systems

MDPI

Review

Research Challenges for the Internet of Things: What Role Can OR Play?

Peter J. Ryan [1] and Richard B. Watson [2,*]

[1] Defence Science & Technology Group, Fishermans Bend VIC 3207, Australia; peter.ryan@dsto.defence.gov.au
[2] 72 Glenburnie Rd, Vermont VIC 3133, Australia
* Correspondence: richardwatson@tpg.com.au; Tel.: +61-3-9874-1490

Academic Editor: Ockie Bosch
Received: 16 December 2016; Accepted: 8 March 2017; Published: 14 March 2017

Abstract: The Internet of Things (IoT) is an extension of the Internet in which large numbers of "things", including sensors, actuators and processors, in addition to human users, are networked and able to provide high resolution data on their environment and exercise a degree of control over it. It is still at an early stage of development, and many problems/research challenges must be solved before it is widely adopted. Many of these are technical, including interoperability and scalability, as billions of heterogeneous devices will be connected, but deciding on how to invest in the IoT is a challenge for business, and there are also major social, legal and ethical challenges, including security and privacy of data collection, which must be resolved. As the future IoT will be a multi-national, multi-industry, multi-technology infrastructure, the paper reviews the global standardization efforts that are underway to facilitate its worldwide creation and adoption. The main purpose of the paper is to give a broad survey, based on published literature, of the methods of Operations Research (OR), both the mathematical tools and techniques of "hard" OR, and the various approaches of Systems Thinking, including "soft" OR, which may assist in dealing with these problems. A subset of these is described in greater depth to better convey what might be involved in applying OR and Systems Thinking to the IoT. It is suggested that OR has a role to play in balancing the technical and non-technical research challenges which confront the IoT.

Keywords: Internet of Things; Operations Research; hard OR; soft OR; Data Analytics; Soft Systems Methodology; Systems Thinking; General Systems Theory; Complexity Theory

1. Introduction

The field of Operations Research (OR) is an applied discipline which aims to help solve real world problems. It includes many mathematical tools and techniques, plus the sub-discipline of Systems Thinking, which itself has many varieties, both quantitative and qualitative. Both forms of OR can support the design, management and use of the Internet of Things (IoT) which, as discussed in the next section, is a type of new technology which promises to change the world. Conversely, the "big data" obtained from the IoT can support some of the quantitative tools and techniques of OR, e.g., the OR sub-discipline of Data Analytics [1]. OR and the IoT have many application areas, to which they may both be applied jointly or separately, e.g., the "smart city", where the OR techniques of routing, scheduling, discrete-event simulation, etc., may enable more efficient traffic management, energy usage, etc. Many OR techniques require much real-world data, and so OR techniques combined with "big data" from the IoT can be a powerful combination. The "things" making up the IoT include processors which can carry out some of the computational tools and techniques of OR, so this part of OR can be considered part of the IoT.

Hundreds of papers have been written on the IoT, mostly dealing with the supporting technologies and technical research challenges, but increasingly also dealing with the IoT business ecosystem,

and the social, legal and ethical problems that will arise with its adoption. Few single papers discuss both the technical and non-technical research challenges of the IoT on an equal footing. We believe that the holistic view provided by OR and Systems Thinking presented here [2] is going to be needed to solve the many problems which must be overcome for the IoT to realize its full potential. Studying the IoT as a whole requires knowledge from many technical disciplines, including distributed systems, mobile computing, human-computer interaction, cloud computing, artificial intelligence and data semantics, as well as many non-technical disciplines, and the many business, domestic and personal fields to which the IoT is or will be applied. Thus writing about the IoT from a holistic perspective requires a breadth of knowledge and experience rarely found in one individual and is best done by a multidisciplinary team. The authors of this paper have long experience in some branches of OR and Systems Thinking and some fields of Information and Communications Technology (ICT), but are naturally not experts in all the fields which it covers.

The aim of this paper is to identify the main research challenges for the future IoT to which OR, including Systems Thinking, may make a significant contribution. The research approach we take is, in part, a survey of existing papers which apply particular OR tools, techniques and systems methodologies to the IoT. Some IoT research challenges may not have been tackled by OR as yet, or we may not have found any accounts thereof, and in such cases the authors use their knowledge of OR, systems methodologies and the IoT to outline how we think these approaches could support the IoT. The paper does not present any detailed "solutions" to the problems/research challenges we discuss, but does try to give some idea of what might be involved in applying OR and systems methodologies to them.

The remainder of this paper is organized as follows. Section 2 reviews the IoT, both present and future, including research challenges to its development and adoption, and the worldwide standardization efforts now underway to facilitate the interoperability of the many networks and systems making up the IoT. Section 3 gives an overview of the contribution that both the mathematical tools and techniques of OR and Systems Thinking can make to the development of the IoT, and how the sensor-derived data and data processing of the IoT can support the computational techniques of OR. Section 4 gives a more detailed overview of how OR and Systems Thinking can be applied to some of the major research challenges of the future IoT. Finally, Section 5 presents our conclusions.

2. The Internet of Things

2.1. General Concept of the IoT

The IoT is regarded as the next phase in the evolution of the internet. It will enable commonplace devices to be connected to the internet to achieve many disparate goals. With potentially billions of devices to be connected, it is clear that standardization will be required in order to avoid chaos. One estimate is that only 0.6% of objects that could be part of the IoT are currently connected. By 2020, there could be up to 50 billion devices connected to the internet, far greater than the number of human users as shown in Figure 1 below. The growth in the IoT follows an exponential curve while the growth in the number of human users follows a logarithmic curve.

Electronics miniaturization, cost of electronic components, and the trend towards wireless communications are the three main drivers for IoT. These features are enabling physical objects to contain tiny embedded sensors and actuators that can connect to the internet. The core components of the IoT will be sensors and actuators, embedded processing, and connectivity and the cloud. Smart objects such as modern phones use sensors and actuators to interact with the real world. Embedded processing gives smart objects intelligence while connectivity and the cloud provide the means to communicate and store data. The IoT will ultimately evolve into a network of people, processes, data, and physical objects that intercommunicate using wireless protocols.

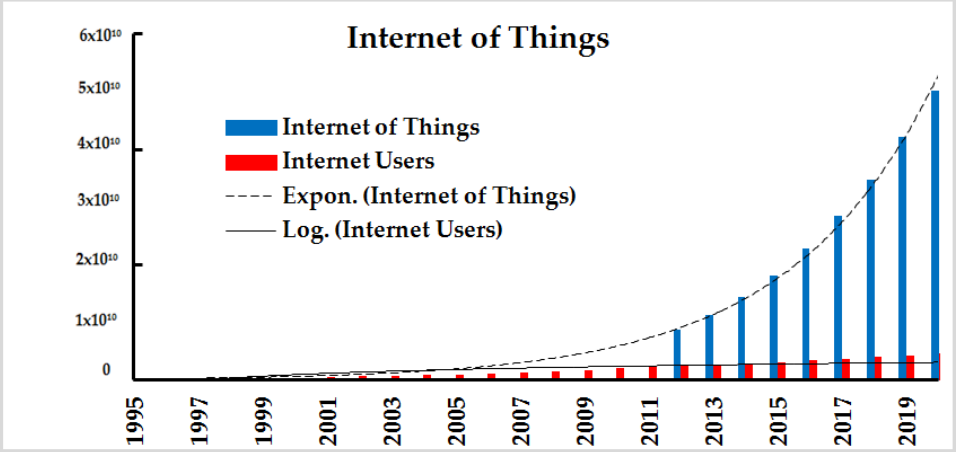

Figure 1. Internet of Things growth (data from http://www.internetlivestats.com/internet-users/ and IoT stats: statista.com). The red bars show the number of human internet users for the period 1995–2020; the blue bars show the number of devices connected to the internet, while the trend lines show a logarithmic growth for human users and exponential growth for number of devices connected.

2.2. Research Challenges for the Future IoT

There are many research challenges associated with the IoT. We know some of them now, others will emerge in the future. These cover the whole field, including the technical challenges of designing, managing and using a multi-national, multi-industry, multi-technology infrastructure, the business challenges of developing IoT business models, and the organizational, political and social challenges of a new technology which promises to change the way we live and work in major ways.

Before we consider the role OR might play in supporting the IoT, the major research challenges must be identified. Many recent surveys of the IoT include a section on research challenges, and we have attempted to consolidate their results for our purposes. This was a difficult task due to differences in terminology by different authors, the fact that the different research challenges cannot be completely separated from each other, and the fact that they can be described at different levels of detail. For example, a very high level research challenge might be "IoT design", but this includes a number of lower level research challenges such as "architecture", "interoperability" and "scalability". Each of these lower level research challenges may include other still lower level research challenges, e.g., IEEE's Standard for an Architectural Framework for the IoT includes the research challenges of protection, security, privacy and safety [3]. Some authors consider IoT Standardization to be a research challenge in its own right, however we consider this to be a high level research challenge which encompasses many lower level research challenges and so do not list it separately. We discuss standardization in Section 2.3 below.

The main survey papers on which we have drawn for our list of technical research challenges are the following: Borgia [4], Jain [5], Stankovic [6], Mattern [7], Elkhodr [8], Gubbi [9], Chen [10], Muralidharan [11] and Al-Fuqaha [12]. Our consolidated list is shown in Table 1.

Table 1. The main IoT technical research challenges linked to the main papers mentioning them, marked as x.

Papers Mentioning	Borgia 2014	Jain 2014	Stankovic 2014	Mattern 2010	Elkhodr 2013	Gubbi 2013	Chen 2014	Muralidharan 2016	Al-Fuqaha 2015
Design									
Architecture	x		x			x	x	x	x
Interoper-ability	x	x		x	x			x	x
Scalability		x	x	x					x
Mobility	x			x					x
Security/Privacy	x	x	x	x	x	x	x	x	x
Scientific/Engineering									
Energy Efficiency/Power		x		x		x	x	x	
Reliability/Robustness	x		x	x					x
Management/Operations									
Software Development				x				x	
Availability									x
Data Management/ Information Fusion	x	x	x	x		x	x		
Cloud Computing		x				x			
Performance	x					x			x

We have divided these research challenges into the categories of Design, Scientific/Engineering and Management/Operations, although this is somewhat artificial, as several research challenges belong to more than one category. For example, Reliability/Robustness is a challenge at both the design and operational stages, as is Security/Privacy. For detailed discussion of these technical research challenges, the reader is referred to the original references. Some challenges are only mentioned by a few references, e.g., Availability by Al-Fuqaha et al. [12] and Cloud Computing by Gubbi et al. [9] and Jain [5]. This is perhaps understandable as there are so many technologies which contribute to the IoT that developing expertise in all of them is a considerable challenge. We note that a recent special issue of the journal *Computer Communications* [13] is entirely devoted to IoT research challenges, albeit predominantly technical. The research challenges listed in Table 1 apply to all or most IoT application areas, however their relative importance may vary between particular areas. There are also special research challenges that apply in particular application areas, such as defence and public safety [14].

The business challenges confronting the IoT are covered by the following main references: Chen et al. [10], Dijkman et al. [15] Kim and Kim [16], Lee and Lee [17], Mazhelis et al. [18] and Westerlund et al. [19]. We discuss some of them in connection with the OR techniques of Decision Analysis (Section 3.1.2) and Game Theory (Section 4.3), and with the Multimethodology approach of Systems Thinking (Section 4.9).

Some of the technical and business challenges of the IoT may be solved with the help of the mathematical tools and techniques of OR. This paper is only concerned with the contributions the discipline of OR can make, not the many other disciplines which can contribute. However we consider OR to include Systems Thinking, which sees the IoT as a complex, self-organizing system, with a large number of components, an environment, and emergent properties. A bibliometric study of the articles published on IoT from 2000 to 2015 [20] concluded that much more research was needed that shifts the focus from purely technological to the socio-organizational implications of IoT adoption. Some work along these lines has been done in recent years in the UK [21–26] as well as several reports on many aspects of the IoT by the European Research Cluster on the Internet of Things [27]. The key social, legal and ethical issues facing the IoT, as discussed by the Oxford Internet Institute [26] are:

- Privacy and data protection;
- Global misinformation systems;
- Big data problems;
- Public attitudes, opinions and behavior;
- Tightly coupled systems;
- Quality of service issues;
- New forms of risk; and
- Linking the IoT to work on responsible innovation

In Section 3 we present a table cross-referencing the technical and business research challenges for the IoT, and the applicable mathematical tools and techniques of OR (optimization, simulation, etc.), and another table for all the main research challenges for the IoT, including some social and policy challenges, and the varieties of Systems Thinking (General Systems Theory, SD, SSM) which have been or could be used to help improve (not "solve") them. Some Systems Thinking approaches, e.g., self-organizing systems theory, can contribute to both the technical challenges and the social and policy challenges. In this paper, we take a holistic view which sees the technical, social and policy challenges of the IoT as being intertwined.

2.3. Development of Standards for the Future IoT

By standards we mean guidelines for "how to do" the activities which must be done at all levels in designing, managing and using the IoT, not just highly technical standards, e.g., the Constrained Restful Environments (CoRE) standard for integrating constrained devices with the Internet. Standards are needed for application requirements, communication protocols, identification of objects, security,

applications, data, information processing, and the service platforms [10]. Indeed IoT itself does not yet have a standard definition [11]!

Major international standards development organizations (SDOs) including IETF, ISO, IEEE, IEC, and ITU are examining what needs to be standardized for the IoT to succeed. These efforts are focussed on the technical level, addressing data link protocols (such as Radio-Frequency IDentification (RFID), Zigbee, Bluetooth, Near Field Communication (NFC), network/transport protocols (Internet Protocol version 6 (IPv6), IPv6 over Low power Personal Area Networks (6LoWPAN) and Routing Protocol for Low-Power and Lossy Networks (RPL)) and session protocols (such as Message Queue Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Extensible Messaging and Presence Protocol (XMPP), and HyperText Transfer Protocol (HTTP). The efforts of these major organizations are discussed below.

The Internet Engineering Task Force (IETF) has been specifying and documenting IoT standards for over a decade [28,29]. This organization has developed protocols and open standards for connecting wireless sensor networks (WSN) to the internet. These standards include:

- IPv6 over Low Power Wireless Personal Area Networks which defines IPv6 adaption layer and header compression suitable for constrained radio links;
- Routing over Low Power and Lossy Networks (ROLL), which focusses on routing protocols for constrained-node networks; and
- Constrained Restful Environments which aims to extend Web architecture to most constrained networks and embedded devices.

More recently, IETF has been working in the area of IoT security. A key project is the Datagram Transport Layer Security (DTLS) that is the most suitable way to achieve channel security.

ISO (the International Organization for Standardization) collaborates with its partners in international standardization, the IEC (International Electrotechnical Commission) and the ITU (International Telecommunication Union). These three organizations, all based in Geneva, Switzerland have formed the World Standards Cooperation to better coordinate their activities, as well as the implementation of International Standards.

ISO/IEC created a Special Working Group (SWG) IDO/IEC JTC 1/SWG 5 within its Joint Technical Committee 1 in the information technology domain in 2013 [30]. IEEE and ITU also contributed to this SWG. This SWG released a preliminary report in 2014 [31] that considered a common understanding of IoT, market requirements, standardization gaps, and reference architectures. ISO also produced this definition of IoT:

> *"An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react."*

A catalogue of more than 400 existing standards that relate to IoT was examined and mapped to the relevant IoT technology such as common interfaces and protocols, power requirements, and security constraints. The SWG has been disbanded and was replaced by an official ISO working group in 2014: WG10: Internet of Things. There are nearly 500 working documents on the ISO WG10 site that address aspects of IoT including reference architectures, interoperability, security, definition and syntax. A draft standard IoT Reference Architecture (ISO/IEC N13119) has been developed [32]. The reference architecture describes characteristics of IoT systems, defines IoT domains, describes a reference model for IoT systems and the interoperability of IoT entities. This working group has now been converted to an official subcommittee of JTC1—SC41 [33]. SC41 has 3 working groups—Sensor Networks, Internet of Things, and Wearable Technologies.

IEEE formed an IoT Technical Community that runs conferences and also publishes the IEEE Internet of Things journal [34]. The IEEE IoT group is also engaging its stakeholders in standardization efforts, such as IEEE P2413 a draft standard for an architectural framework for the IoT [3]. P2413

describes IoT domains, and identifies commonalities between different domains. It also provides a model for data abstraction and quality.

ITU initially established an IoT Global Standards Initiative [35] that aimed to promote a unified approach to development of technical standards for IoT. This initiative ended its activities in 2015 and ITU has now established a new Study Group on IoT and its applications including smart cities and communities.

The Simulation Interoperability Standards Organization (SISO) is also looking at opportunities for IoT standardization from a modelling and simulation (M&S) perspective [36]. Many of the goals of the M&S community are similar to the goals of IoT: timely environmental data (for live simulations), representation of systems, and representation of human behavior. The IoT can provide these inputs to the virtual world through sensors embedded in the real world that provide live environmental feeds, and human biometric and behavior data. This would enhance representation of live entities in Live Virtual Constructive simulations. We note that SISO researchers have applied a process model (IEEE Std 1730) developed for distributed simulations to a simulation of IoT cyber security that can include real devices [37].

Various other organizations and industry consortia are working on aspects of IoT standardization under a range of projects and alliances. The main consortia include the AllSeen Alliance (includes CISCO and Microsoft), the Industrial Internet Consortium (includes Intel, Dell, and Samsung), Open Interconnect Consortium (includes IBM, Intel), and Thread (includes ARM and Samsung) [38]. These consortia are not mutually exclusive with some companies in several consortia. OneM2M is another initiative that is developing specifications for machine to machine services for IoT. This initiative also comprises the major SDOs IETF, IEEE, ISO/IEC, OGC, and ITU.

Systems Engineering will also be critical for the IoT to succeed [39,40]. Systems Engineering Standards such as ISO/IEC 15288, Software Engineering Standards including ISO/IEC 12207 and ISO/IEC 29110 for very small software development organizations [41] and Project Management Standards (e.g., ISO 21500) have been developed by SDOs in recent years. However, as will be discussed in Section 4.4, the IoT can be viewed as a Complex Adaptive System, and traditional Systems Engineering standards may break down for such systems [42]. Table 2 contains the profiles of five key traditional Systems Engineering standards.

Table 2. Profiles of the five Systems Engineering Standards (adapted from [43]). Note INCOSE—International Council on Systems Engineering; SEBoK—Systems Engineering Body of Knowledge; SEMP—Systems Engineering Management Processes.

	ANSI/EIA-632	**IEEE-1220**	**ISO/IEC-15288**	**INCOSE HANDBOOK**	**SEBoK**
Content	13 processes 34 requirements	8 processes	25 processes	25 processes	26 processes
Focus of systems life cycle	Conception and development	all systems	all systems	all systems	all systems
Pages	110	70	70	400	850
Level of details	2/5	2/5	2/5	4/5	5/5
Context of applications	Program and project environment	Program and project environment	Enterprise environment	Enterprise environment	External environment
Publication Year	1998	2005	2008	2010	2013
Reversion frequency	2/5	2/5	5/5	3/5	1/5
No. SEMPS	3	1	12	12	12
SEMP's proportion	3/13	1/14	12/25	12/25	12/26

3. How can OR Support the Future IoT?

3.1. The Mathematical Tools and Techniques of OR Which May Support the IoT

Below we give a brief synopsis of the main OR tools and techniques which may support the IoT, and our reasons for thinking so. These are drawn from OR textbooks, such as Daellenbach and Flood [44] and the many journal articles and conference papers we have reviewed for this survey.

3.1.1. Data Analytics/Databases

Data Analytics is the science of studying data to draw conclusions. With billions or even trillions of devices connected to the IoT, there will be vast amounts of data including identification, positional, environmental, historical, and descriptive data [45]. This IoT data will create data management and analysis issues. According to Ma et al. [46], IoT data will have characteristics of heterogeneity, inaccuracy, massive real time, and implicit semantics leading to significant data management issues.

Cooper and James [45] and Ma et al. [46] addressed challenges for database management in IoT that will bring vast amounts of data. Data is categorized into RFID, address/identifiers, description, positional and environmental, sensor, historical, physics and command. eXtensible Markup Language (XML) offers a means of representing unstructured data; while Structured Query Language (SQL) is unlikely to be useful since IoT data will not be uniform and structured. Service Oriented Architecture may be used to support interoperability among IoT systems. Data indexing, archival and protection must also be considered with respect to national data protection laws. Methods for querying semi-structured data, data streaming, sampling continuous data and data mining will need to be developed to manage the size of IoT databases.

3.1.2. Decision Analysis/Support Systems Including Analytic Hierarchy Process (AHP), Multi-Criteria Decision Making (MCDM) and Data Envelopment Analysis (DEA)

Dijkman et al. [15] developed a business model framework for the IoT using a literature survey and interviews. Their model has nine building blocks: customer streams, value proposition, channels, customer relations, revenue streams, key resources, key activities, key partners and cost structure. The model showed that the value proposition is the most important item while customer relationships and key partnerships are also considered important. Data were sourced mainly from Netherlands and US as the authors acknowledge.

Westerlund et al. [19] explored the challenges relating to the development IoT business models. These include the diversity of the objects, the general immaturity of IoT and the unstructured nature of the IoT ecosystems. They suggest a potential solution with a conceptual model that includes value drivers, value nodes, value exchanges, and value extracts as pillars.

Kim and Kim [16] adapted an Analytic Hierarchy Process model to three IoT applications: healthcare, logistics, and energy management using criteria of technology, market potential, and regulatory environment. Survey data that were analyzed using the model showed that market potential was the most important criterion in the first layer of the model and concluded that IoT logistics is the most promising application from the perspective of ICT experts. Healthcare needs to overcome user barriers and technical reliability to be accepted whereas energy management requires government support (Korean Smart Grid initiative [11]).

Petkov et al. [47] combined multiple criteria decision making with a soft systems approach for what they term 'messy problems', ill-structured situations with multiple independent problems. This approach is applied to several test cases including a rural telecommunication system in South Africa. This approach may also be applicable to complex ICT systems that will make up the IoT.

Decision support has been widely used for IoT applications, generally for assessment of potential IoT solutions. It is likely to continue to be an important tool as the range of IoT applications develops.

3.1.3. Game Theory

Game theory is a method of understanding interactions among groups in conflict with each other. Each side can choose between several actions with the outcome dependent on the actions taken by all players.

Haghighi et al. [48] used a game theory approach to optimize task distribution and energy consumption in IoT networks. An auction-based approach to determine prices was adopted to solve conflicts among network peers.

Wang et al. [49] applied a game theory approach with a Pervasive Multipath Architecture approach to investigate multi-tasking and data distribution in the IoT using the OPNET simulation tool. The scenario studied featured multiple selfish overlays delivering traffic in a shared multipath network. The optimal criterion used is to maximize each overlay's utility function.

Game Theory has also been applied to develop business models [50] as discussed in Section 4.3.

3.1.4. Simulation

Discrete-event simulation simulates the operation of a system as a discrete sequence of events with each event marking a change of state of the system. Between events, no change in the system state is assumed. Discrete-event simulation can be applied to the study of issues in IoT networks. Dyk et al. [51] applied discrete-event simulation to model a heterogeneous sensor network with smart devices connected. The model can incorporate the effects of phenomena such as weather and crisis situations on the network state. This could be readily extended to examining similar effects for heterogenous IoT networks.

There are many simulation models available for networks that can be applied to IoT. Musznicki and Zwierzykowski [52] identified 36 such systems for WSNs ranging from low level emulators to simulators for topology and environment (see Section 4.1). Atarraya, for example, is a discrete-event simulation that simulates topologies for networks enabling testing of algorithms and protocols [53]. An earlier survey of WSN simulation tools was done by Korkalainen et al. in 2009 [54].

Discrete-event simulation would appear to be an ideal approach to studying many of the design and engineering challenges for IoT such as scalability and energy efficiency by constructing a synthetic environment where new concepts can be safely tested. We discuss in more detail how simulation can support the IoT research challenge of Scalability in Section 4.1.

3.1.5. Fuzzy Systems Theory/Artificial Neural Networks

Fuzzy systems use fuzzy logic where input variables can take on continuous values, in contrast to digital systems that operate on discrete values. Ribiero et al. [55] developed a fuzzy information algorithm using multi-criteria decision analysis and applied it to spacecraft landing safety. This technique could also be applied to IoT research areas.

Artificial Neural Networks represent an approach to Artificial Intelligence that uses a network of many interconnected units generally organized into layers. These units operate on inputs from units in lower layers using an approach that mimics the human brain.

Fuzzy logic and artificial neural networks are important techniques in data fusion, in which the data from many sensors is combined in various ways [56,57]. This is an important function in the IoT.

Chen et al. [58] developed an artificial neural network trust and reputation model and applied it to predict vulnerability of the IoT against malicious attacks.

3.1.6. Routing/Scheduling

Routing describes techniques to select best paths for a set of processes. Scheduling is an OR technique for allocating time to tasks for machines, jobs, and projects.

Both these techniques have application for the IoT. For example, routing could be applied to network design while scheduling could be applied to traffic management within the IoT. Dhumane et al. [59] conducted a survey of current routing protocol issues used for IoT and identified challenges for research including context awareness, heterogeneity, node death, topology changes, scalability, latency, incentive based routing, congestion control, data security, data redundancies, and multipath routing. They emphasized the importance of routing processes for the IoT and demonstrated the need to develop new routing protocols.

3.1.7. Reliability Theory

Reliability theory can describe the probability of a system achieving its expected performance. The reliability of a system is determined by considering the reliability function of each component.

Yong-Fei et al. [60] used reliability theory to evaluate the reliability of the IoT. Five reliability functions were included for perception layer, Internet, mobile network, satellite communications, and application layer. A value of 0.87 was determined for the overall IoT reliability based on their assumptions. However, this must be considered as an estimate only since the IoT is still rapidly developing and the authors may not have considered all factors.

Reliability Theory can further be applied to other IoT requirements such as Quality of Service and even data management. How reliable is the data acquired by the IoT? Ma et al. [46] note that the reliability of data from IoT sensors will depend on factors such as data loss, noise, invalid data, and data redundancy where several sensors have measured the same object. A reliability model for IoT data could be constructed from consideration of all these factors.

We discuss in more detail how Reliability Theory can support the IoT research challenge of Robustness in Section 4.2.

3.1.8. Queuing Theory

Queuing theory is the mathematical study of queues. It is used in OR for developing more efficient queuing systems such as customer service in a bank. Queuing Theory is an ideal tool for studying behavior of computer networks where the messages (packets) are the customers and the service is the assignment of the messages to communication links [61]. Queuing Theory can help determine network response and throughput by making assumptions about message distribution and node response.

Mahamure et al. [62] applied queuing theory to a hypothetical IoT email system that uses the IMAP protocol (Inter Mail Access Protocol). They propose to use email for human users to communicate with IoT devices such as found in the future home (appliances, security devices etc.) using SMS messages.

3.1.9. Graph Theory

Graph theory uses geometric structures (graphs) to model relations between objects. It was invented in the 1700s to solve the Konigsberg Bridge Problem by the famous Swiss mathematician Leonard Euler [63].

Yao et al. [64] applied graph theory to assist in defining and understanding the IoT. Graph theory is used to show that the IoT is the union of three networks: a topological network, a data-functional network and a domi-functional network. It has also been applied to computer network security [65], mobile phone networks, ad-hoc networks, sensor networks and fault tolerance computing [66], all relevant to the IoT.

3.1.10. Other OR Techniques

Other OR techniques that can be applied include evolutionary algorithms such as genetic algorithms (GA). These are a class of search heuristics modelled on nature that were developed in 1975 by Holland [67]. Esmaeili and Jamali applied GA to optimize energy consumption, a key issue for IoT networks [68]. These authors developed and tested several new algorithms to optimize energy consumption in WSNs.

Singh et al. [69] surveyed optimization techniques for RFID used in the IoT, finding that approaches including Ant Colony Optimization, Differential Evolution, Particle Swarm Optimization, GA Optimization, and Artificial Bees Colony Optimization have been proposed. Comparison of these approaches showed that no single method was ideal; each had its strengths and limitations.

Fortino et al. [70] applied an agent-based paradigm to simulate agent-oriented IoT systems in various scenarios assuming that the IoT is mostly composed of smart objects (as well as RFIDs). They found this to be an effective approach to study IoT features such as traffic load and protocol reliability. Houston et al. [71] recently applied this technique to study return on investment for IoT.

3.1.11. Summary

Table 3 contains a non-exhaustive list of mathematical OR techniques that have been applied to understand and develop the IoT.

Table 3. Mathematical OR techniques applied to IoT.

Method	Application
Game Theory	Multi-tasking, data distribution
Math programming—Linear, nonlinear, integer, dynamic	Network design
Simulation	Environmental effects on IoT
Neural Nets	Security; sensor data analysis
Stochastic (Markov) Processes	Reliability/robustness
Graph Theory	Network flow; Routing
Queueing Theory	Network response; Network
Critical Path Method	
Decision Analysis—Multi criteria, analytic hierarchy	Assessing business models for IoT
Genetic algorithms	Energy consumption
Optimization approaches	RFID
Agent-based modelling	Traffic load; protocol selection; smart object interaction

Table 4 lists the main IoT Technical and Business research challenges together with OR tools that can be applied. As in Section 2.2, the Technical research challenges are divided into three areas: Design, Scientific/Engineering and Operations/Management. Many OR approaches are being applied to understand and develop the IoT, although these efforts are still in their early stages.

Table 4. IoT Technical and Business Research Challenges and OR Tools/Techniques applicable.

IoT Challenge	OR Tools/Techniques Applicable	Examples; Notes
	Design	
Architecture	Data analytics, optimization, game theory	Wang et al. [49] use GT to study architectures
Interoperability (Addressing/ Naming Objects)		
Scalability	Simulation	Musznicki and Zwierzykowski [52]
Mobility	Simulation	
Security/Privacy	Data analytics; fuzzy systems; graph theory	Chen et al. [58]; Yao et al. [64]; Shirinivas et al. [66]
	Scientific/Engineering	
Energy Efficiency/Power	Simulation; Game theory; decision analysis	Haghighi et al. [48]—GT; Kim et al. [16]—decision analysis
Reliability/Robustness	Reliability theory	Yong-fei et al. [60]—RT
	Management/Operations	
Software Development	Expect simulation to help?	Musznicki et al. [52]
Availability	Reliability theory; simulation should apply	
Data Management/Information Fusion	Game theory; data analytics	Cooper and James [45] Petkov et al. [47]
Cloud Computing	Decision analysis; data analytics	Cooper and James [45] Petkov et al. [47]
Performance (Quality of Service)	Optimisation; reliability theory; queuing theory; math programming; stochastic processes	
	Business	
Business Models	Decision analysis; Game theory; Agent-based modelling; Data analytics	Dijkman et al. [15]; Westurland et al. [19]; Houston et al. [71]
Use cases (e.g., Korea/China); killer apps (e.g., medical)	Decision analysis; MCDM	Kim et al. [16]; healthcare, energy

3.2. Application of General Systems Thinking to the IoT

In this paper we follow the classification of Systems Thinking approaches used by the comprehensive review of Mingers and White [2]. An alternative classification of Systems Thinking approaches, and the types of problem situation for which they are considered most appropriate, are given by Jackson and Keys [72]. Table 5 depicts the Systems Thinking approaches we consider, cross-referenced to the main IoT research challenges to which we think they could contribute. We do not claim that these are the only IoT research challenges that may be addressed by these Systems Thinking approaches, but they certainly include the most important. All these research challenges may be supported by more than one Systems Thinking approach, and this is why we show the CST/Multimethodology approach as being applicable to all. In Section 4 we discuss in detail how we see some of the research challenges being addressed by one of the applicable Systems Thinking approaches.

Table 5. Cross referencing the main IoT multi-disciplinary Research Challenges to which the various Systems Thinking Approaches may make an important contribution, marked as x.

Systems Thinking Approach →	GST/ Complexity Theory	Self-Organizing Systems Theory	Cybernetics/ System Dynamics	Soft Systems	CST/ Multimethodology
Network Design	x	x	x		x
Complex Adaptive System	x	x	x		x
Self Organizing System	x	x	x		x
Intelligence & Context Awareness	x	x	x	x	x
Software Development			x	x	x
Network Management/Operations		x	x	x	x
Technology Transfer			x	x	x
Politics/Cross Border Data Flows				x	x
Work Restructuring				x	x
Industry Investment in IoT			x	x	x
Ethical & Legal Framework of IoT				x	x
Security & Privacy				x	x

3.2.1. General Systems Theory (GST)/Complexity Theory

General Systems Theory (GST) was founded by Ludwig von Bertalanffy, an organismic biologist, in the mid-1920s with the intention of identifying and describing systems concepts which could be applied across a range of disciplines, initially to the physical, biological and human sciences and later to the social sciences [73]. These concepts include parts/wholes/sub-systems, system/boundary/environment, structure/process and emergent properties [2]. Complexity Theory is a branch of GST applicable to Complex Adaptive Systems (CAS), which is a type of system that exhibits unpredictable behavior arising from non-linear spatio-temporal interaction among a large number of components and sub-systems [74]. It was developed in the 1970s in a range of disciplines including biology, chemistry, mathematics and economics. In the 1990s it was extended in the US by Holland [75], Bar-Yam [76], and others and is seen as an approach which may assist in tackling the seemingly intractable problems of the modern world including overpopulation and the depletion of the earth's resources, business globalization, the emergence of terrorism, and the extremely complex problem of global warming. In this paper we take a holistic view of the IoT as a CAS, which is why it needs to be tackled by multiple methods drawn from the mathematical techniques of OR and several Systems Thinking approaches, and many other disciplines including law, economics and sociology. We discuss in more detail how GST and Complexity Theory can be applied to the IoT in Section 4.4.

3.2.2. Self-Organizing Systems Theory

The term Self-Organizing Systems refers to a class of systems that are able to change their internal structure and their function in response to external circumstances [77]. The concept was introduced by Ashby in 1947 [78] and the theory started with the study of living systems, but now has applications in fields including organization theory, business strategy, information systems, law and sociology. Note that self-producing or *autopoietic* systems are non-teleological self-organizing systems, i.e., they do not have a specific purpose except their own existence [79]. Note also that many self-organizing systems are CAS. The networks and systems making up the IoT will be subject to disasters, outages and other adversarial conditions, and so will need to be self-organizing. We discuss in more detail how Self-Organizing Systems Theory can be applied to the IoT in Section 4.5.

3.2.3. Cybernetics/Systems Dynamics

The field of cybernetics was founded by Norbert Wiener in the 1940s with the aim of establishing basic principles of automatic control or response mechanisms used by living systems and autonomous operations of complex electromechanical systems [80]. Stafford Beer's Viable Systems Model (VSM) incorporates the principles of cybernetics into an abstract model of any viable or autonomous system [81]. Today the theory has a broad range of application areas including biomedical systems, man-machine systems and large scale socio-economic systems [2]. In this paper we only consider cybernetics as it is embodied into the technique of System Dynamics (SD), which models system behavior in the form of differential equations that relate the time trajectory of system variables, called stocks or levels, and rates-of-flow. We discuss the application of SD to the IoT research challenge of Software Development in Section 4.7.

3.2.4. Soft Systems

Soft Systems methods are a family of approaches for dealing with complex problem situations, which are characterized by multiple actors, multiple perspectives, incommensurable and/or conflicting interests, prominent intangibles and key uncertainties [2]. They include hypergame analysis, Soft Systems Methodology (SSM), interactive planning, social systems design, cognitive mapping, and strategic assumption surfacing and testing. In this paper we only consider SSM as one of the authors (RBW) has used it extensively in researching some very complex socio-technical systems [82,83]. We discuss the application of SSM to the IoT research challenges of Intelligence and Context Awareness in Section 4.6, and that of IoT Technology Transfer in Section 4.8.

3.2.5. CST/Multimethodology

All Systems Thinking approaches aim to view the IoT in a holistic (non-reductionist) way, i.e., not view the IoT components and research challenges in isolation from each other and accept that the IoT will have emergent properties. But it is generally recognized that the different Systems Thinking approaches have different strengths and weaknesses. The approaches can be "hard", which include the mathematical tools and techniques of OR, "soft", such as SSM, or other Systems Thinking approaches like SD, which have both "hard" and "soft" aspects and so cannot really be classified as exclusively one or the other. Critical Systems Thinking (CST) and the Multimethodology approach take a "contingency approach", and adapt the approach taken to the particular problem/research challenge. CST is sometimes regarded as the third stage in the evolution of the history of OR from "hard" to "soft" to "critical", and focusses more on the methodology of OR practice than its tools and techniques. These approaches [84–86] basically say that different aspects of a problem situation, or different stages in an OR intervention, need to be tackled by different OR techniques or systems approaches. The research challenge of investing in the IoT has been addressed by several approaches, some "hard" and some "soft" and we discuss the application of the Multimethodology approach to this problem in Section 4.9.

4. Detailed Discussion of some IoT Research Challenges Which OR and Systems Thinking May Help Address

4.1. IoT Scalability Studied Using Simulation

The first key challenge according to Stankovic [6] is scalability. The IoT will have billions or even trillions of devices connected and these must be managed, maintained, operated and supported using appropriate addressing conventions, protocols, and power. Existing approaches to these challenges may well be inadequate and fail to scale for the anticipated huge number and range of IoT objects.

A simple visualization can show how IoT networks can rapidly become extremely complex. Figure 2 shows three IoT networks composed of equal numbers of sensors and actuators where all nodes are connected to each other. The number of connections grows rapidly from only 6 for a 4-node network, 120 for a 16-node network to 2016 for a 64-node network, since the number of connections for such an N-node network is trivially $N \times (N-1)/2$.

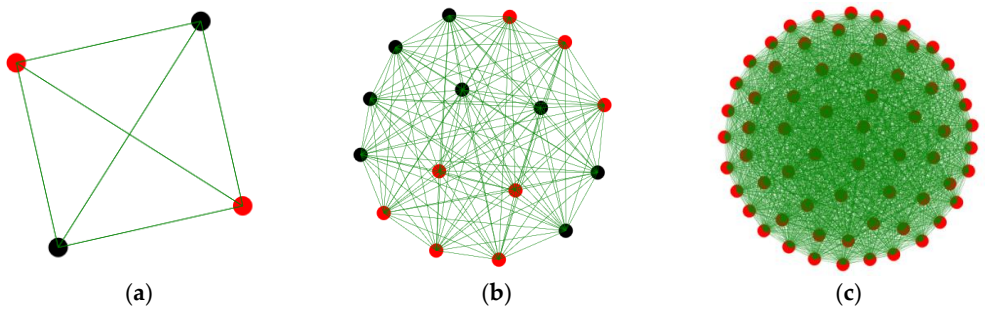

Figure 2. Scaling in IoT networks with: (**a**) 4 nodes; (**b**) 16 nodes; and (**c**) 64 nodes (red circles represents sensors; black circles actuators) (These images were created using the D3 javascript library (https://d3js.org/). One of the authors (PJR) is experimenting with the use of D3 for simulation of the IoT).

To assess scalability, discrete-event Simulation can be applied. As shown, IoT networks can become so complex that traditional analytic methods will not be tractable. Discrete-event simulation enables a hypothetical system to be studied under a wide variety of conditions and provide averaged results from running the same scenario over many replications. Dyk et al. [51] and D'Angelo et al. [87,88] have developed simulation systems for the IoT. D'Angelo's model, for example, addresses scalability using a multi-level simulation approach where both coarse and fine grained models are combined.

Musznicki and Zwierzykowski [52] identified 36 such systems in 2012 for WSNs and classified them into eight types: (a) emulators; (b) topology simulators; (c) environment and wireless simulators; (d) network and application level simulators; (e) cross level simulators, then a series of simulators based on specific software; (f) NS-32 based simulators; (g) OMNeT++ simulators; and (h) Ptolemy II based simulators. Many of these could be applied to address IoT issues such as scalability including type (b) topology simulators such as Atarraya [53] that enables comparison of performance and efficiency of different network topologies, type (c) environment and wireless simulators such as the Wireless Sensor Network Localization Simulator that can determine the location of sensor nodes in different sized networks and type (d) network simulators such as Sensor Security Simulator that can evaluate security in large sensor networks and SIDnet-SWANS that can model network behavior at different levels of granularity.

Discrete-event simulation is readily applicable to studying problems such as traffic flow through an IoT network of nodes. Events would include transmission of packets from one node (perhaps triggered by a sensor) and their reception and processing at other nodes. With many expected wireless nodes, issues such as propagation modelling may also be required [89]. Packet arrival and transmission times would be determined by sampling from appropriate probability distributions. Simulation of the system would show how it performs as a function of number of nodes.

4.2. IoT Robustness Studied Using Reliability Theory

Related to scalability are robustness and reliability. The IoT will be composed of billions of electronic devices, many of which may be impossible to reconfigure or replace in contrast to one's desktop computer or tablet that requires regular software updates and possibly hardware upgrades for more memory, CPU power, or disk space. As stated by Metcalfe's Law, the more interconnections between independent components or subsystems within a system, the greater the complexity and higher the probability of system failures [39]. The ability of the IoT to operate reliably long term despite hardware and software failures is critical to gain user acceptance and trust. According to Kempf et al. [90], bit errors can lead to unmanageable problems in large networks that will characterize the IoT.

OR techniques such as reliability theory can readily be applied to predict IoT robustness and reliability. Yong-Fei and Li-Qin [60] developed an approach using reliability theory for the three IoT subsystems of perception layer, network layer and application layer. Their model assumes that the transmission networks are independent and that the perception and application layers are dependent so that total reliability R_T is given by:

$$R_T = R_1 \times R_5 \times (1 - \prod_{k=2}^{4}(1 - R_k)), \quad (1)$$

where R_1 and R_5 are the reliabilities of the perception and application layers, and R_2, R_3, R_4 are the reliabilities of the internet, mobile network, and satellite communication network. This model could be expanded and updated to include other IoT characteristics and features of newer IoT devices as they come into operation, leading to additional terms in the reliability equation.

Reliability theory could also be applied to other features of the IoT such as the reliability of the data collected [90]. Bonomi et al. [91] discussed the application of so-called Fog Computing to the IoT while Madsen et al. [92] estimated the reliability of this approach by combining the reliability requirements of the grid and cloud with those of the sensors and actuators in the IoT and demonstrate that a reliable system can be achieved.

The reliability of the IoT software itself may be another significant issue since software reliability can be considered as a special case of reliability theory. Hardware reliability is determined by component or material failure that prevents a system performing its intended function. Software reliability in the IoT is more difficult to assess since software may produce unanticipated results for many reasons such as unusual data coming from another device that was not considered in the design phase. Obsolescence of embedded software in IoT systems that cannot be readily maintained (for example, IoT sensors in a nuclear reactor exposed to radiation) may also affect reliability.

4.3. IoT Business Investment Studied Using Game Theory

Establishing business models for the IoT is a key challenge that can be addressed by OR. Decision Analysis has already been applied to this area. However other techniques such as Game Theory (GT) and Discrete-event Simulation may also be applied.

GT has been used to explore technical issues such as multipath selection [49] and data distribution [48] in IoT networks. It could also be used to determine payoffs from different application areas of the IoT. GT has long been applied for business [50] to determine optimal strategies. Major US corporations such as Coca Cola and Pepsi have applied GT to assess business tactics.

Niyato et al. applied GT to study price competition of IoT sensing services noting that traditional system optimization may be unsuitable for IoT due to its complex, heterogeneous nature with multiple entities and incentive mechanisms [93]. Considering the spectrum of potential IoT applications and markets ranging from personal (wearable devices), home (automation, security), transport (driverless cars), enterprise (e.g., smart cities, healthcare) (see [94]), GT could be applied to assess market strategies for developing and timing the release of new IoT products. Home automation systems, for example, may not all be provided by the same supplier but will need to be interdependent and interoperable.

Companies providing competing or complementary systems could use GT to determine appropriate strategies to maximize their market penetration and profits.

Which games types might be most appropriate to assist with making IoT business strategies? Of the 13 game descriptors defined in Wikipedia (Game Theory: https://en.wikipedia.org/wiki/Game_theory), the likely types to study business investment are: (1) cooperative/non-cooperative; (2) symmetric/asymmetric; (3) zero sum/non-zero-sum; (4) simultaneous/sequential; (5) perfect/imperfect information (note that games can have a combination of these characteristics). Consider a situation where three companies provide home automation systems. While each company can supply the full range of equipment and services, Company A specializes in internal devices (such as smart refrigerators and lighting systems), Company B specializes in external devices (watering systems, weather monitors), while Company C specializes in security systems (cameras, monitors, alarms) as shown in Table 6.

Table 6. Three IoT companies and competing business strategies.

Company	Specialty	Potential Investment Area
Company A	Internal systems	External systems
Company B	External systems	Internal systems
Company C	Security systems	All non security systems

Strategies for each company to obtain a profitable share of the marketplace could be determined using the cooperative gaming approach while the decision to invest in their non-specialist areas could also be assessed using other gaming approaches such as constant sum games. In the latter case, this leads to $2^3 = 8$ possible outcomes since each company has 2 strategies: to decide whether to diversify or not. A 3-dimensional payoff matrix is required to describe this case [95].

4.4. Complex Adaptive Systems Theory and the IoT

A Complex Adaptive System (CAS) is a "complex macroscopic collection" of relatively "similar and partially connected micro-structures" formed in order to adapt to the changing environment and increase its survivability as a macro-structure" (wiki and [96,97]). CAS theory was pioneered by John Holland, a computer scientist and founder of the Genetic Algorithm technique, to describe systems with many components that interact and can adapt [75]. The natural world has many CAS systems such as large molecules, human brains, and human societies and economies.

Although early work [98] suggested that the Internet did not exhibit emergent behavior since the packet routing follows an engineering design, it is now generally regarded as a CAS since it is a complex open network that uses adaptive behavior [99]. The IoT is an evolution of the Internet that will dominate the human component by 2020 and thus is also a CAS. CAS theory has also been applied to defense issues where it has been noted that defense systems are now too complex for any human to comprehend [100]. Since a defense force can be shown to exhibit CAS properties, CAS theory can help understand emergent behaviors in adaptive defense systems by analogy with naturally occurring CAS such as living organisms. A NetLogo (https://ccl.northwestern.edu/netlogo/) agent-based CAS model was developed to understand various terrorist scenarios and showed counter-intuitive outcomes [101].

Yan and Ji-hong [102] applied CAS to analyze WSNs. They showed that a WSN has all the characteristics of a CAS such as complexity, emergence and self-organization. Haghnevis and Askin [103] developed a framework for Engineered CAS. They suggest that this could be applied to predict properties of complex engineered systems such as WSNs, and by extension the IoT. Batool et al. [104] discussed the development of a NetLogo agent-based model for CAS. This looks to be a promising approach for modelling the IoT as a CAS using agents.

How can CAS assist in exploring IoT issues and solving challenges? CAS should be able to contribute towards the set of Design Challenges in Table 5. For example, they could provide a better

understanding of emergent IoT behaviors as IoT networks expand in numbers and types of things added (scalability) and have already been applied to networking issues, at least for WSNs. Further, Hernandez-Bravo and Cattero [105] investigated a hierarchical approach to model complexity in IoT and Smart Cities; however this approach had limitations and the authors suggested an alternative approach using semi-lattice structures and reasoning tools.

4.5. Self-Organizing Systems and the IoT

Self-organizing systems are systems that evolve into ordered systems from interactions among components of an initially disordered system. Self-organization concepts date from the 1940s and 1950s when neural networks were first proposed [97]. Scale-free computer networks can be self-organizing. CAS include self-organization as one of their characteristics. Wikipedia is an example of a self-organizing system; there is no central editor and numerous, mainly anonymous contributors [106]. It is continually created and updated with its reference articles tending to become more comprehensive and reliable due to editing. Blogs can also be considered as self-organizing systems [106].

Wenyang and Xue [107] showed how self-organization is needed to organize smart appliances in an IoT application such as a smart home to enhance usability and thus gain consumer support. Object recognition, IoT sensing devices and network integration are all required for such self-organization. Yamamoto et al. [108] described a self-organized system for online shopping. The online system self organizes, adapting to users' needs by monitoring IoT data to analyze user behavior and modify the price and presentation of products and services.

IoT networks will need to be self-organizing [109] so that they can continue to operate as designed. IoT devices must monitor their environment so that when a failure occurs, they can connect to neighboring devices and cooperate, establish communication paths and then recover from local faults to restore normal operations. Challenges include cross layer design for self-organization, heterogeneity in computation and communications of IoT networks, multi-channel radio communications, load balancing, and delay tolerant networking.

4.6. Intelligence and Context Awareness in the IoT

Context-aware computer systems have been an important research challenge for at least 20 years [110], and will become more so for the IoT, which will not only provide information to users but include intelligent processors which will take actions such as monitoring our personal health and fitness and controlling traffic in our cities, which will affect personal, business and community life in major ways. Context-aware computer services are defined as software applications that can operate in a dynamic environment and have the capability to run anytime, anywhere and on any device with minimal user attention. Context is defined as "any information relevant to the interaction of the user with the service, where both the user and the application's environment are of particular interest" [111]. Context awareness is a complex process due to the diversity of sources from which context information is obtained. In conventional services input comes mainly as input from the user and this manually supplied information drives the service execution. Context-aware services, on the other hand, rely on information that arises from a variety of sources, such as sensors, repositories and users. When multiple users are involved, who may have different requirements, problems of conflict may arise [112,113]. Context aware service creation is described in the technical literature as being by means of two complementary approaches, one based on providing a general purpose context infrastructure and the other, termed context modelling, that uses a context model tailored to the services provided [111].

Systems Thinking can contribute to this research challenge via Complex Adaptive Systems Theory, which originated in the study of living organisms. Living organisms are aware of their environment/context in different ways and degrees through information derived by their sensors (sight, hearing, touch, smell, etc.) and conveyed to the brain, which processes this information to

form some sort of model of the context in which they are embedded. In humans, a very sophisticated model of their environment/context, conscious or unconscious, is constructed by poorly understood cognitive processes.

The Soft Systems Thinking approach can also contribute to the research challenge of designing context-aware information systems in the IoT. Most of the literature on context-aware systems is technology focussed, and to deal with the full complexity of context modelling is beyond the scope of this paper. However to clarify some of the issues of context modelling we present an SSM conceptual model of a very simple context-aware application, a home security system. To introduce the idea, Figure 3 is a type of abstract conceptual model [114], which is a set of very general activities which could be tailored to any root definition. In a context-aware system, a service can be provided in different ways, depending on the context. Context modelling defines the alternative ways, and the criteria for selecting which one or more ways will be acted on. As in all correctly constructed SSM conceptual models, activities are needed to monitor the doing and taking control action to try to ensure the meeting of criteria of efficacy (is the system doing what it is supposed to?) and efficiency (is it being done with a minimum use of resources?) [115].

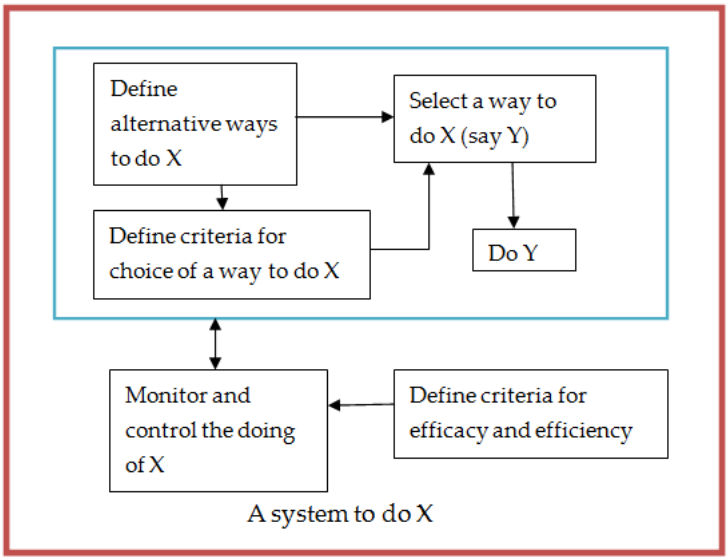

Figure 3. A Soft Systems Methodology (SSM) abstract conceptual model.

In Figure 4 below we present an SSM conceptual model of one of the context aware services in a "smart home" [113]. Our root definition of a simplified "Home Security Service System" is as follows:

> *"A system to provide home security by, when activated, collecting primary security sensor data including entry and exit of people, movements in the property and CCTV images of areas of the property, fusing sensor data, deciding if a security threat is likely, deciding appropriate responses to take to security threats by means of a context model and generated secondary threat data, executing chosen responses, and archiving of sensor and incident data".*

This conceptual model arguably contains the minimum necessary set of activities that are required by the root definition. As discussed by Mingers [114], the root definition specifies "what" is done, and the conceptual model depicts "how" it is done. You will note that various types of information are input to this conceptual model (represented in Figure 4 by heavy arrows) and a "context model" is also used by three of the activities. The input information may be used to determine the context or be required for activities independently of the context. Our root definition does not specify "how" the context model works, but it does specify that a context model will be used to decide "how" the system will respond to security threats. In Figure 4 some options, not specified in the root

definition, are annotated on some activities for understanding only. Also some mathematical logic statements (IF . . . THEN . . . ELSE) are annotated on the context model to clarify how it might work in this application, for understanding only. In the real world (as opposed to the conceptual world of our model) a context model can be a very complex computer program, and can be classed as either an Expert System (which often uses mathematical logic), an Operations Research Model (such as a Multi-Criteria Decision Model or a Discrete-event Simulation Model) or something else. In our illustrative conceptual model the context model is used for three activities:

- Fusion of sensor data;
- Deciding if a security threat is likely; and
- Deciding on appropriate responses to a threat

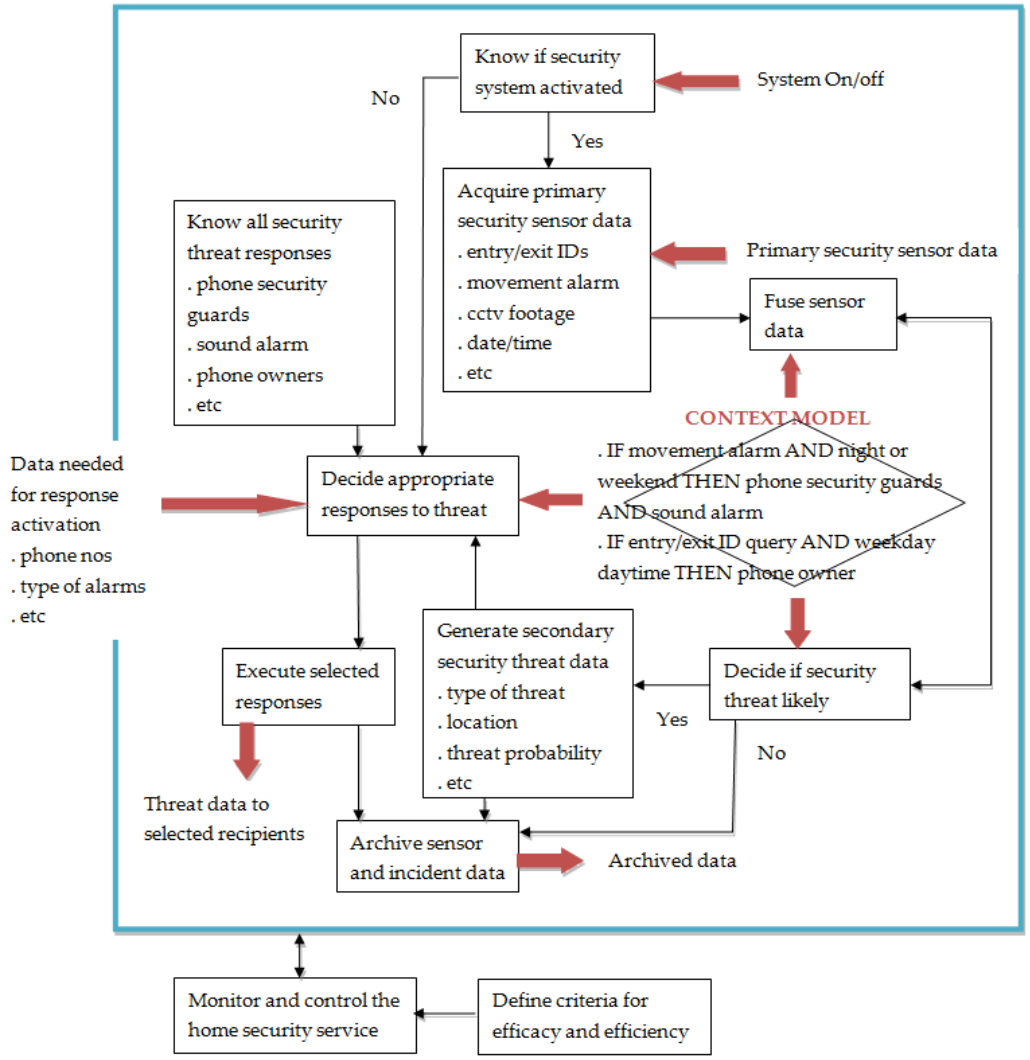

Figure 4. SSM Conceptual Model of a Simplified Home Security Service System.

Fusion of sensor data is, in general, a process that integrates multisource heterogeneous data from multiple sensor measurements in order to improve processing efficiency and provide advanced intelligence [116]. Deciding if a security threat is likely is a process that may use a variety of techniques, usually based on probability theory. Deciding on appropriate responses to a threat is a process that combines the context information deduced from secondary sensor data (in our simple example this includes the security threat probability and location) together with other data needed for responses

to a threat, usually stored on a repository. A comprehensive survey of context-aware computing for the IoT is given by Perera et al. [117]. This covers many technical issues including the categories of context information, primary and secondary context data and context reasoning decision models. We note from the last of these topics that the simplest, most straightforward and most popular method of context reasoning is in terms of rules (which have an IF ... THEN ... ELSE format), as depicted in Figure 4. These technical details are beyond the scope of this paper; our SSM conceptual model is intended to illustrate the feature of SSM of being able to make sense of complex problem situations.

In principle, the root definition could specify the specific nature of the context model, i.e., which of an alternative set of context models is used, or give more detail on "how" any of the activities in the conceptual model are carried out. Wang et al. [116] discuss two main types of data fusion, one using mathematical or computational methods and the other using semantics derived from representations of sensor data and sensor observations. Further, OR techniques such as Bayesian and Dempster-Shafer inference, fuzzy logic and artificial neural networks may be used in the former type of data fusion [56]. These were discussed in Section 3.1.5. However, SSM conceptual models are meant to be compared with the real world, in order to help make sense of, and suggest improvements to, real world complexity, and not necessarily to be an exact map of the real world. Mingers [114] makes a useful distinction between "conceptual hows" and "actual hows". Conceptual hows are not meant to describe actual activities in the real-world, but possibilities that might exist, deriving from a particular "what".

Actual hows refer to that which occurs in the real world, which may be incredibly complex and reflect many and varied whats. He also notes that introducing more conceptual hows to a conceptual model could give rise to a "what/how hierarchy" of more and more detailed conceptual models. Note that these are alternative ways of doing things, models at the same level of resolution, not an expansion to a higher level of resolution, which is done via root definitions of the component activities and their expansion into sets of necessary complementary activities.

The Soft Systems Thinking approach could potentially be used to identify the requirements of context-aware systems, which are often viewed in a very simplistic technical sense in the computing literature [118]. Two main conceptions of context (to be distinguished from the two technical context-aware service creation approaches discussed above) can be distinguished, the representational view and the interactional view. The former defines context as information that can be encoded and represented much like other forms of information (as discussed above for a home security system). Several types of context data model are based on this view [119], as is the context metamodel of Imen et al. [120]. The interactional view of context defines context as an occasioned property arising from the interaction of people, artefacts and groups. An action research study of designing a context-aware application using the interactional view [118] supported the usefulness of this view, while calling for more sophisticated theoretical frameworks that can capture the socio-technical complexity of designing context-aware applications. A comparison of these two views and how they incorporate context into system design is given by Ploesser [121]. An SSM-based approach to information requirements analysis similar to the above is given by Stowell [122].

4.7. IoT Software Development—An Application of System Dynamics

System Dynamics (SD) is a methodology for studying complex dynamic system behavior from a holistic perspective. It was developed by Jay Forrester of MIT to model industrial systems with physical flows (personnel, money, material and machinery), their respective accumulations, and information-based decision-making mechanisms that control the flows to achieve desired accumulation levels [123,124]. Forrester's approach was to model the relationships between the various systems components, express these as differential or difference equations, and then run the model as a computer simulation. Causal-loop diagrams are used to show the dynamic cause and effect relationships between various system variables and the resulting feedback loops.

A feedback loop can generate one of two types of effects, a snowball effect where a change in state generates action that causes a bigger change in the state (a reinforcing, R, loop), or a balancing

effect where a change in state generates action to absorb the change (a balancing, B, loop), as shown in Figure 5. The polarity of a link (±) indicates the direction of change that a change in the cause induces in the effect. A pair of parallel lines on a link indicates a time delay between cause and effect.

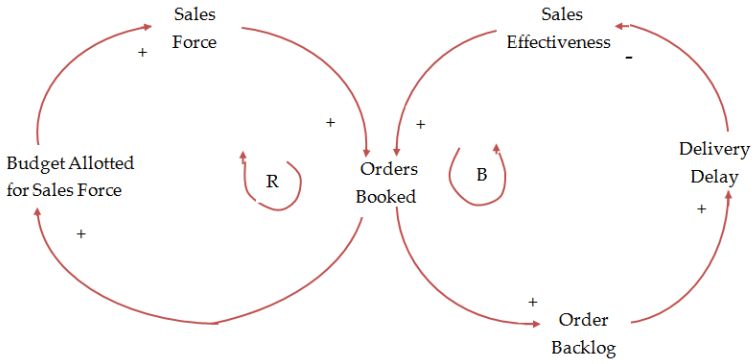

Figure 5. Feedback loops: Reinforcing loop (**left**) and Balancing loop (**right**), (redrawn from Dutta and Roy [123]).

Since its foundation, SD has been applied to a wide range of problems, including supply chain management, project management, IT infrastructure and strategic planning. It has been used to model Internet diffusion [125] and similar use can be expected for modelling industry investment in the IoT (see Section 4.9). Figure 6 shows a causal loop diagram of Internet diffusion in India.

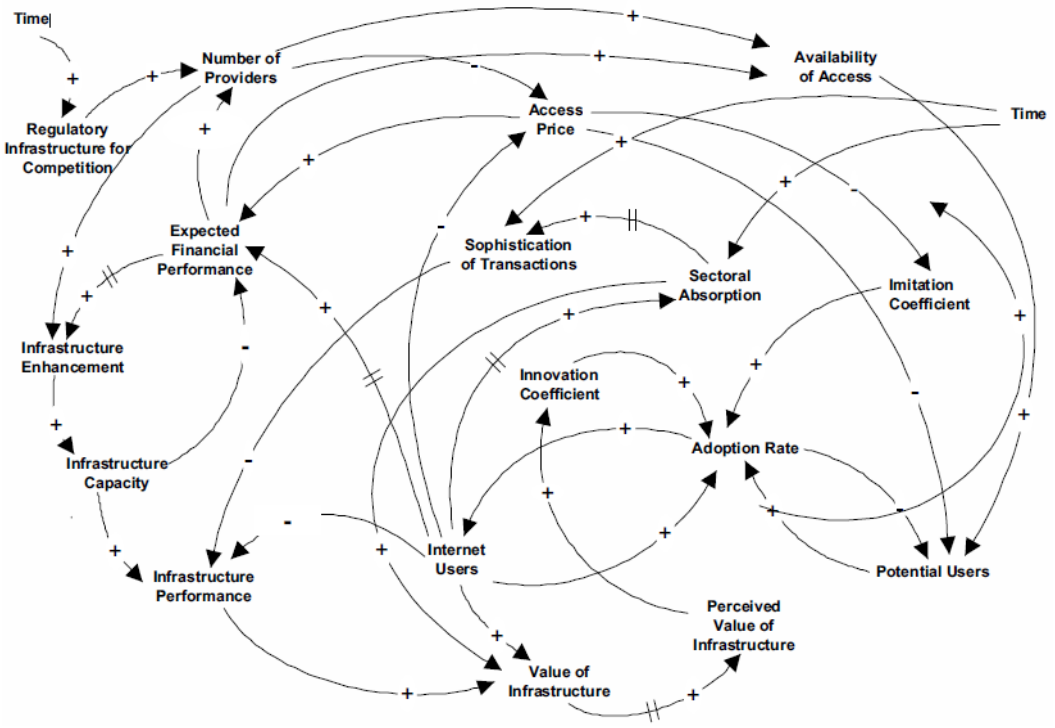

Figure 6. Causal loop diagram of Internet diffusion in India (reproduced with permission from [125]).

As discussed in Section 2.2, the future IoT is envisaged as an ecosystem or system of systems, and SD modelling could be carried out at different levels. The highest level might be the overall IoT core infrastructure, similar to the above Internet diffusion model, below which might be individual application areas such as energy, health care and the smart city. At a lower level, SD could model IoT project management, including software development. Much work has already been

done in SD modelling of the agile software development process [126,127] and software project management [128,129]. Madachy et al. [130] used SD to assess a hybrid plan-driven and agile process, based on a scalable spiral model, to cope with a rapidly changing software environment. In the context of IoT software development, where many systems must interoperate, there is much interest in the relative effectiveness of standards versus Open Source processes [39,131,132]. As discussed in Section 2.3, ISO has developed standards for systems engineering (ISO/IEC 15288), software engineering (ISO/IEC 12207) and project management (ISO 21500). Further lower level standards govern the technical design of the IoT in a layered model, which may be broadly divided into technical, syntactic, semantic and pragmatic categories [131]. New technical developments such as software defined networking [133] can be expected as development of the IoT gathers momentum. There is clearly scope for SD modelling of many aspects of IoT design, development and operations.

The other main role that SD modelling can play is to model the operational use of the IoT's "big data", utilizing intelligent processors. This has been done in the application area of smart transportation in an urban environment [134], which evaluated policies for:

- Real-time train and bus schedules
- Smart traffic signalling
- Smart parking
- Autonomous and cooperative vehicles
- "Uber" vehicle sharing

Another major area for SD modelling is IoT-enabled industrial logistics systems [135,136]. These applications extend Forrester's early work on industrial dynamics to the present day environment of RFID identification of raw materials, work-in-progress and finished products, and the real-time tracking, via IoT sensors, of every stage of the logistics chain.

4.8. IoT Technology Transfer—An Application of SSM

Soft Systems Methodology (SSM) emerged in the 1970s as a response to the inability of traditional OR to deal with complex, ill-structured problem situations in which objectives are not clear or not agreed by all stakeholders. It is a form of action research that uses conceptual models of notional systems ("human activity systems") to learn about, and bring about improvements to, problem situations of all kinds. Although it has been mainly used for management problems within human organizations, it can be used for making sense of complex socio-technical systems such as the IoT. Many books, journal articles and unpublished consultancy reports have been written on SSM. The most up to date account is that of Checkland and Poulter [115]. SSM studies have been reported at Australian Society for Operations Research (ASOR) conferences since 1985, the first being that of Watson and Smith [82]. Its place in the Systems Thinking sub-discipline of OR is now well established.

Adoption, transfer and appropriate use of the IoT infrastructure, and the education of developers, businesses and users is a major "soft" research challenge which needs to be addressed by SDOs. It has been reported on in a European Commission report [137]. Some work on technology transfer in Australia (in the context of remote sensing technology) using SSM has been done by Andrew Finegan [138]. A root definition adapted (and made IoT specific) from his work is as follows:

> *"An industry driven system operating within SDOs with the objective of transferring IoT technology by: knowing about IoT technology and operations, knowing the technical, business and social barriers to acceptance, knowing about targeted industries, selecting IoT technology to be transferred, selecting means of transferring IoT technology, applying those means to targeted industries, stimulating the ongoing transfer, and monitoring the success of such transfers; in order to benefit all involved parties, in an environment of standards, industrial competitiveness, and national and international economic development."*

The CATWOE elements (Customers, Actors, Transformation, World view, Owners, Environment [115]) for this root definition are:

C Industry that can benefit from IoT technology transfer
A SDO researchers who wish to promote IoT technology
T Untransferred IoT technology becomes transferred technology
W Transfer of IoT technology is desirable
O Industry (that has the power to accept or reject transferred IoT technology)
E International SDOs/Industrial Competitiveness/National and International Economies

An SSM conceptual model of this root definition of an "IoT Technology Transfer System" (Figure 7) shows the minimum necessary set of activities to define what the system does at a particular resolution level. The logical expansion of the root definition results in a conceptual model of three subsystems, "knowledge", "criteria" and "application". The activity "monitor and control" remains at the first level of resolution. Criteria for efficacy (is the transformation working?), efficiency (is the transformation being achieved with a minimum use of resources?) and effectiveness (is the transformation achieving the goals of the owner, in this case industry?) are needed for monitoring and controlling this human activity system. This can be compared with perceptions of "what we are doing", by interviewing appropriate people, searching written material with the model in mind, or by some other means.

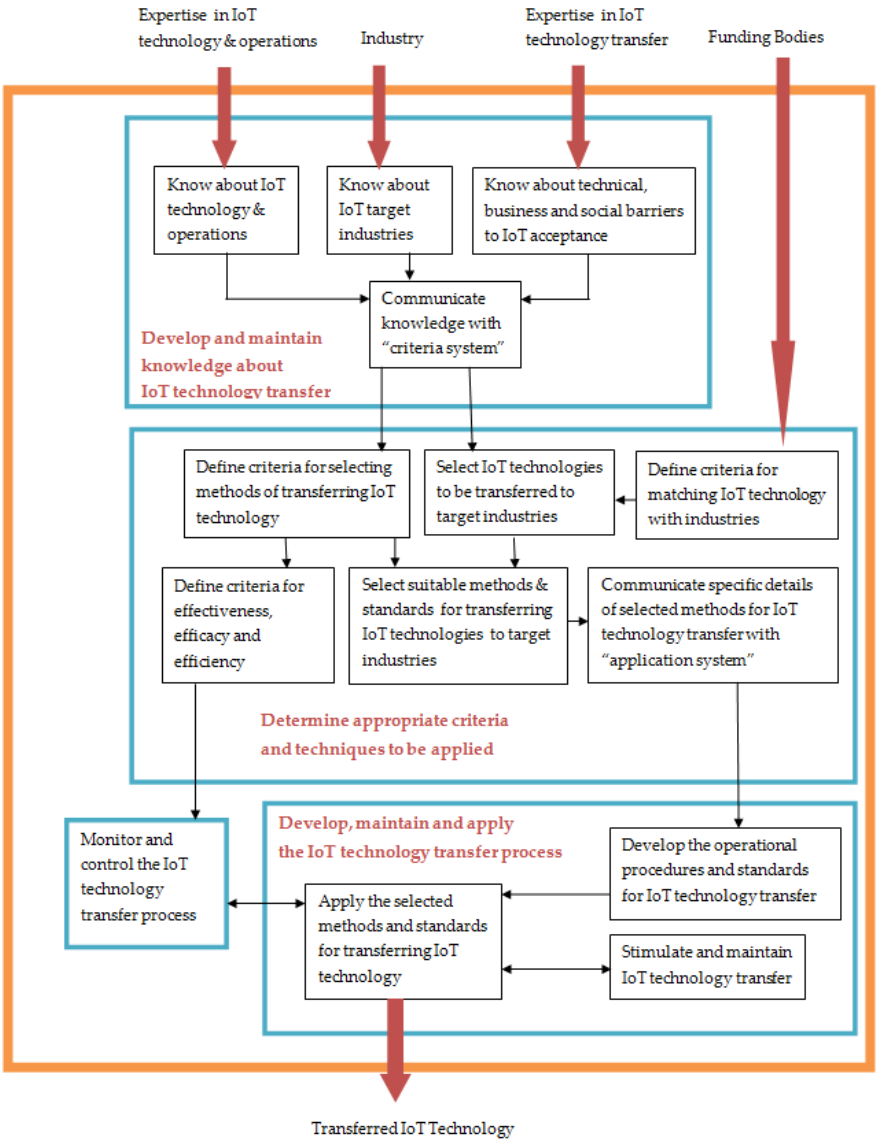

Figure 7. SSM Conceptual Model of an "IoT Technology Transfer System" (adapted from Finegan [138]).

4.9. Industry Investment in IoT—An Application of the Multimethodology Approach

OR support for decisions on industry investment in IoT has been discussed in Section 4.3 in terms of the OR mathematical technique of Game Theory. A case study of the problem of investing in the IoT has also been reported using the OR techniques of agent-based modelling and Data Analytics [71]. Several Systems Thinking approaches can also be applied to this problem situation/research challenge. Thus it is an IoT problem/research challenge which might be best addressed by the Multimethodology approach. In fact, all the IoT research challenges listed in Table 5 need to be tackled by more than one systems approach, i.e., using the Multimethodology approach. In this paper, we only discuss one systems approach for each research challenge to explain that particular approach, but a full systems study would probably use the Multimethodology approach.

Some of the advantages and challenges of using the Multimethodology approach are listed in Gil-Garcia and Pardo [139]. Their study of e-government highlighted the need for better research methods for studying complex socio-technical systems, and the IoT must be one of the most complex systems of this type. Research into the Multimethodology approach has been scarce [140] and the OR/Systems Thinking community must address the need for better education and research in this approach in the future.

The IoT has been described as a System of Systems (SoS) or ecosystem [141], which may be defined as:

> *"A composition of systems in which its constituent systems are individually discovered, selected, and composed possibly at run-time to build a more complex system. The constituent systems are managed (at least in part) for their own purposes rather than the purposes of the whole and maintain a continuing operational existence independent of the collaborative system. The resulting composed system (the SoS) is more complex and offers more functionality and performance than simply the sum of its constituent systems."*

Business investment in the IoT is going to be much more complex than investments in the products and services of an individual firm, and even more complex than currently existing investments in e-commerce over the Internet. New business models for the IoT which view it as a "business ecosystem" will need to be developed. This is *"a complex adaptive system (whose) population develops through co-evolution with the greater environment, self-organization and emergence (i.e., the ability and process to create new order), and adaptation to the environment"* (Peltoniemi [142] quoted in Westerlund et al. [19]). This is shown in Figure 8 below.

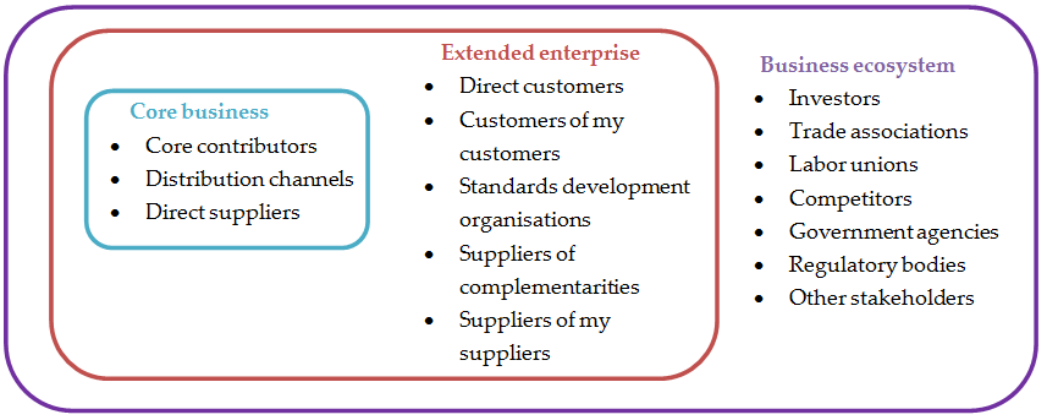

Figure 8. Generic actors in a business ecosystem (redrawn from Mazhelis et al. [18]).

Fleisch [143] provides a useful explanation of how the IoT can add business value to companies. The IoT differs from other information systems in providing high resolution data in real time. This reduces the cost of transferring data from the real world to the virtual world, e.g., RFID tags

eliminate expensive manual stock taking and keying of data into PCs. Fleisch's analysis identified seven ways that the IoT adds business value, including proximity triggers, e.g., self checkout in libraries, automatic sensor triggers, e.g., networked smoke detectors, and automatic product security, e.g., anti-counterfeiting cryptography. It shows that the IoT represents a quantum leap forward from the Internet and has the potential to become a tool that advances the entire discipline of how to manage organizations and complex systems.

Another Systems Thinking approach, System Dynamics (SD), has also been applied to industry investment in new technology, in particular the diffusion of the Internet in India and China [125]. In principle, industry investment in the IoT could be modeled in a similar way. As these authors discuss, SD can represent quantifiable as well as "soft" variables, which is useful since the diffusion context has both social and technical aspects. As discussed in Section 4.7, the basic premise in SD is that system behavior results from interaction among its feedback loops. Various standard feedback loops or archetypes have been identified, including "Fixes that Fail" and "Shifting the Burden" [144]. The dominant structure in Internet diffusion was found to be the Contagion Effect: innovators start the adoption process and then, by a communication process—the contagion effect—spread the word to the remaining population and the adoption process gradually gets taken over by imitators. Ultimately there are no new customers left, and the adoption tapers off, resulting in market saturation. There are also negative feedback effects on adoption, such as concerns about security issues, and the dynamics of Internet, and IoT, diffusion depends on the balance between these opposing feedback loop structures.

5. Conclusions

This paper gives a brief overview of the Internet of Things (IoT), research challenges to its design, use and widespread adoption, and the important contemporary worldwide efforts to develop interoperability standards. The aim of the paper is to survey the application of Operations Research (OR) methods, including the OR sub-discipline of Systems Thinking, to the IoT. The methods were subdivided into "hard" OR tools and techniques, which mainly address the technical and business challenges of the IoT, and Systems Thinking approaches, which can address both technical, business and non-technical challenges, including social, legal and ethical challenges. The research for the paper included review of a very large number of journal articles, conference papers and industry reports on the IoT, the numbers of which are rapidly increasing as the IoT has become a popular area for academic research and business investment. Most of this work is theoretical and few case studies have been reported. Reports on the application of OR and Systems Thinking to the IoT have so far been relatively scarce, although their numbers can be expected to increase in future years. Nevertheless, we were surprised at the amount of work on OR applied to the IoT that is out there, so far mainly in conference papers. The OR journals have been slower to report this application area, although many papers on the adoption of new technology in general have appeared in recent years.

Our review has shown that OR techniques are starting to be applied to some of the major research challenges of the IoT, particularly that of Data Management, where the OR sub-discipline of Data Analytics is developing new approaches to the analysis of "big data" and has become a field whose skills are much in demand by business. The challenge of developing business models for investing in the IoT is also seeing a significant amount of work done by OR practitioners in the field of Decision Analysis, including Game Theory, Analytical Hierarchy Process (AHP) and Data Envelopment Analysis (DEA). The more Information and Communications Technology (ICT)-oriented challenges of the IoT such as network architecture have not attracted as much OR attention as yet, although the OR techniques of Routing and Graph Theory have much potential for contributing to the solution of such problems. Few case studies which attempt to evaluate the efficiency and effectiveness of the IoT have been reported, partly due to its complexity and partly due to the lack of real-world data with which to evaluate such performance measures as return-on-investment (Houston et al. [71]).

In this paper we discuss some selected research challenges and applicable OR methods in greater depth—the breadth of topics in the paper precluded doing so for all research challenges and OR methods. Of the "hard" OR methods the topics selected were: the application of Simulation to the

challenge of Scalability, the application of Reliability Theory to the challenge of Robustness and the application of Game Theory to the challenge of industry investment in the IoT. Of the Systems Thinking methods the topics selected were General Systems and Complexity theory, Self-organizing Systems theory, the application of Soft Systems Methodology (SSM) to Intelligence and Context Awareness, the application of System Dynamics (SD) to Internet/IoT Diffusion and Software Engineering, the application of SSM to Technology Transfer and the application of Multimethodology to industry investment in the IoT.

Systems Thinking approaches such as General Systems Theory (GST) and Complexity Theory are, we believe, of great importance for improving (not "solving") some of the technical and non-technical problems of the IoT, and an increasing amount of work is being done by the systems thinking community, as published in such new journals as *International Journal of Information Technologies and Systems Approach*, and *Systems*.

The IoT is best viewed as a Complex Adaptive System (CAS) and will require new forms of Systems Engineering, Software Engineering, Project Management and other disciplines to develop and manage it in the years ahead. The SD approach has great potential for solving several of the research challenges of the IoT. The main strength of the SSM approach is its support to learning about, and making sense of, complex problem situations, i.e., its epistemological framework. The systems approach termed Multimethodology can potentially be applied to many IoT research challenges, as they require a mix of several "hard" and "soft" techniques. The global IoT business ecosystem includes so many businesses, technologies, governments, legal systems and cultures, and is changing so fast, that the vision of the early founders of OR as being "the search for an overall balance between multiple, changing, conflicting, partly incommensurable and partly immeasurable or intangible objectives, as distinguished from a notion of optimality that aims at maximizing or minimizing the quantitative value of an objective function" (Ulrich [84]) is sorely needed in this field.

Acknowledgments: No grants were provided for this work. The research was done in the authors' own time out of interest in the topic. One of the authors is an Honorary Research Fellow at the Australian Defence Science and Technology Group (DSTG) and some research was carried out within that organization. The authors wish to acknowledge support from the DSTG research library system (PJR) and the University of Melbourne research library (RBW). They are grateful to Professor Hussein Abbass and the anonymous *Systems* reviewers for their helpful comments on improving it.

Author Contributions: PJR and RBW jointly conceived the research topic. R.W.'s contribution was focussed on the Soft Systems area of OR while P.R.'s contribution focussed on the hard OR techniques and their potential to address challenges provided by the emerging Internet of Things.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mortenson, M.J.; Doherty, N.F.; Robinson, S. Operational research from Taylorism to Terabytes: A research agenda for the analytics age. *Eur. J. Oper. Res.* **2015**, *241*, 583–595. [CrossRef]
2. Mingers, J.; White, L. A review of the recent contribution of systems thinking to operational research and management science. *Eur. J. Oper. Res.* **2010**, *207*, 1147–1161. [CrossRef]
3. IEEE. P2413—Standard for an Architectural Framework for the Internet of Things (IoT). 2016. Available online: https://standards.ieee.org/develop/project/2413.html (accessed on 12 March 2017).
4. Borgia, E. The Internet of Things vision: Key features, applications and open issues. *Comput. Commun.* **2014**, *54*, 1–31. [CrossRef]
5. Jain, R. Internet of Things: Challenges and Issues. In Proceedings of the 20th Annual Conference on Advanced Computing and Communications (ADCOM 2014), Bangalore, India, 19–22 September 2014.
6. Stankovic, J.A. Research directions for the internet of things. *IEEE Internet Things J.* **2014**, *1*, 3–9. [CrossRef]
7. Mattern, F.; Floerkemeier, C. From the Internet of Computers to the Internet of Things. In *From Active Data Management to Event-Based Systems and More*; Springer: Berlin, Germany, 2010; pp. 242–259.
8. Elkhodr, M.; Shahrestani, S.; Cheung, H. The Internet of Things: Vision & Challenges. In Proceedings of the TENCON Spring Conference, Sydney, Australia, 17–19 April 2013; pp. 218–222.
9. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]

10. Chen, S.; Xu, H.; Liu, D.; Hu, B.; Wang, H. A vision of IoT: Applications, challenges, and opportunities with China perspective. *IEEE Internet Things J.* **2014**, *1*, 349–359. [CrossRef]
11. Muralidharan, S.; Roy, A.; Saxena, N. An Exhaustive Review on Internet of Things from Korea's Perspective. *Wirel. Pers. Commun.* **2016**, *90*, 1463–1486. [CrossRef]
12. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
13. Borgia, E. Special Issue on Ïnternet of Things: Research Challenges and Solutions (editorial). *Comput. Commun.* **2016**, *89*, 1–4. [CrossRef]
14. Fraga-Lamas, P.; Fernandez-Carames, T.M.; Suarez-Albela, M.; Castedo, L.; Gonzalez-Lopez, M. A review on internet of things for defense and public safety. *Sensors* **2016**, *16*, 1644. [CrossRef] [PubMed]
15. Dijkman, R.M.; Sprenkels, B.; Peeters, T.; Janssen, A. Business models for the Internet of Things. *Int. J. Inf. Manag.* **2015**, *35*, 672–678. [CrossRef]
16. Kim, S.; Kim, S. A multi-criteria approach toward discovering killer IoT application in Korea. *Technol. Forecast. Soc. Chang.* **2016**, *102*, 143–155. [CrossRef]
17. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Bus. Horiz.* **2015**, *58*, 431–440. [CrossRef]
18. Mazhelis, O.; Luoma, E.; Warma, H. Defining an internet-of-things ecosystem. In *Internet of Things, Smart Spaces, and Next Generation Networking*; Springer: Berlin, Germany, 2012; pp. 1–14.
19. Westerlund, M.; Leminen, S.; Rajahonka, M. Designing business models for the internet of things. *Technol. Innov. Manag. Rev.* **2014**, *4*, 5.
20. Mishra, D.; Gunasekaran, A.; Childe, S.J.; Papadopoulos, T.; Dubey, R.; Wamba, S. Vision, applications and future challenges of Internet of Things: A bibliometric study of the recent literature. *Ind. Manag. Data Syst.* **2016**, *116*, 1331–1355. [CrossRef]
21. UK Technology Strategy Board (TSB). *A Roadmap for Interdisciplinary Research on the Internet of Things*; Internet of Things Special Interest Group: London, UK, 2012.
22. Dutton, W.H.; Capra, L.; Ciaraldi, M.; Evans, D.; Furness, A.; Graham, I.; Jirotka, M.; Kupai, A.; Maguire, M.; Matthews, N.; et al. *A Roadmap for Interdisciplinary Research on the Internet of Things: Social Sciences*; Internet of Things Special Interest Group, Technology Strategy Board: London, UK, 2013.
23. Innovate UK. *IoT Special Interest Group, Internet of Things (IoT) and Machine to Machine Communications (M2M) Challenges and Opportunities*; Innovate UK: London, UK, 2013.
24. Rose, K.; Eldridge, S.; Chapin, L. The internet of things: An overview. In *Understanding the Issues and Challenges of a More Connected World*; The Internet Society (ISOC): Washington, DC, USA, 2015; pp. 1–50.
25. Dutton, W. Putting Things to Work: Social and Policy Challenges for the Internet of Things. In *Internet of Things Meetup*; Culham Science Centre, Culham: Abingdon, UK, 2014.
26. Dutton, W.H. The Internet of Things. Oxford Institute, 2013. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2324902 (accessed on 12 March 2017).
27. European Research Cluster on the Internet of Things (IERC). Available online: http://www.internet-of-things-research.eu/documents.htm (accessed on 12 March 2017).
28. Ishaq, I.; Carels, D.; Teklemariam, G.K.; Hoebeke, J.; Van den Abeele, F.; De Poorter, E.; Moerman, I.; Demeester, P. IETF Standardization in the field of the internet of things (IoT): A survey. *J. Sens. Actuator Netw.* **2013**, *2*, 235–287. [CrossRef]
29. Internet Society. Internet of Things: Standards and Guidance from the IETF. 2016. Available online: https://www.internetsociety.org/publications/ietf-journal-april-2016/internet-things-standards-and-guidance-ietf (accessed on 12 March 2017).
30. ISO/IEC JTC1. Resolutions Adopted at the 28th Meeting of ISO/IEC JTC1 (N11894). In *ISO/IEC JTC1 Plenary*; ISO/IEC: Perros-Guirec, France, 2013.
31. ISO/IEC JTC1. *Internet of Things Preliminary Report (2014)*; ISO/IEC: Geneva, Switzerland, 2014.
32. ISO/IEC JTC1. *ISO/IEC JTC1 N13119 Text of CD 30141 Information Technology*; ISO/IEC: Geneva, Switzerland, 2016.
33. ISO/IEC JTC1. Resolutions Adopted at the 31st Meeting of ISO/IEC JTC1 (N13270). In *ISO/IEC JTC1 Plenary*; ISO/IEC: Lillehammer, Norway, 2016.
34. IEEE. IEEE Internet of Things. 2016. Available online: http://iot.ieee.org/ (accessed on 12 March 2017).

35. ITU. Internet of Things Global Standards Initiative. 2016. Available online: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (accessed on 12 March 2017).
36. Gustavsson, P.; Serbinski, M. The Internet of Things and the Future of M&S—Where are We Going and What are the Opportunities? In Proceedings of the 2015 Fall Simulation Interoperability Workshop, Orlando, FL, USA, 31 August–4 September 2015.
37. Lessman, K.; Riecken, M.; O'Connor, M.J. Modeling & Simulation of the Internet of Things and Cyber Physical Systems for Cybersecurity. In Proceedings of the Simulation Innovation Workshop, Orlando, FL, USA, 11–16 September 2016.
38. Kondepudi, S. IOT Standards Wars. In *Forum on Internet of Things: Empowering the New Urban Agenda*; ITU: Geneva, Switzerland, 2015.
39. Brown, B.R. What the Internet of Things Needs: Systems Engineering. *International Council on Systems Engineering News*. 2016. Available online: http://www.ecnmag.com/blog/2016/04/what-internet-things-needs-systems-engineering (accessed on 11 March 2017).
40. Kljajić, M.; Farr, J.V. Chapter 4: Importance of Systems Engineering in the Development of Information Systems. In *Emerging Systems Approaches in Information Technologies*; Paradice, D., Ed.; Information Science Reference (an Imprint of IGI Global): New York, NY, USA, 2010.
41. O'Connor, R.V.; Laporte, C.Y. The Evolution of the ISO/IEC 29110 Set of Standards and Guides. *Int. J. Inf. Technol. Syst. Approach* **2017**, *10*, 1–21. [CrossRef]
42. White, B. A complex adaptive systems engineering (CASE) methodology—The ten-year update. In Proceedings of the 2016 Annual IEEE Systems Conference (SysCon), Orlando, FL, USA, 18–21 April 2016; pp. 1–8.
43. Xue, R.; Baron, C.; Esteban, P.; Sahraoui, A. Aligning systems engineering and project management standards to improve the management of processes. In *Progress in Systems Engineering*; Springer: Heidelberg, Germany, 2015; pp. 547–553.
44. Daellenbach, H.G.; Flood, R.L. *The Informed Student Guide to Management Science*; Thomson Learning: London, UK, 2002.
45. Cooper, J.; James, A. Challenges for database management in the internet of things. *IETE Tech. Rev.* **2009**, *26*, 320–329. [CrossRef]
46. Ma, M.; Wang, P.; Chu, C.H. Data Management for Internet of Things: Challenges, Approaches and Opportunities. In Proceedings of the Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, Beijing, China, 20–23 August 2013; pp. 1144–1151.
47. Petkov, D.; Petkova, O.; Andrews, T.; Nepal, T. Mixing multiple criteria decision making with soft systems thinking techniques for decision support in complex situations. *Decis. Support Syst.* **2007**, *43*, 1615–1629. [CrossRef]
48. Haghighi, M.; Maraslis, K.; Tryfonas, T.; Oikonomou, G.; Burrows, A.; Woznowski, P.; Piechocki, R. Game Theoretic approach towards Optimal Multi-tasking and Data-distribution in IoT. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 406–411.
49. Wang, J.; Liao, J.; Li, T.; Wang, J. Game-theoretic model of asymmetrical multipath selection in pervasive computing environment. *Pervasive Mob. Comput.* **2016**, *27*, 37–57. [CrossRef]
50. Brandenburger, A.M.; Nalebuff, B.J. The right game: Use game theory to shape strategy. *Harvard Bus. Rev.* **1995**, *73*, 57–71.
51. Dyk, M.; Najgebauer, A.; Pierzchala, D. SenseSim: An agent-based and discrete event simulator for Wireless Sensor Networks and the Internet of Things. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 345–350.
52. Musznicki, B.; Zwierzykowski, P. Survey of simulators for wireless sensor networks. *Int. J. Grid Distrib. Comput.* **2012**, *5*, 23–50.
53. Wightman, P.M.; Labrador, M.A. Atarraya: A simulation tool to teach and research topology control algorithms for wireless sensor networks. In Proceedings of the 2nd International Conference on Simulation Tools and Techniques, Rome, Italy, 2–6 March 2009.
54. Korkalainen, M.; Sallinen, M.; Karkkainen, N.; Tukeva, P. Survey of Wireless Sensor Networks Simulation Tools for Demanding Applications. In Proceedings of the 2009 Fifth International Conference on Networking and Services, Valencia, Spain, 20–25 April 2009.

55. Ribeiro, R.A.; Falcao, A.; Mora, A.; Fonseca, J.M. FIF: A fuzzy information fusion algorithm based on multi-criteria decision making. *Knowl.-Based Syst.* **2014**, *58*, 23–32. [CrossRef]
56. Nakamura, E.F.; Loureiro, A.A.; Frery, A.C. Information fusion for wireless sensor networks: Methods, models, and classifications. *ACM Comput. Surv.* **2007**, *39*, 9. [CrossRef]
57. De Coninck, E.; Verbelen, T.; Vankeirsbilck, B.; Bohez, S.; Simoens, P.; Demeester, P.; Dhoedt, B. Distributed neural networks for Internet of Things: The Big-Little approach. In Proceedings of the 2nd EAI International Conference on Software Defined Wireless Networks and Cognitive Technologies for IoT, Rome, Italy, 26–27 October 2015; pp. 1–9.
58. Chen, D.; Chang, G.; Sun, D.; Li, J.; Jia, J.; Wang, X. TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Comput. Sci. Inf. Syst.* **2011**, *8*, 1207–1228. [CrossRef]
59. Dhumane, A.; Prasad, R.; Prasad, J. Routing Issues in Internet of Things: A Survey. In Proceedings of the International MultiConference of Engineers and Computer Scientists, Hong Kong, China, 16–18 March 2016; pp. 16–18.
60. Yong-Fei, L.; Li-Qin, T. Comprehensive evaluation method of Reliability of Internet of Things. In Proceedings of the 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Guangzhou, China, 8–10 November 2014; pp. 262–266.
61. Mneimneh, S. *Computer Networks A Gentle Introduction to Queuing Theory*; Hunter College of CUNY: New York, NY, USA, 2013.
62. Mahamure, S.; Railkar, P.N.; Mahall, N. Communication Protocol and Queueing Theory-based Modelling for the Internet of Things. *J. ICT* **2016**, *3*, 157–176.
63. Euler, L. Leonhard Euler and the Königsberg bridges. *Sci. Am.* **1953**, *189*, 66–70. [CrossRef]
64. Yao, B.; Liu, X.; Zhang, W.; Chen, X.; Zhang, X.; Yao, M.; Zhao, Z. Applying Graph theory to the Internet of Things. In Proceedings of the 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, Zhangjiajie, China, 13–15 November 2013.
65. Pirzada, S. Applications of graph theory. *PAMM* **2007**, *7*, 2070013. [CrossRef]
66. Shirinivas, S.; Vetrivel, S.; Elango, N. Applications of graph theory in computer science an overview. *Int. J. Eng. Sci. Technol.* **2010**, *2*, 4610–4621.
67. Holland, J.H. Adaptation in natural and artificial systems. In *An Introductory Analysis with Application to Biology, Control, and Artificial Intelligence*; University of Michigan Press: Ann Arbor, MI, USA, 1975.
68. Esmaeili, M.; Jamali, S. A Survey: Optimization of Energy Consumption by using the Genetic Algorithm in WSN based Internet of Things. *Wirel. Commun.* **2016**, *8*, 65–73.
69. Singh, K.; Aggarwal, A. Survey on Optimization Techniques of RFID for Internet of Things. *Int. J. Comput. Appl.* **2016**, *148*, 9. [CrossRef]
70. Fortino, G.; Russo, W.; Savaglio, C. Simulation of Agent-oriented Internet of Things Systems. In Proceedings of the 17th Workshop" From Objects to Agents, Catania, Italy, 29–30 July 2016.
71. Houston, C.; Gooberman-Hill, S.; Mathie, R.; Kennedy, A.; Li, Y.; Baiz, P. Case Study for the Return on Investment of Internet of Things Using Agent-Based Modelling and Data Science. *Systems* **2017**, *5*, 4. [CrossRef]
72. Jackson, M.C.; Keys, P. Towards a system of systems methodologies. *J. Oper. Res. Soc.* **1984**, *35*, 473–486. [CrossRef]
73. Von Bertalanffy, L. General Systems Theory: Foundations, Development, Applications. *JAMA* **1968**, *208*, 870.
74. Courtney, J.; Merali, Y.; Paradice, D.; Wynn, E. On the study of complexity in information systems. *Int. J. Inf. Technol. Syst. Approach* **2008**. [CrossRef]
75. Holland, J.H. *Hidden Order: How Adaptation Builds Complexity*; Basic Books: New York, NY, USA, 1995.
76. Bar-Yam, Y. *Dynamics of Complex Systems*; Addison-Wesley: Reading, MA, USA, 1997.
77. Banzhaf, W. Self-organizing Systems. In *Encyclopedia of Complexity and Systems Science*; Springer: Heidelberg, Germany, 2009; pp. 8040–8050.
78. Ashby, W.R. Principles of the self-organizing dynamic system. *J. Gener. Psychol.* **1947**, *37*, 125–128. [CrossRef] [PubMed]
79. Mingers, J. *Self-Producing Systems: Implications and Applications of Autopoiesis*; Springer Science & Business Media: New York, NY, USA, 1994.
80. Wiener, N. *Cybernetics*; Hermann: Paris, France, 1948.

81. Beer, S. The viable system model: Its provenance, development, methodology and pathology. *J. Oper. Res. Soc.* **1984**, *35*, 7–25. [CrossRef]
82. Watson, R.B.; Smith, R. A Macro Analysis of the RAAF Logistics System. In Proceedings of the Australian Society for Operations Research 7th National Conference, Adelaide, Australia, 26–28th August 1985.
83. Watson, R.B. Suggestions for new application areas for soft systems methodology in the information age. *Syst. Pract. Action Res.* **2012**, *25*, 441–456. [CrossRef]
84. Ulrich, W. Operational research and critical systems thinking—an integrated perspective Part 1: OR as applied systems thinking. *J. Oper. Res. Soc.* **2012**, *63*, 1228–1247. [CrossRef]
85. Mingers, J.; Brocklesby, J. Multimethodology: Towards a framework for mixing methodologies. *Omega* **1997**, *25*, 489–509. [CrossRef]
86. Howick, S.; Ackermann, F. Mixing OR methods in practice: Past, present and future directions. *Eur. J. Oper. Res.* **2011**, *215*, 503–511. [CrossRef]
87. D'Angelo, G.; Ferretti, S.; Ghini, V. Simulation of the Internet of Things. In Proceedings of the IEEE 2016 International Conference on High Performance Computing and Simulation (HPCS 2016), Innsbruck, Austria, 18–22 July 2016.
88. D'Angelo, G.; Ferretti, S.; Ghini, V. Multi-level simulation of Internet of Things on smart territories. *Simul. Model. Pract. Theory* **2016**. [CrossRef]
89. Zola, E.; Martin-Escanola, I.; Barcelo-Arroyo, F. Discrete Event Simulation of Wireless Cellular Networks. In *Discrete Event Simulations*; Goti, A., Ed.; InTech: Vienna, Austria, 2010.
90. Kempf, J.; Arkko, J.; Beheshti, N.; Yedavalli, K. Thoughts on reliability in the internet of things. In Proceedings of the Interconnecting Smart Objects with the Internet Workshop, Prague, Czech, 25–26 March 2011; pp. 1–4.
91. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 13–17 August 2012.
92. Madsen, H.; Burtschy, B.; Albeanu, G.; Popentiu-Vladicescu, F. Reliability in the utility computing era: Towards reliable fog computing. In Proceedings of the 2013 20th International Conference on Systems, Signals and Image Processing (IWSSIP), Bucharest, Romania, 7–9 July 2013.
93. Niyato, D.; Lu, X.; Wang, P.; Kim, D.I.; Han, Z. Economics of Internet of Things: An information market approach. *IEEE Wirel. Commun.* **2016**, *23*, 136–145. [CrossRef]
94. Turk, M. Internet of Things: Are We There Yet? (The 2016 IoT Landscape). 2016. Available online: http://mattturck.com/2016/03/28/2016-iot-landscape/ (accessed on 12 March 2017).
95. Lee, K.-H.; Baldick, R. Solving three-player games by the matrix approach with application to an electric power market. *IEEE Trans. Power Syst.* **2003**, *18*, 1573–1580.
96. Mitleton-Kelly, E. Ten principles of complexity and enabling infrastructures. In *Complex Systems and Evolutionary Perspectives on Organisations: The Application of Complexity Theory to Organisations*; Elsevier Science: Oxford, UK, 2003; pp. 23–50.
97. Anish, S.; Gupta, A. Insights from Complexity Theory: Understanding Organizations Better. ISSUES 2010. Available online: http://tejas.iimb.ac.in/articles/12.php (accessed on 11 March 2017).
98. Chan, S. Complex adaptive systems. In *ESD. 83 Research Seminar in Engineering Systems*; MIT: Cambridge, MA, USA, 2001.
99. Rupert, M.; Hassas, S.; Rattrout, A. The web and complex adaptive systems. In Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06), Vienna, Austria, 18–20 April 2006; pp. 200–204.
100. Grisogono, A.-M.; Ryan, A. Designing complex adaptive systems for defence. In Proceedings of the Systems Engineering Test and Evaluation Conference, Canberra, Australia, 27–29 October 2003.
101. Ryan, A.; Grisogono, A.-M. Hybrid complex adaptive engineered systems: A case study in defence. In Proceedings of the International Conference on Complex Systems, Boston, MA, USA, 16–21 May 2004.
102. Yan, C.; Ji-Hong, Q. Application analysis of complex adaptive systems for WSN. In Proceedings of the 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), Taiyuan, China, 22–24 October 2010.
103. Haghnevis, M.; Askin, R.G. A modeling framework for engineered complex adaptive systems. *IEEE Syst. J.* **2012**, *6*, 520–530. [CrossRef]

104. Batool, K.; Niazi, M.A.; Sadik, S.; Shakil, A.R.R. Towards modeling complex wireless sensor networks using agents and networks: A systematic approach. In Proceedings of the TENCON 2014 IEEE Region 10 Conference, Bangkok, Thailand, 22–25 October 2014; pp. 1–6.
105. Hernandez-Bravo, A.; Carretero, J. Approach to manage Complexity in Internet of Things. *Procedia Comput. Sci.* **2014**, *36*, 210–217. [CrossRef]
106. Andrus, D.C. The wiki and the blog: Toward a complex adaptive intelligence community. *Stud. Intell.* **2005**, *49*, 3.
107. Liu, W.; Li, X. A study of the application of self-organizing networks in designing appliances of Internet of Things. In Proceedings of the 2013 3rd International Conference on Consumer Electronics, Communications and Networks (CECNet), Xianning, China, 20–22 November 2013; pp. 45–48.
108. Yamamoto, Y.; Kawabe, T.; Tsuruta, S.; Damiani, E.; Yoshitaka, A.; Mizuno, Y.; Knauf, R. Towards Self-Organizing Internet of Things-Aware Systems for Online Sales. In Proceedings of the 2015 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Bangkok, Thailand, 23–27 November 2015; pp. 208–215.
109. Athreya, A.P.; Tague, P. Network self-organization in the internet of things. In Proceedings of the 2013 10th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), New Orleans, LA, USA, 24–27 June 2013.
110. Hong, J.-Y.; Suh, E.-H.; Kim, S.-J. Context-aware systems: A literature review and classification. *Expert Syst. Appl.* **2009**, *36*, 8509–8522. [CrossRef]
111. Achilleos, A.; Yang, K.; Georgalas, N. Context modelling and a context-aware framework for pervasive service creation: A model-driven approach. *Pervasive Mob. Comput.* **2010**, *6*, 281–296. [CrossRef]
112. Jameson, A. Modelling both the Context and the User. *Pers. Ubiquitous Comput.* **2001**, *5*, 29–33. [CrossRef]
113. Baek, S.; Lee, H.; Lim, S.; Huh, J. Managing mechanism for service compatibility and interaction issues in context-aware ubiquitous home. *IEEE Trans. Consum. Electron.* **2005**, *51*, 524–528. [CrossRef]
114. Mingers, J. The what/how distinction and conceptual models: A reappraisal. *J. Appl. Syst. Anal.* **1990**, *17*, 21–28.
115. Checkland, P.; Poulter, J. *Learning for Action: A Short Definitive Account of Soft Systems Methodology and Its Use, for Practitioners, Teachers and Students*; John Wiley and Sons Ltd.: Chichester, UK, 2006.
116. Wang, F.; Hu, L.; Hu, J.; Zhou, J.; Zhou, K. Recent Advances in the Internet of Things: Multiple Perspectives. *IETE Tech. Rev.* **2016**. [CrossRef]
117. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Context aware computing for the internet of things: A survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 414–454. [CrossRef]
118. Olsson, C.M.; Henfridsson, O. Designing context-aware interaction: An action research study. In *Designing Ubiquitous Information Environments: Socio-Technical Issues and Challenges*; Springer: Boston, MA, USA, 2005; pp. 233–247.
119. Strang, T.; Linnhoff-Popien, C. A context modeling survey. In Proceedings of the Workshop Proceedings, Nottingham, UK, 22–23 January 2004.
120. Imen, J.; Raoudha, B.D.; Hanene, B.A. Proposal for a Generic Context Metamodel. *World Acad. Sci. Eng. Technol. Int. J. Comput. Electr. Autom. Control Inf. Eng.* **2015**, *8*, 408–414.
121. Ploesser, K. A Design Theory for Context-Aware Information Systems. Ph.D. Thesis, School of Information Systems, Science & Engineering Faculty, Queensland University of Technology, Brisbane, Australia, 2013; p. 302.
122. Stowell, F. Towards client-led development of information systems. *Inf. Syst. J.* **1991**, *1*, 173–189. [CrossRef]
123. Dutta, A.; Roy, R. System Dynamics Tutorial provides a primer on a set of tools and techniques aimed at improving decision-making in integrated value chain. *OR MS TODAY* **2002**, *29*, 30–35.
124. Forrester, J.W. System dynamics—a personal view of the first fifty years. *Syst. Dyn. Rev.* **2007**, *23*, 345–358. [CrossRef]
125. Dutta, A.; Roy, R. Internet diffusion in India and China-comparison based on feedback loop dominance. In Proceedings of the 37th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 5–8 January 2004; p. 10.
126. Cao, L.; Ramesh, B.; Abdel-Hamid, T. Modeling dynamics in agile software development. *ACM Tran. Manag. Inf. Syst.* **2010**, *1*, 5. [CrossRef]

127. White, A. An Agile Project System Dynamics Simulation Model. *Int. J. Inf. Technol. Syst. Approach* **2014**, *7*, 55–79. [CrossRef]
128. Lyneis, J.M.; Ford, D.N. System dynamics applied to project management: A survey, assessment, and directions for future research. *Syst. Dyn. Rev.* **2007**, *23*, 157–189. [CrossRef]
129. Kljajić, M.; Borstnar, M.K.; Skraba, A.; Kofjac, D. System approach to MIS and DSS and its modeling within SD. *Res. Methodol. Innov. Philos. Softw. Syst. Eng. Inf. Syst.* **2012**. [CrossRef]
130. Madachy, R.; Boehm, B.; Lane, J.A. Assessing hybrid incremental processes for SISOS development. *Softw. Process Improv. Pract.* **2007**, *12*, 461–473. [CrossRef]
131. Milojicic, D.; Nikolich, P.; Leiba, B. *Standards for Tomorrow: The Internet of Things (Ubiquity symposium)*; Ubiquity: Copenhagen, Denmark, 2015; p. 1.
132. Cowling, J.A.; Ivins, W.K. Assessing the Potential Improvement an Open Systems Development Perspective Could Offer to the Software Evolution Paradigm. *Int. J. Inf. Technol. Syst. Approach* **2016**, *9*, 68–87. [CrossRef]
133. Sood, K.; Yu, S.; Xiang, Y. Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review. *IEEE Internet Things J.* **2016**, *3*, 453–463. [CrossRef]
134. Marshall, P. System dynamics modeling of the impact of Internet-of-Things on intelligent urban transportation. In Proceedings of the 2015 Regional Conference of the International Telecommunications Society (ITS), Los Angeles, CA, USA, 25–28 October 2015.
135. Qu, T.; Thurer, M.; Wang, J.; Wang, Z.; Fu, H.; Li, C.; Huang, G.Q. System dynamics analysis for an Internet-of-Things-enabled production logistics system. *Int. J. Prod. Res.* **2016**. [CrossRef]
136. Hsu, A.P.; Lee, W.T.; Trappey, A.J.C.; Chang, A.-C.; Trappey, C.V. Using System Dynamics Analysis for Performance Evaluation of IoT Enabled One-Stop Logistic Services. In Proceedings of the 2015 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Hong Kong, China, 9–12 October 2015.
137. Chevillard, S.V.; Guri, G.; Frete, O.; Clari, F.; Gluhak, A.; Vermesan, O.; Bahr, R.; Moretto, P. Report on the factors of user's acceptance framework and societal and education stakeholders, H2020—UNIFY-IoT Project. 2016. European Research Cluster on the Internet of Things. Available online: http://www.internet-of-things-research.eu/index.html (accessed on 12 March 2017).
138. Finegan, A. A methodology to design an expert system for remote sensing technology management. *Int. Arch. Photogarmm. Remote Sens.* **1993**, *29*, 982.
139. Gil-Garcia, J.R.; Pardo, T.A. Multimethod Approaches to Understanding the Complexity of e-Government. *Int. J. Comput. Syst. Signal* **2006**, *7*, 3–17.
140. Mingers, J. The paucity of multimethod research: A review of the information systems literature. *Inf. Syst. J.* **2003**, *13*, 233–249. [CrossRef]
141. Delicato, F.C.; Pires, P.F.; Batista, T.; Cavalcante, E.; Costa, B.; Barros, T. Towards an IoT ecosystem. In Proceedings of the First International Workshop on Software Engineering for Systems-of-Systems, Montpellier, France, 1 July 2013; pp. 25–28.
142. Peltoniemi, M. Business ecosystem: A conceptual model of an organisation population from the perspectives of complexity and evolution. In *Research Reports 18*; e-Business Research Center: Tampere, Finland, 2005.
143. Fleisch, E. What is the internet of things? An economic perspective. *Econ. Manag. Financ. Markets* **2010**, *2*, 125–157.
144. Dowling, A.M.; MacDonald, R.H.; Richardson, G.P. Simulation of systems archetypes. In Proceedings of the 1995 International System Dynamics Conference, Tokyo, Japan, 30 July–4 August 1995.