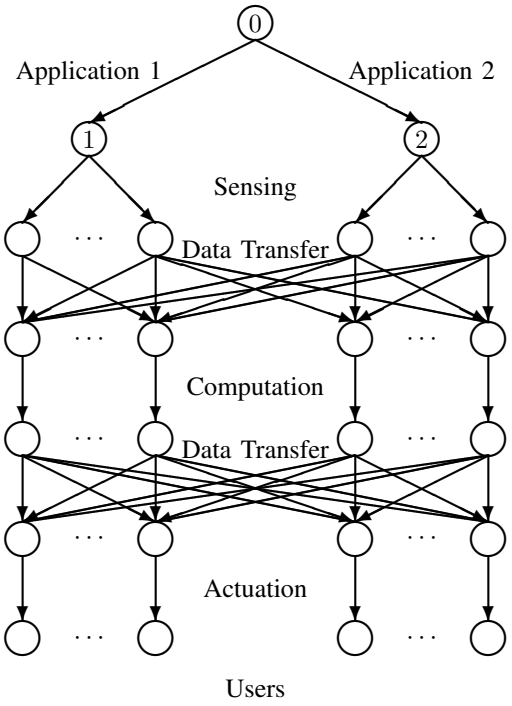


Figure 8. Case 3: Full Horizontal Integration

where recall that TC^i is the total cost associated with the value of the total cost objective function evaluated at the

optimal solution for Case i. Note that $\mathcal{S}^i$; $i = 1, 2, 3$ may also be interpreted as *synergy*.

We can expect, for example, positive synergies in Case 3, if the computations can be done more "cheaply" and reallocated accordingly by using one application's resources, assuming that there is sufficient capacity. Similarly, for the sensor activities, users may avail themselves of the sensors of the other application, after the reoptimization, if those are less costly.

C. Remark

In quantifying the synergy associated with horizontal integration above, we have assumed that system-optimization, in the form of total cost minimization with the desired criterion. This reflects, in a sense, centralized decision-making. We can, of course, also construct synergy measures associated with decentralized decision-making and profit maximization. For example, as discussed previously, sensors and computational resources may be owned by distinct decision-makers and each of these may wish to maximize profits. One could then construct measures associated with such decentralized decision-making behavior.

In addition, we emphasize that, since the costs correspond to generalized costs, this gives us the flexibility to include risk measures, emission measures (if there are environmental concerns), and other relevant criteria, and, with appropriate extensions, even time. Moreover, we emphasize that, in the vertically integrated networks depicted in Figure 6, there can be upper bounds associated with the links and these would remain in the horizontal integrations. This is highly reasonable since sensors, computational machines, etc., can have capacities in terms of processing and other capabilities. In addition, through the identification of the Lagrange multipliers, that is, the prices associated with the various link capacities, one can then determine the best payoffs in terms of where investments in enhanced capacities lie. Our synergy framework, hence, enables the quantification of the potential benefits of horizontal integration also in capacitated environments and identifies more "efficient" topologies in terms of reduced total cost.

Horizontal integration and associated synergies have also been investigated in the context of supply chain economic networks in the context of mergers and acquisitions, For example, [30] identified synergies associated with supply chain network economic activities of manufacturing and distribution to retailers, also under cost minimization. In supply chain network applications, thus far, the network topologies (cf. Figure 6) have been less expansive than in the IoT context revealed here. Moreover, the added links in the horizontal integration cases corresponded to transportation activities and not data transfer activities as in Figures 6, 7, and 8. [31] showed how risk reduction can be determined in mergers and acquisitions using a related approach to that detailed here but, again, in a supply chain network context. [37], on the other hand, presented synergy measures for environmental and cost concerns. [29] considered profit-maximizing firms involved in horizontal integration in the context of supply chains and mergers and acquisitions. Unlike our synergy framework for IoT and the papers above, the models therein handled elastic, price-dependent demands, rather than fixed demands. Horizontal integration associated with teaming in humanitarian operations is discussed in [37].

As we discuss in this paper, a marketplace can be envisioned in which users act as both consumers and producers. The topmost links in Figures 6, 7, and 8 incur costs, which can correspond to prices in the marketplace, and these can also reflect the level of trust associated with producers/consumers of the various applications. Hence, such costs/prices may change over time. In addition, the synergy framework can capture multiple applications, that is, more than two, if the need arises.

VII. Vision for IoT

The successful development of the theoretical foundations and practical implementation of the proposed IoT protocol stack, interfaces, exchange points, etc. can have impact on the way IoT systems are designed and implemented, on the scale and ubiquity of their deployment, and on the range of possible applications. Our long-term vision for the impact of our work includes the following:

- Scale and ubiquity of IoT: Separating the deployment of sensor from computational applications of IoT and from action responses – the principle of horizontal integration – is a critical enabler for large scale and ubiquitous IoT deployments, since sharable resources lower the bar of entry. For example, an individual can put a weather sensor in their backyard and sell the data it generates instead of having to deploy a complete IoT solution. Thus, everyone can participate in and benefit from IoT systems and the solutions they provide.
- Innovative new IoT applications: Ubiquitous deployment of IoT components can bring about many new applications that could not be realized with stovepipe architectures (either due to cost or due to complexity). Examples include advanced building automation, smart traffic management in cities, large-scale epidemics studies based on sensor information from individuals (e.g., related body-mass-index to geographic locations), financial decisions based on environmental conditions (e.g., decision to buy certain futures based on localized weather information), enhanced emergency preparedness and disaster recovery, etc. This type of enabling of innovation is analogous to how common data formats in the Internet enabled new applications through mash-ups, except that the IoT domain involves the real world and thus provides more practical and broader solutions.
- Participation of individuals in the "IoT economy:" IoT systems have the potential to revolutionize the

economic marketplace with existing boundaries between "buyers" and "sellers" being completely redrawn. For example, individuals and households may act not only as consumers of information derived from sensors but actually become producers and obtain economic/financial rewards. This shift can transform the current economic landscape and facilitate a new level of entrepreneurship.

Clearly, there are also limitations to our proposed approach: not all types of IoT application domains can or should be "open" (e.g., defense, some aspects of health care, some industrial control, etc.). Nevertheless, the vast majority of IoT applications can benefit from the technical contributions of the proposed IoT protocol stack and IoT marketplace. Individuals can benefit from the societal contributions of this work and by becoming active participants in the IoT economy.

VIII. Summary and Conclusion

In this paper, we presented an argument for why horizontal integration is essential for the Internet of Things in order to scale to global scale and to become a useful vehicle for solving many of today's problems that overlap the physical and the computational domain. We describe a layered architecture for IoT that ranges from the physical and device level all the way to users and applications. We describe how exchange points can be used to enable context that meet complex requirements, such as economic agreements between entities. We discussed how horizontal integration changes the underlying economic model and provide broader synergies than can be achieved in stovepipe architectures. We believe that this work provides a useful structure to guide the development of a scalable, globally interconnected Internet of Things that can provide innovative solutions to practical problems.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. 1551444.

References

[1] V. G. Cerf and R. E. Kahn, "A protocol for packet network intercommunication," *IEEE Transactions on Communications*, vol. COM-22, no. 5, pp. 637–648, May 1974.

[2] *International Standard ISO/IEC 7498-1 – Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*, 2nd ed., International Organization for Standardization / International Electrotechnical Commission, Geneve, Switzerland, Nov. 1994.

[3] T. Berners-Lee, "Hypertext markup language – 2.0," Network Working Group, RFC 1866, Nov. 1995.

[4] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[5] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things architecture, possible applications and key challenges," in *Proc. of the 10th International Conference on Frontiers of Information Technology (FIT)*, Islamabad, Pakistan, Dec. 2012, pp. 257–260.

[6] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the Internet of things," *IEEE Internet Computing*, vol. 14, no. 1, pp. 44–51, Jan. 2010.

[7] *Web of Things Interest Group*, World Wide Web Consortium, http://www.w3.org/WoT/IG/.

[8] E. A. Lee, "CPS foundations," in *Proc. of the 47th Design Automation Conference (DAC)*, Anaheim, California, Jun. 2010, pp. 737–742.

[9] ——, "Cyber physical systems: Design challenges," in *Proc. of IEEE International Symposium on Object-Oriented Real-Time Distributed Computing*, Orlando, FL, May 2008, pp. 363–369.

[10] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical systems: A new frontier," in *Machine Learning in Cyber Trust*, P. S. Yu and J. J. P. Tsai, Eds. Springer US, 2009, ch. 1, pp. 3–13.

[11] W. Wolf, "Cyber-physical systems," *Computer*, vol. 42, no. 3, pp. 88–89, Mar. 2009.

[12] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in *Proc. of the 47th Design Automation Conference (DAC)*, Anaheim, California, Jun. 2010, pp. 731–736.

[13] M. D. Ilic, L. Xie, U. A. Khan, and J. M. F. Moura, "Modeling future cyber-physical energy systems," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, Pittsburgh, PA, Jul. 2008, pp. 1–9.

[14] D. B. Work and A. M. Bayen, "Impacts of the mobile internet on transportation cyberphysical systems: Traffic monitoring using smartphones," in *Proc. of National Workshop for Research on High-Confidence Transportation Cyber-Physical Systems: Automotive, Aviation and Rail*, Washington, DC, Nov. 2008.

[15] R. L. Bashshur, T. G. Reardon, and G. W. Shannon, "Telemedicine: A new health care delivery system," *Annual Review of Public Health*, vol. 21, no. 1, pp. 613–637, 2000.

[16] J. A. Stankovic, I. Lee, A. Mok, and R. Rajkumar, "Opportunities and obligations for physical computing systems," *Computer*, vol. 38, no. 11, pp. 23–31, Nov. 2005.

[17] A. Sorensen and H. Gardner, "Programming with time: cyber-physical programming with impromptu," in *Proc. of the ACM international conference on Object oriented programming systems languages and applications (OOPSLA)*, Reno/Tahoe, NV, Oct. 2010, pp. 822–834.

[18] A. Benveniste, "Loosely time-triggered architectures for cyber-physical systems," in *Proc. of the Conference on Design, Automation and Test in Europe (DATE)*, Dresden, Germany, Mar. 2010, pp. 3–8.

[19] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proceedings of the 3rd conference on Hot topics in security*, San Jose, CA, 2008, pp. 6:1–6:6.

[20] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[21] J. Sztipanovits, "Composition of cyber-physical systems," in *Proc. of 14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS)*, Tucson, AZ, Mar. 2007, pp. 3–6.

[22] T. Wolf, M. Zink, and A. Nagurney, "The cyber-physical marketplace: A framework for large-scale horizontal integration in distributed cyber-physical systems," in *Proc. of the Third International Workshop on Cyber-Physical Networking Systems (CPNS) held in conjunction with the IEEE 33rd International Conference on Distributed Computing Systems (ICDCS)*, Philadelphia, PA, Jul. 2013, pp. 296–302.

[23] T. Wolf, J. Griffioen, K. L. Calvert, R. Dutta, G. N. Rouskas, I. Baldine, and A. Nagurney, "Choice as a principle in network architecture," in *Proc. of ACM Annual Conference of the Special Interest Group on Data Communication (SIGCOMM)*, Helsinki, Finland, Aug. 2012, pp. 105–106, (Poster).

[24] ——, "ChoiceNet: toward an economy plane for the Internet," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 58–65, Jul. 2014.

[25] X. Chen, T. Wolf, J. Griffioen, O. Ascigil, R. Dutta, G. Rouskas, S. Bhat, I. Baldin, and K. Calvert, "Design of a protocol to enable economic transactions for network services," in *Proc. of IEEE International Conference on Communications (ICC)*, London, UK, Jun. 2015, pp. 5354–5359.

[26] X. Chen, H. Cai, and T. Wolf, "Multi-criteria routing in networks with path choices," in *Proc. of 23rd IEEE International Conference on Network Protocols (ICNP)*, San Francisco, CA, Nov. 2015.

[27] N. Javed and T. Wolf, "Automated sensor verification using outlier detection in the internet of things," in *Proc. of The Second International Workshop on Cyber-Physical Networking Systems (CPNS) held in conjunction with The IEEE 32nd International Conference on Distributed Computing Systems (ICDCS)*, Macau, China, Jun. 2012, pp. 291–296.

[28] A. Nagurney, "Supply chain network design under profit maximization and oligopolistic competition," *Transportation Research E*, vol. 46, pp. 281–294, May 2010.

[29] ——, "Formulation and analysis of horizontal mergers among oligopolistic firms with insights into the merger pradox: A supply chain network perspective," *Computational Management Science*, vol. 7, pp. 377–401, 2010.

[30] ——, "A system-optimization perspective for supply chain network integration: The horizontal merger case," *Transportation Research E*, vol. 45, pp. 1–15, 2009.

[31] Z. Liu and A. Nagurney, "Risk reduction and cost synergy in mergers and acquisitions via supply chain network integration," *Journal of Financial Decision Making*, 2011.

[32] A. Nagurney and T. Woolley, "Environmental and cost synergy in supply chain network integration in mergers and acquisitions," in *Sustainable Energy and Transportation Systems, Proc. of the 19th International Conference on Multiple Criteria Decision Making*, ser. Lecture Notes in Economics and Mathematical Systems, M. Ehrgotta, B. Naujoks, T. Stewart, and J. Wallenius, Eds., Berlin, Germany, 2010, pp. 51–78.

[33] D. Coffield and D. Shepherd, "Tutorial guide to Unix sockets for network communications," *Computer Communications*, vol. 10, no. 1, pp. 21–29, Feb. 1987.

[34] P. Stelmach, P. Schauer, A. Kokot, and M. Demkiewicz, "Universal platform for composite data stream processing services management," in *New Results in Dependability and Computer Systems: Proceedings of the 8th International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, September 9-13, 2013, Brunów, Poland*, W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, and J. Kacprzyk, Eds. Heidelberg: Springer International Publishing, 2013, pp. 399–407.

[35] J. C. Cardona Restrepo and R. Stanojevic, "A history of an internet exchange point," *SIGCOMM Computer Communication Review*, vol. 42, no. 2, pp. 58–64, Apr. 2012.

[36] A. Gupta, L. Vanbever, M. Shahbaz, S. P. Donovan, B. Schlinker, N. Feamster, J. Rexford, S. Shenker, R. Clark, and E. Katz-Bassett, "SDX: A software defined internet exchange," in *Proc. of the 2014 ACM Annual Conference of the Special Interest Group on Data Communication (SIGCOMM)*, Chicago, IL, Aug. 2014, pp. 551–562.

[37] A. Nagurney and Q. Qiang, *Fragile Networks: Identifying Vulnerabilities and Synergies in an Uncertain World*. Wiley Publishing, 2009.