Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2016, Article ID 8178417, 15 pages
http://dx.doi.org/10.1155/2016/8178417

Review Article

Beyond the Internet of Things: The Social Networking of Machines

Marina Pticek,[1,2,3] Vedran Podobnik,[1,2] and Gordan Jezic[1,3]

[1] *Department of Telecommunications, Faculty of Electrical Engineering and Computing, University of Zagreb, 10000 Zagreb, Croatia*
[2] *Social Networking and Computing Laboratory (socialLAB), Faculty of Electrical Engineering and Computing, University of Zagreb, 10000 Zagreb, Croatia*
[3] *Internet of Things Laboratory (IoT-lab), Faculty of Electrical Engineering and Computing, University of Zagreb, 10000 Zagreb, Croatia*

Correspondence should be addressed to Vedran Podobnik; vedran.podobnik@fer.hr

Received 27 November 2015; Revised 31 March 2016; Accepted 26 April 2016

Academic Editor: Andrei Gurtov

Communication is a prerequisite for any form of social activity, including social networking. Nowadays, communication is not reserved only for humans, but machines can also communicate. This paper reviews the state-of-the-art technology in the area of Machine-to-Machine (M2M) communication by comparing the M2M concept with other related research paradigms such as Wireless Sensor Networks, Cyber-Physical Systems, Internet of Things, and Human-Agent Collectives. Furthermore, the paper analyses trends in the interconnecting of machines and identifies an evolutionary path in which future (smart) machines will form mostly or completely autonomous communities bonded through social connections. Such communities—*machine social networks*—will be formed dynamically, just like human connections, and based on the needs of machines, their context, and state of their environment. Finally, the paper outlines the current evolutionary stage and identifies key research challenges of machine social networking.

1. Introduction

Due to increased affordability of information and communication technology (ICT), now available more than ever, there is an endeavour to connect not only everyone, but also *everything*. Besides the Internet, other networks are also increasingly connecting things every day and everywhere. Such connected things include a variety of devices and a particular group of them is known as *machines*.

Intermachine communication originally emerged from telemetry technology, and its main purpose was to measure data and automatically transmit it from remote sources typically by cable or a radio. Nowadays, new types of sensors are being developed, which have better perceptual abilities than humans and can detect information that humans cannot. Affordable electronic devices have led to an increasing number of them being connected to the Internet [1]. According to Cisco [2], humans became the minority on the Internet around 2008 or 2009, and that trend is accelerating each year. In the near future, the number of connected devices is expected to grow tenfold, resulting in connected devices outnumbering connected humans by a hundredfold. The estimation is that by 2020 there will be 8 billion people, and the number of various machines will be 50 billion [3]. Other more reserved estimations predict between 18 and 26 billion machines [4–6]. Nevertheless, regardless of which estimation will turn out to be more accurate, the trend is obvious and irreversible.

The increasing number of machines makes managing their communication and coordination a complex and time-consuming task, while the devices themselves remain quite simple-functioning. Each connected entity is part of one or more communities and/or networks, hence the assertion that we now live in a *networked society* [7]. In any networking scenario, entities connect and form groups and collaborate in achieving specific collective goals. These facts substantiate why our era has been proclaimed *the second machine age* [8], making it reasonable to expect that devices will also form enormous social networks, *machine social networks*. The contribution of this paper is twofold: (i) a review and comparison of currently relevant research paradigms in the area of interconnecting machines, namely, *Wireless Sensor Networks*, *Machine-to-Machine (M2M)*, *Internet of Things*, *Cyber-Physical Systems,* and *Human-Agent Collectives,* and (ii) an extension to the human scenario of transitioning from Web 1.0 to Web 2.0 era along with a similar scenario for machines and identifying unresolved research challenges caused by machine social networking that provide a motivation and guide for scientists to pursue further the abovementioned research areas.

Section 1 of this paper analyses key features of a *machine* and proposes a definition of a device classified as a machine taking part in M2M communication. Similarly, key features of M2M communication are described. Section 2 analyses similarities and differences among related research paradigms in the area of interconnecting machines. An evolutionary path of machine networking and the associated concept describing ongoing development leading to machine social networks are explained in Section 3. Section 4 focuses on machine social networks and defines them and their main building blocks: *machine profiles* and *machine social connections*. Additionally, future possible applications of machine social networking, the "*machine Facebook*" and the "*machine Twitter,*" are elaborated upon. Section 6 concludes the paper by identifying research challenges that machine social networking might possibly face.

2. What Is a "Machine" in the Machine-to-Machine Paradigm?

The term *Machine-to-Machine (M2M)* is often used synonymously to (and is defined by) the term *Machine-to-Machine Communication (M2MC)* and *Machine-Type Communications (MTC)* [9–17] because in its essence M2M involves communication between *machines*. M2M has the role of establishing conditions allowing devices to bidirectionally exchange information with an application over a communication network; thus, the communication network has the key role: a device that communicates with an application running is not considered an M2M relationship. In [18], the authors explain that the term M2M is an acronym of *M2(CN2)M: Machine-to-(Communication-Network-to-)Machine*. The rationale behind M2M communication is based on two observations: (i) a networked machine is more valuable than an isolated one and (ii) an interconnection of multiple (smart) machines enables development of more autonomous and intelligent applications [17]. Some definitions even denote the process of two (electronic) systems autonomously communicating as M2MC [11, 17]. M2M is also used as a common term for the technologies that enable M2M communication or even declared as a technology itself [19]. However, the key features of communication for it to be classified as communication between machines are diverse.

All definitions of M2M(C) have a common key feature: communication takes place between machines with *minimum or no human intervention*. The main goal of M2MC is "to enable the sharing of information between electronic systems autonomously" [14]. The means of communication in M2M may vary. The definition in [12] states that communication generally occurs through a telecommunications network. Further, a variety of media is covered in the definitions of [10, 17], which points out that communication takes place via wire, wireless, or both. Communication is classified in [10] into three types: (i) the first type demands real-time communication and high density data flow (e.g., tracking); (ii) the second type demands medium density data flow and schedules data transmissions (e.g., logging); and (iii) in the third type, communication occurs sporadically and the data have a minimal alert-message size (e.g., exception-based applications for notifications and signalling). The M2M Alliance describes M2MC as "communicative networking of mobile or stationary (intelligent) objects, where data transfer is automated and independent of the underlying network infrastructure" [20]. The definitions and specifications by the 3GPP standardization body point out that M2MC is different from previous communication models and that it involves "a potentially very large number of communicating terminals" that have "to a large extent little traffic per terminal" [11].

The definitions also do not provide clear specifications as to what these terminals, systems, or devices, *machines,* that take part in the M2M communication actually are. While some assert that communicating devices should be of the same type or have the same capabilities [17] or be similar [18], others implicitly disagree by providing a more flexible definition of the device; that is, it can be many things [21]: a meter, sensor, mobile device, computer, or even an entire (embedded) system. Furthermore, some authors consider machines to be just sensors [22].

In the M2M context, it is more important to clarify what key features and essential functionalities a device should have in order to be perceived as a "*machine,*" rather than considering what kind of device could be a machine (e.g., if it is a simple sensor or a smart watch or phone). In [22], machines are considered sensors "activated by certain events and report a small amount of data to the network." The definition in [23] does not specify a machine in terms of type of device; instead, it points out that machines capture events and send the data through a network to an application that translates the data into relevant information. The authors in [24] do not consider the machines as solely "dummy" devices that consume energy and perform certain functions but refer to them as *smart* machines "equipped with hardware (processors and memory) and software (artificial intelligence algorithms) with a certain level of intelligence and autonomy." This definition requires determining the relationship between a machine and a smart device.

The *smart device* is described as an electronic device that connects to other devices and networks via a wireless connection and operates to some extent autonomously and interactively [25]. The most common types of smart devices are smartphones, tablets, phablets (phones/tablets), smart watches, smart bands, and smart key chains. However, the term can also refer to a pervasive and ubiquitous computing device, exhibiting some of the properties of pervasive and ubiquitous computing and which may also include artificial intelligence [26]. These definitions consider advanced devices as *smart*, meaning that less advanced devices are not considered smart devices. This implies that a smart device is considered a machine, but not every machine is a smart device. The smarter the device, the more likely its ability to play a dual role in an M2M system. At the same time, the smart device can be (i) an interface to a machine or an M2M system and (ii) a machine itself. Smart devices are most often physically located on the *human* side of the system, given that people carry their smart devices with them. These devices provide people with an (application-based) *interface* towards M2M systems, but the device may not necessarily perform measurements and thus generate data. In that case, a smart device is considered to be a part of the system representing a human. Smart devices also play a true *machine* role by performing measurements and gathering data through various sensors built in it and in that case can be considered a nonhuman entity, a machine. An example of a dual role smart device is a smartphone and is considered (i) an interface towards an M2M system if used as a proxy to access measurements made by a smart watch (e.g., an iPhone smartphone connected to a heart rate sensor on an Apple Watch smartwatch) and (ii) a machine if used as a sensor (e.g., an iPhone smartphone used as an accelerometer).

Two major M2M standardization bodies, *ETSI* and *oneM2M*, also provide definitions of a machine, but in terms of the *M2M device*. According to the ETSI definition, the M2M device runs application(s) using M2M capabilities and network domain functions [27]. The oneM2M definition says that the M2M device is a physical piece of equipment featuring communication capabilities, while also providing computing, sensing, and actuation services [28].

Based on the given definitions of Machine-to-Machine (M2M) communications and the concept of a machine, several general conclusions can be drawn:

(i) A *machine* is a device that contains both hardware and software and has some form of autonomy, intelligence, and smartness. It is most often automated and its main role is to capture events in its environment and react accordingly, most often by sending captured data through a network, either via wired or wireless communication.

(ii) The term *Machine-to-Machine Communications* relates to the term *Machine-to-Machine*, because the essence of M2M is the communication among machines.

(iii) M2M refers to communication performed from two to any large number of machines and exhibiting the features given in the definition of a machine. Communication occurs with minimal or no human intervention, via wire or wireless, and its main purpose is to transmit real-time machine data of any size in a scheduled or spontaneous manner.

3. Machine-to-Machine Research Paradigms

Literature presents research paradigms like Wireless Sensor Networks, Internet of Things, Cyber-Physical Systems, and Human-Agent Collectives as having features similar to M2M, and sometimes they are even considered as being equivalent. The following analysis presents similarities and differences of related research paradigms.

3.1. Related Research Paradigms

3.1.1. Wireless Sensor Networks. Wireless Sensor Networks (WSNs) refer to a group of spatially distributed autonomous sensors that monitor physical conditions, work in unison, and pass collected data through a network to a centralized location. By definition [29], sensor nodes are loosely connected and deployed only once and use a wireless medium for communication. Similar to M2M, WSNs support a large number of nodes, self-organization, autonomous operation, and seamless domain-interoperability [17], but two features distinguish them from M2M: (i) various sensors are the only included hardware entities in WSNs and (ii) communication is exclusively wireless. The definition of M2M(C) in the previous section denoted machines as sensors and more advanced hardware and also whether they communicated via wire or wireless.

An example of an M2M system is a smart vending machine that detects and responds to a person in a personalized way, also identifying the product being dispensed and maintaining contact with the operator. The vending machine is an *M2M machine* in its entirety, equipped with software and hardware for communicating via wire and wireless. But if we observe only the product identification subsystem of this vending machine, this subsystem can be perceived as an integrated WSN. If the products in the vending machine are tagged with an RFID (*radio-frequency identification*) tag, then the RFID-readers play the role of WSN's sensors that communicate wirelessly.

3.1.2. Internet of Things. The Internet of Things (IoT) is a term used to describe "technologies, systems, and design principles associated with the emerging wave of Internet-connected things that are based on the physical environment" [30]. It refers to the network of uniquely identifiable things (objects) and their virtual representations in the Internet-like structure, which are able to collect and exchange data and are remotely controlled across the existing network infrastructure [17, 31, 32]. It comprises major components like sensing, heterogeneous access, information processing, security, privacy, and applications and services. IoT is sometimes referred to as *pervasive and ubiquitous computing* because the two concepts overlap in terms of embedding microprocessors into, and, by doing so, adding intelligence to, everyday devices, so they can be connected and communicate information [25, 26, 33]. Pervasiveness implies that such devices exist everywhere around us and are constantly connected and available. It relies on the "convergence of wireless technologies, advanced electronics, and the Internet" [34] and has the goal to create *smart* products that communicate unobtrusively via the Internet.

IoT has gained popularity over the last few years, becoming present as wearable gadgets, in vehicles, buildings, industry, public spaces, and assets (from refrigerators to transport ships) and as support in the production of resources necessary for human survival (e.g., agriculture and environmental monitoring). Representative IoT use-cases are intelligent public and/or automotive transportation [35], smart cities [36] along with smart buildings and homes [37], industrial automation, health/telemedicine monitoring [38], intelligent infrastructure (e.g., "smart grid" [39] and waste management and heating [40]), and retail banking [30]. The latest emerging form of IoT is *participatory sensing*, where groups of people owning smart devices equipped with various sensors, such as smartphones, are being utilized as mobile sensor carriers that contribute their data to form a greater body of knowledge about environment, pollution, mobility, and traffic congestion. This form of data collection is studied in the academic community as mobile crowd sensing [41, 42], with the goal of turning IoT to *openness* (towards open IoT). The aim is to develop open IoT platforms which would enhance value addition to the initially collected data and support development of related applications and services.

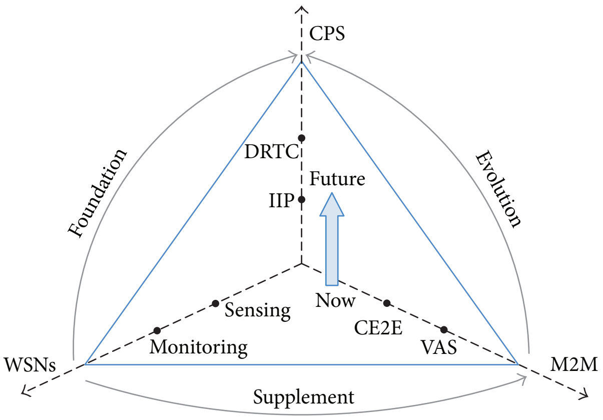
The authors in [17] assert that M2M and WSNs belong to the IoT, given that all of these possess the previously mentioned components and differ only in design. They view WSNs as the basic IoT scenario and M2M as a higher level system. In [43], IoT is considered the equivalent of M2M, due to the similar methods of data collection, information exchange between devices, and automated reaction to such processes. However, this comparison is considered cursory and has not been analysed adequately as M2M may not entirely belong to the IoT. Machines in M2M communications need not necessarily interact over the Internet if they belong to an isolated system for a specific purpose, if spatially close to each other. The IoT may initially look like M2M communication, with sensors and other devices linked by wired or wireless networks to ICT systems, but the main feature distinguishing IoT from M2M is connecting such systems and sensors to the broader Internet and the general use of Internet technologies. M2M is "point problem-orientated" [44]: solutions, devices, and applications are dedicated to solving a single task, and that restricts the devices to being application-specific. This results in nonreusability of such devices beyond a single M2M solution, whereas IoT demands flexibility in applications. Consequently, if progress is to be expected in the future, devices that are part of the IoT will no longer be application-specific as is the case in M2M solutions. Devices used in a variety of applications will provide greater benefit and represent a shift from application-specific to application-independent devices in order to achieve true IoT.

3.1.3. Cyber-Physical Systems. Cyber-Physical Systems (CPSs) are systems that feature a higher combination and coordination between their computational and physical elements [45]. Real-time computing and physical systems interact tightly, providing a strong emphasis on interaction with the physical world and connectivity, for example, over the Internet. CPSs are "large complex physical systems that are interacting with a considerable number of distributed computing elements for monitoring, control, and management which can exchange information between them and with human users" [46]. The exchanging of information, material, energy, and/or use of common resources (e.g., waterways, airspace, rail-tracks, and roads) connects the elements of a physical system, whereas communication networks connect the elements of the control and management system. The main enablers of CPS are advanced network technologies, distributed multiagent controls, and cloud computing, with the key features being reactive and real-time computation, concurrency, safety-critical applications, and feedback control of the physical world.

Based on previous definitions, sensor and actuator networks are considered precursors of CPS. Authors in [17] agree with this evolution line; the common denominators are the concepts of sensing, information processing, heterogeneous access, and applications and services. In this evolution line, the authors consider CPS also as a part of IoT, along with WSNs and M2M systems. When considering the complexity of interacting elements, M2M and CPS are considered higher level systems, while WSNs are viewed as the basic IoT scenario. When comparing CPS to M2M systems, CPS is considered an evolved form of M2M, integrating the concepts of IoT and autonomous control in M2M and also possessing ambient intelligence. An object's "identity" in CPS consisted of two interconnected parts: (i) a physical entity and (ii) its virtual (cyber) representation or entity. The virtual entity acts as a "simulation model" that replicates the behaviour of the physical machine in a virtual fashion, for example, programmatically changing machine's virtual "states" according to changes in machine's "real-life" (hardware) states. The interconnection between these two object identity parts is done by sensors and actuators. Still, a CPS is a complete, individual entity as a whole, but viewed from the global perspective it is disconnected from other CPSs. A connected CPS forms the Internet of Things.

The CPS focuses on making the interaction intelligent and making interactive applications and distributed real-time control, which M2M lacks. CPS is slowly becoming a reality and CPS applications can potentially benefit from huge wireless networks and numerous smart devices providing intelligent services based on knowledge gathered from the physical world.

3.1.4. Human-Agent Collectives. The term Human-Agent Collectives (HAC) [47], the most recent paradigm analysed in this paper, emerged to fulfil the need for a paradigm depicting new sociotechnical systems that interleave humans and computers. HAC is based on the idea that incorporating humans as information gatherers and processors in autonomous systems, which include autonomous software agents [48], is necessary and beneficial [49, 50]. In the HAC paradigm, humans and smart software agents engage dynamically in flexible social relationships needed to achieve both their individual and collective goals. This way, depending on the particular task, "different constellations of people, resources, and information come together, operate in a coordinated fashion, and then disband" [47]. This implies that such systems display a greater autonomy and are characterized as being *social*. As they operate in a real-world context, HAC operation processes include data capturing (by a sensor or



IIP: intelligent information processing
CE2E: communicating end-to-end
DRTC: distributed real-time control
VAS: value-added services

Figure 1: Correlations among M2M, WSN, CPS, and IoT [17].

a human participant), data fusion, and decision processes and take actions based on calculated information, where the collective actions result in acceptable social outcomes, for example, fairness, stability, or efficiency. HAC systems thus demand an accountable information structure that provides accuracy and the seamless merging of human and agent decisions, sensor data, and crowd-generated content.

3.2. A Comparison of M2M, WSN, CPS, IoT, and HAC. Despite the similarities between WSNs and M2M systems, WSNs are considered a basic scenario of IoT, whereas that part of M2M that communicates over the Internet is deemed more advanced because it supports both wired and wireless communication systems and, as its most highlighted feature, implements machine-type communication, implying no or minimal human intervention in the communication among devices. However, the relation between M2M and IoT is viewed differently in [51] and according to this approach, M2M and IoT are concepts that overlap to some extent. Such viewpoint was also taken in the analysis of M2M and IoT relation in [52]. This analysis pointed out that the main difference between M2M and IoT is in what lies in their focus. IoT is focused on connecting things to Internet by the standard IP protocol and exchange, semantic organization, and processing of the data. IoT does not consider potential problems on the underlying network level "beneath" the IP layer. However, M2M does focus on it, for example, how a large number of connected devices would impact the mobile network, which is optimized for exchanging large data over high speed and not for the occasional transmissions of few bytes of machine readings. Besides that, M2M also focuses on connection security and identification and management of devices.

Intelligent information processing (e.g., neural networks and data fusion), ambient intelligence, and distributed real-time control are neglected in the M2M concept and thus are its main limitations. Once the capabilities of intelligent information processing, such as decision-making and autonomous control, are built into an M2M system, it becomes a CPS. Whereas M2M systems are currently the main instantiations of IoT, CPS will be an important future technical form of the IoT. Though the IoT is sometimes considered equivalent to CPS, they are different levels of vertical digital integration. The IoT is made up of "physical entities" within CPSs and networked for information transfer. However, as simple hardware is not capable of connectivity, it is then transformed to a software ("virtual entity") level for connection purposes. In other words, this specific hardware, that is, the physical entity of a CPS, is the "thing" connected to the IoT. Accordingly, CPS forms the first level of vertical digital integration (intrasystem components interacting harmoniously), whereas the IoT is the second level (ubiquitous intersystem connections). Importantly, CPS is given greater attention in academic research, whereas the term of IoT is widely used in industry and by governments.

Analysis presented above generally supports ideas about relations among WSN, M2M, CPS, and IoT that were presented and analysed in [17]. All of these concepts are drawn from the same evolutionary line and are characterized by the internetworking of large numbers of devices that communicate autonomously, eventually leading to emergence of large *machine social networks*. In the evolution towards machine social networks, the IoT is considered to be just an intermediate step [53]. Figure 1 shows the described relations. The IoT domain comprises three main paradigms: WSNs, M2M, and CPS, which are represented by the axes. Basic WSNs are those that perform *sensing* only, while their ultimate purpose is *monitoring*. WSNs *supplement* M2M systems and are also *foundation* of CPS, which will appear with the ongoing *evolution* of M2M. In Figure 1, M2M is identified by *end-to-end communication* which is the fundamental purpose of M2M and *value-added services* as the ultimate purpose of M2M systems, which are built on data communicated from one end to the other. The figure indicates that M2M systems are currently the most widespread type of systems, but in the future CPSs are expected to dominate. CPSs are characterized

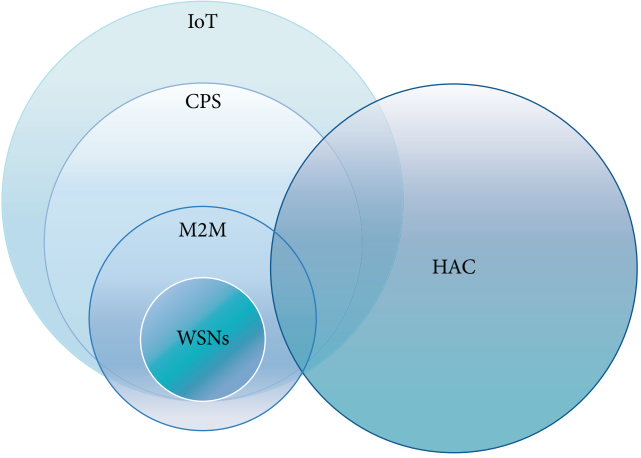


Figure 2: Correlation between IoT and HAC.

by their advanced features, *intelligent information processing* and *distributed real-time control*, being the ultimate purpose.

In comparing IoT and HAC paradigms, it becomes evident that they share the common concept of autonomous system communications comprising a large number of networked devices. However, the difference between the two paradigms lies in human involvement. Whereas the IoT emphasizes the evolution of device communication without involving humans, the HAC paradigm relies on benefits from human involvement in data acquisition processes and even data processing. For this reason, these two concepts overlap.

If we observe the subsets of IoT, WSN, M2M, and CPS, then HAC conceptually intersects with M2M and CPS, but not with WSN. The latter is just the basic scenario of the IoT and covers basic monitoring activities and data transfer. Sensors in WSN can be considered as mere data collectors. Whereas M2M and CPS include all of WSNs, they also include more autonomy and intelligence emerging from the social component incorporated in machine networking. Consequently, these two concepts fit in the segment of the HAC paradigm that refers to the nonhuman part: CPS devices interact with the physical world through sensors and actuators in a feedback loop [29]. Figure 2 displays the described relation among the concepts.

The proliferation of M2M has helped the industry realize the important challenge it is faced with in the global development of M2M, specifically a lack of M2M standards. Open standards are key enablers for the success of any kind of M2M communication, as is the case with IoT [54]. Significant improvements in standardization have been achieved with the emergence of oneM2M (http://www.onem2m.org), a global M2M standard.

4. Machine Internetworking 1.0

In the web era known as Web 1.0, people browsing the Internet were only mere consumers of the Internet's mostly static contents. Subsequently, the turn of the millennium was marked by the emergence of Web 2.0, a ubiquitous web of blogs, wikis, and social networking websites [55]. Web 2.0 has established a new information exchange model where users themselves have become the creators and consumers of web content, and they possess the ability to spontaneously create and edit websites. During the Web 2.0 era, the web became a P2P (*peer-to-peer*) network, where all users have an equal participation status and are considered active users, in comparison to Web 1.0 where users were only passive consumers. When compared to Web 1.0 which was content focused, Web 2.0 shifts the focus onto the user and web services. The Web 1.0 era could well be described as a network of data producers and consumers. In the Web 2.0 era, the roles of producers and consumers have merged into a single entity, that of the *prosumer* (producer and consumer). Hence, Web 2.0 could well be described as a peer-to-peer network of prosumers, who take part in numerous social networking activities.

However, today's social networking has been raised to a whole new level when compared to its initial phase [56]. There is a growing trend in the emergence of various stakeholders from industry that aim to benefit commercially from social networks. As a side effect, a new demand on social networks has been created: social networks and platforms need to evolve to more advanced forms in terms of adding *smartness* and intelligence into their background. Industry aims to offer social network users personalized and intelligent services and applications. This cannot be achieved just by mere information gathering, but a sophisticated analysis for deeper knowledge extraction is needed. Complex decisions rely on vast amounts of diverse data, which includes both metadata and collected data. So far, profiles have only served as an essential collection of information describing the various attributes of connected entities. For all these reasons, social networking has to become *context-aware* and, consequentially, network entity profiles need to be information-richer [57].

4.1. Web 1.0 Era of the Machines. Taking the point further, machines are nowadays in the Web 1.0 era; that is, they only send data to servers and perform no other networking functions. Certain parallels can be drawn between the human Web 1.0 and the current trends in the exploitation of (smart) machines. Machines are connected only at the lowest, *physical layer* and act as content producers. Their connections are static and predefined by humans, as is the flow of the data they produce. *Servers* along with installed *databases* perform the role of data consumers. The data may not be directly sent to servers by machines, but the usage of a machine coordinator, a router or a proxy, is more frequent. The machine coordinator intermediates in the communication and, in some cases, aggregates the collected data. Data is processed upon arrival at the servers and stored or may be passed along to other servers. The processed data are the basis for *services* that can be built on top of them (Figure 3).

In the near future, connected devices will serve as generators of big data, based on which numerous value-added services will be built [58]. According to the described processes, four major components in the M2M are identified: (i) sensors/machines, (ii) communication, (iii) computation, and (iv) services [43]. Each of these faces challenges for further

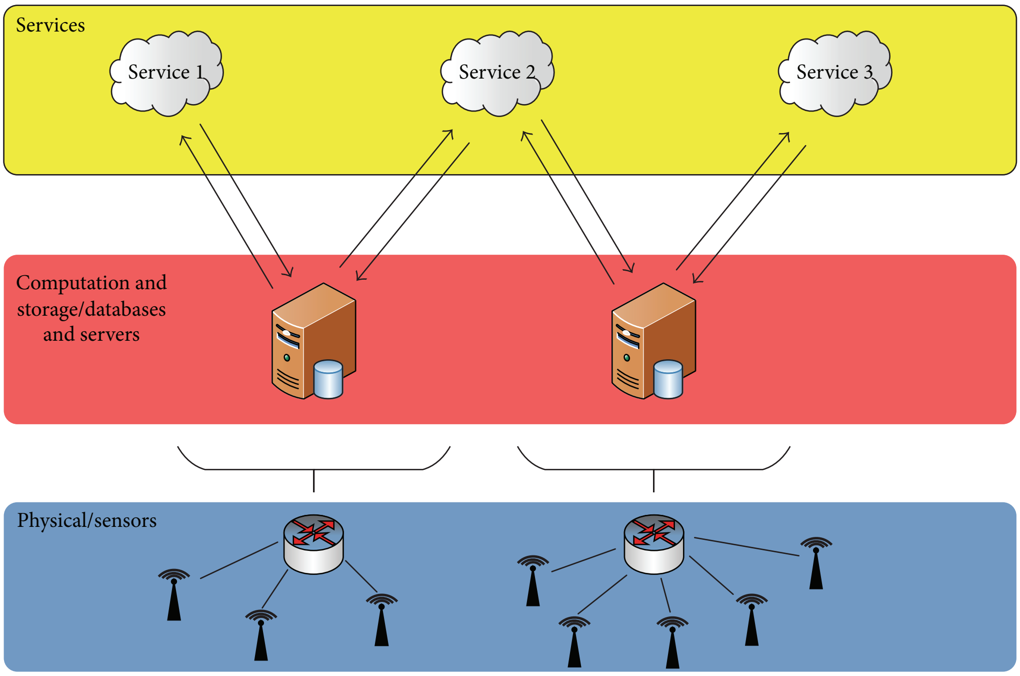


Figure 3: Web 1.0 of the machines.

advancement in machine networking. First, *sensors/machines* will have to be more energy efficient, without the need for battery changes and hands-on work with a physical piece of equipment. For the same reason, machines must be remotely manageable. *Communication* will have to be secure (e.g., data privacy), as well as robust (e.g., handling large number of connected devices). Data *computation* procedures will have to be adjusted for the real-time processing of large volumes of data and will require optimal distribution of computational servers, data storage, and cloud intelligence. To enable ecosystem innovations, both machines and processed data will need to have standard interfaces in order to enable new *services*.

4.2. The Web 2.0 Era of Machines. The machine Web 2.0 era is yet to come, where metadata on humans and machines including gathered data from the environment is exchanged among machines acting as enablers of machine social networking. Over the last decade, the divide separating machine-centric and human- or IT-centric technologies and systems has begun to close. However, the current networking and communication infrastructure is optimized for human communication, especially cellular networks, and many wireless standards are optimized for H2H (*Human-to-Human*) applications [43]. Machine communication demands are different, meaning that machines are application-specific [9] and exhibit different communication patterns; for example, machine mobility is low or nonexistent and communicated data is of the same size and transferred periodically. Despite transferring small amounts of data, the use of existing infrastructure is exceptionally challenging as it may not be able to support the networking of a large number of devices.

Delivering intelligent services requires smarter devices [59], enabling the discovery of new services, creating new connections, exchanging information, utilizing the capabilities of other devices, connecting to external services, and uniting to achieve common goals. The future machine social networks will connect devices possessing different levels of intelligence. They will include both IT-centric devices (e.g., smartphones, tablets, PCs, switches, and servers) and non-IT-centric devices (sensors, actuators, diagnostic equipment, and vending machines) [60]. In order to achieve *smartness* in machine networks, connected devices have to be aware of their environment, not only in terms of their context, but also in terms of awareness of other devices that make up their *neighbourhood* and to which they can be connected. In other words, *network awareness* and *context awareness* have to be built in into devices, which can only be achieved through an interdisciplinary approach to M2M research (Figure 4), due to the specificities of M2M systems. Whereas basic M2M-related research is *sensor-orientated* (e.g., towards energy efficiency) and *communication-orientated* (e.g., size efficiency of communicated message), machine requirements for network awareness and context awareness are the subject of ongoing research on *context computing*. Furthermore, service and application research areas address machine data utilization and the utilization of future social abilities of machines, that is, machine autorealization of the connections required using automated computational methods, with none or minimal human engagement.

Nevertheless, smart objects (devices) are considered only the first step in the evolution leading towards social machine networks [61]. The generation of devices that comes after the *smart* objects (*res sapiens*) is objects with *social consciousness* (*res agens,* an acting object). These *res agens* could possibly translate the awareness of casual relationships into actions. The generation following the *socially conscious* devices is

Table 1: Web 1.0 and Web 2.0 in human and machine scenario.

	Paradigm feature	Human	Machine
Web 1.0	*Roles*	Content producer: web server Content consumer: human (web browser)	Content producer: machine Content consumer: data collection server
	Content exchange	One-way (server-to-human)	One-way (machine-to-server)
	Communication paradigm	Client-server	Client-server
Web 2.0	*Roles*	Prosumers: humans	Prosumers: machines
	Content exchange	Two-way (human-to-human, servers are intermediators)	Two-way (Machine-to-Machine, servers are intermediators)
	Communication paradigm	Peer-to-peer	Peer-to-peer

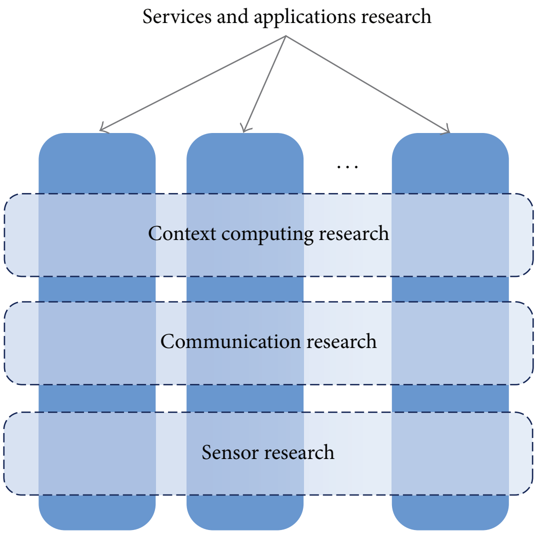

Services and applications research
. . .
Context computing research
Communication research
Sensor research

Figure 4: A scheme of interdisciplinary research efforts in the quest of a unified M2M system architecture [43].

a new type of object: the *social* object (*res socialis*). These evolutionary steps and their main features are displayed in Figure 5. IoT is unachievable without the evolutionary step of the *social* object. Social objects will become parts of social communities incorporating objects and devices, forming and operating within the *social IoT* (SIoT). Social connection among machines would transform them from passive data-collecting devices into active members of a thriving ecosystem. Socially networked machines could operate without human intervention and would thus have the ability to dynamically and automatically make decisions.

In the social machine networking paradigm, the lowest level is the *physical* layer that contains actual devices, similar to the physical layer in the machine Web 1.0 paradigm. However, the crucial difference is the middle layer. In Web 2.0, the middle layer is the *social layer*, which is where the networking of *social* machine happens. The social layer contains social representations of physical machine entities (e.g., machine *profiles*) and their *social connections*. Figure 6 shows what a social layer would look like. Devices that are physically connected would obviously be connected socially as well (bolded line), but the devices that are physically remote could also be connected in this way (dotted line),

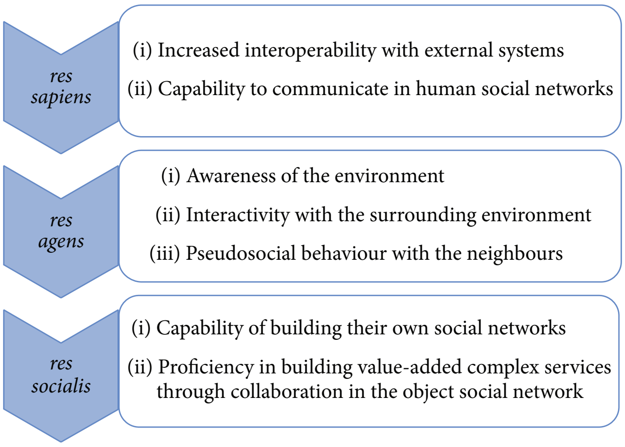

res sapiens
(i) Increased interoperability with external systems
(ii) Capability to communicate in human social networks
res agens
(i) Awareness of the environment
(ii) Interactivity with the surrounding environment
(iii) Pseudosocial behaviour with the neighbours
res socialis
(i) Capability of building their own social networks
(ii) Proficiency in building value-added complex services through collaboration in the object social network

Figure 5: The main features of three phases of IoT objects [61].

providing a true example of a machine social connection. The physical components enabling such machine social networks, for example, servers and data storage, are placed in this paradigm as a layer *behind* the social layer, because they are not in the focus of the machine Web 2.0 paradigm. Therefore, the middle layer in the proposed layer stack has a dual purpose and serves as (i) an enabler of social networking platforms and (ii) a storage for collected data. On top of the middle layer is the *services* layer, similar to the machine Web 1.0 paradigm, but in this case, the services can be offered among the machines as well (i.e., machine peer-to-peer relationship). Table 1 summarizes this described evolution and compares the main characteristics of Web 1.0 and Web 2.0 eras in both the human and machine scenario.

5. Machine Social Networks (Machine Internetworking 2.0)

The machine social network conceptually complies with the machine Web 2.0 paradigm. It is a network of devices that are *contextually, socially, and network* aware and which are able to dynamically create (social) connections between each other in order to offer services to each other and to jointly solve problems.

All social networks comprise entities and their interconnections. Entities are represented by their profiles; the

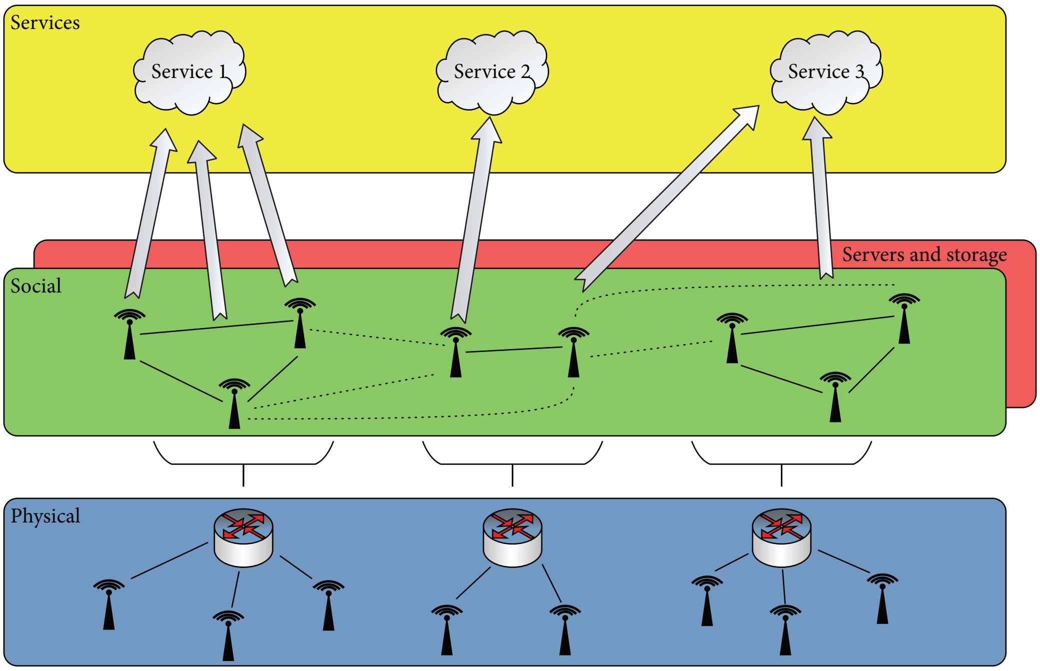


Figure 6: Machines in Web 2.0.

connections define the manner and direction of communication between them. Therefore, in machine social networks, machines are the entities and are represented by *machine profiles*, whereas their associated relationships are characterized as *social connections*.

5.1. Machine Profiles. Machine profiling, advanced or not, is done similar to human profiling [62] in social networks. When profiling is categorized as *advanced*, it suggests that a profile is not created in unidirectional sense (basic user input) but instead from various data sources. When considering possible machine data sources, three domains can be identified: (i) basic (communication) connectivity domain, (ii) contextual domain, and (iii) social domain. Figure 7 illustrates a conceptual social machine profile comprising the three proposed domains.

Basic connectivity enables data transfer back and forth between the machine and the social network. Without this, a machine cannot communicate with any other network component; hence, this is considered one of the crucial aspects of the machine. The basic connectivity aspect is considered as a mediating set of tools that provides machine *network awareness*. However, it does not specify the kind of network to which the machine is connected; it could be any kind of connection: wired, wireless, or hybrid. Furthermore, basic connectivity includes any kind of data on the machine's ability to connect with other machines, that is, connection metadata. It does provide not only general metadata such as data on the service provider but also data necessary for connecting to the device. It may also include security data, such as access rights and privacy descriptors.

Context links a machine's environment to its factual purpose, the ability to perform measurements and/or host data or even host aggregated and processed data (e.g., in the case of *fog* computing), where data processing can be offered in the form of services or procedures invoked by the machine. It includes not only data about the machine's environment but also data about machine's physical instance. Data that refers to physical instance of a machine (i.e., machine metadata) is device-specific and represents a part of machine's contextual data. Other forms of contextual data refer to the machine's environment, which can be either the raw measured data provided by the device or a service invoked by the device.

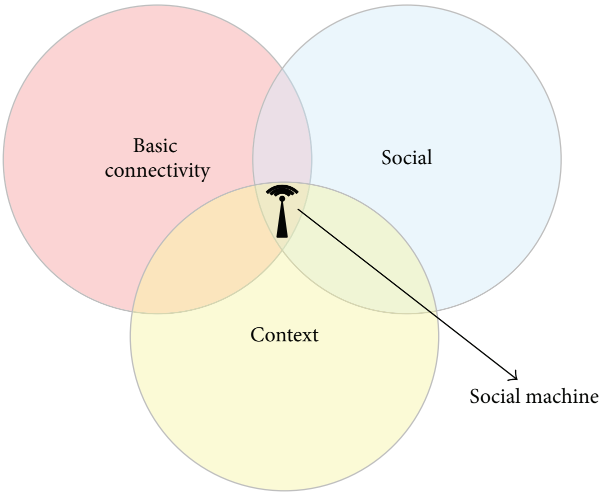


Figure 7: Profile of a social machine.

The *social* aspect of a machine is its ability to form a network with other machines and benefit from social networking. This part of the profile is not about basic communication but about (social) networking, where basic communication and connectivity are a precondition. This part of the profile provides the data necessary to create a "social" representation of a device, along with the relevant data as what it can do and/or provide and which part of it might be useful to other devices. Similar to a "friend list" in a human social network profile, this part of the profile includes information such as the machine's functional and spatial neighbourhood and related entities. Just like on Facebook for humans, applications can be associated with a device once it has used them, and, subsequently, a device can list its needs (interests). This allows other devices to offer their services to the mentioned device based on the needs (interests), as well as offering services, data, and sensors (i.e., metadata on offered resources).

5.2. Social Connections in Machine Social Networks. Social network connections, regardless of whether they are established for physical connection or social benefit, can exhibit a different nature; that is, a social connection can be a function of *friendship*, but it can also be a function of *following*. The friendship function implies a bidirectional connection, whereas the following function implies a unidirectional connection.

In a "machine Facebook" scenario, two machines form a friendship-like (bidirectional) social connection if they require mutual assistance in regard to services they are offering to one another. For example, two machines, capable of performing different types of computation but also requiring the other machine's computational services, browse the social network in search of a machine that offers such a service but at the same time also advertises the kind of service it requires. Having found the most compatible machine (i.e., each other), they then form a bond and request each other's computational service. After accepting the *friendship request*, they exchange data and perform the required analysis. The machines return the results to each other and subsequently decide whether to maintain the connection permanently (dotted line in the illustration) or disconnect it. Besides services, machines can also exchange measured data in this way. Figure 8 illustrates this particular scenario.

Say, for example, that a particular machine (on the left) measures *temperature*, while the other machine (on the right) measures *atmospheric pressure*. In this scenario, two different services are to be established in them by two different operators or developers, for example, prediction of road *visibility during fog* in the first machine and simple *weather forecasting* in the second one. However, none of the machines provide sufficient data for the service, but the situation improves if they each accessed the other's measurements. By browsing a machine social network (platform), they find each other given that each of them provides the data stream of their measurements as a service, and they then enter a *machine friendship*. This *machine friendship* connection is viewed as a logical connection and in Figure 8 is displayed as dotted line. This relationship between machines is similar to a human friendship on Facebook. Specifically, even though two people form only a single connection between each other, Facebook as a platform offers them multiple services based on that one connection, for example, live messaging, photo tagging, and writing on the wall. Therefore, if the first machine were to be upgraded to measure not only temperature but the current air humidity as well, it could offer its humidity readings as another service. In that case, the simple weather forecast service could be upgraded according to the fetched humidity readings from the first machine. The two machines would still be bonded by a single bidirectional connection, but the first machine would offer the second two services (data streams) instead of one.

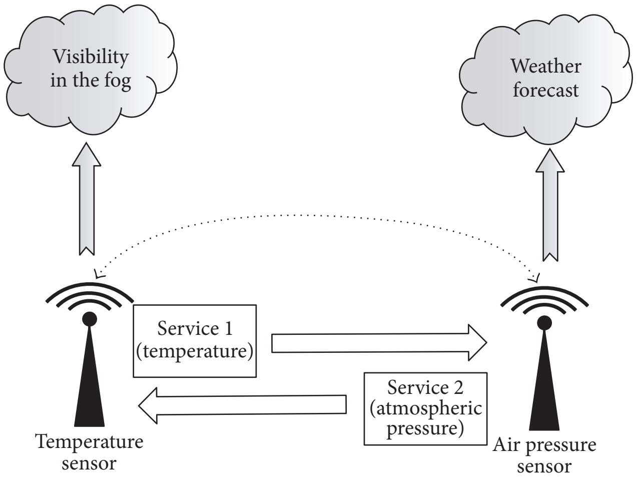


FIGURE 8: A bidirectional social connection between two machines.

However, if only one of the machines were to seek a permanent source of measured data stream (the other machine requested nothing in return), it would be a "machine Twitter" scenario.

In a "machine Twitter" scenario, two machines form a following-like (unidirectional) connection when one machine requires a "subscription" for the other machine's data. For example, one of the machines offers a complex service based on two sets of data: (i) the first data set which it generates itself and (ii) the second data set it acquires from another machine. After browsing the social machine network and finding the most suitable machine whose services include streaming its data to other machines, a bond is formed in which the first machine becomes the follower of the second. After that, the first machine starts receiving data streams in the manner as agreed during negotiations and policy agreements that preceded in establishing the connection. Figure 9 illustrates this specific scenario.

One of the machines (on the left) measures *air humidity*, while the other (on the right) measures *air temperature*. However, in this scenario, a service is to be established only in the machine that measures air temperature. For example, if the service was utilized for road safety so that it notifies drivers as to the presence of road ice, the temperature sensor data might be enough, but the service would be more precise if humidity data were also accessible. In browsing the social network, the temperature sensor finds the available humidity data stream service from the humidity sensor, and it then forms a *following*-like connection (one-way dotted line); that

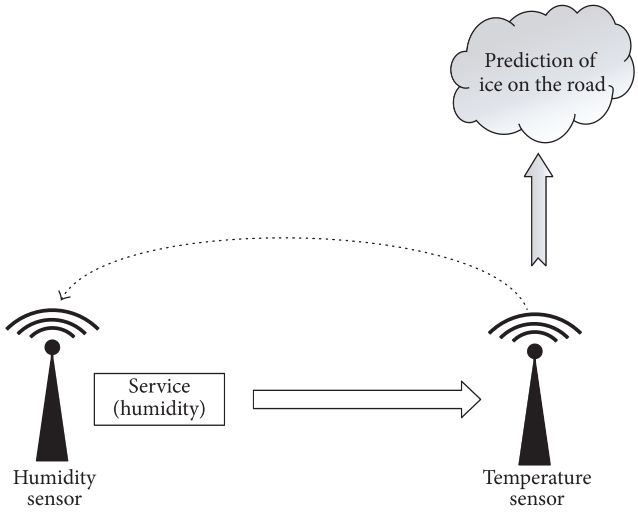


Figure 9: Unidirectional social connection of two machines.

is, it becomes a *follower* and subscribes to the humidity sensor's data stream. Similar to the *machine Facebook* scenario, the social connection is a logical feature supported by the platform and where multiple services can be hosted just like in Twitter for humans (e.g., retweeting content, marking content as favourite, and replying to content); only in this case, the services are defined and offered by sensors participating in the network.

5.3. Examples of Machine Social Networking. Most of the current IoT solutions have been built in isolation, which has led to fragmented and functionally limited small communities of heterogeneous smart objects that are disconnected from each other. In this case, there has been a clear lack of collaborative studies and developments towards interoperability, resulting in a significant barrier for the global proliferation of IoT ecosystems. Nevertheless, the solution describing the problems lies in enabling smart devices to communicate with the external world using common web protocols upon which the Internet is built, and only in this way can smart objects evolve to socially conscious objects. Examples of evolutionary steps in that direction are the web of things (WoT) [63] and Device Profile for Web Services (DPWS) [64, 65].

In the current evolutionary stage of machine social networking, a desirable feature is the capability that allows users and services to sense the physical world and act on it. One approach to this demand is creating a platform where objects are easily found, browsed, exploited, and composed. An example of such a platform is Pachube [66] (rebranded as Xively (http://www.xively.com/)) and the Ericsson platform [67]. Pachube emerged between 2007 and 2011 as a sensor data integration platform that was close to the idea of a social network of objects. It opened the IoT to end users and allowed developers to link sensor data to the web and build applications using the data. However, the objects were unable to form social connections and groups autonomously. Ericsson created a platform for the *social web of things*, which enabled interaction between humans and their home appliances in a blog fashion, but the appliances were still controlled by humans from their smart devices, meaning that control was not automated. Another similar project was SenseShare [68], the first proposal in giving social consciousness to objects. The platform used the Facebook social network to enable users to communicate their sensor data with their friends. Similar to Pachube, sensors were not able to communicate directly. The platform effectively acted only as a data store between sensors and clients.

A platform called Smart-Its Friends [69] was the first to establish pseudosocialization between objects; that is, it contained a prototype of the second evolutionary step (socially conscious objects) in the social networking of machines. Users were able to form social bonds between wireless smart sensing devices called Smart-Its. Another type of object that exhibits pseudosocial behaviour is the Blogjects, that is, objects that blog. The evolutionary step of social objects continues to be the subject of many studies. The most frequently mentioned term in research of that field is the *Social Internet of Things* (SIoT). In the SIoT concept [70, 71], establishing relationships among objects occurs similarly to establishing a human relationship. Devices in the same *neighbourhood* that are seeking a solution to a common problem hook up and find a mutual solution. SIoT research is investigating possibilities of integrating IoT and social networks. Social networks of objects are not human social networks that share the object as in the *res sapiens* evolutionary stage, nor are human social networks enhanced by the presence of these objects as in the *res agens* evolutionary stage. In these networks, establishing connections is not determined by the acquaintance of human owners. These networks offer services to humans by exchanging information through the social relationships that objects had previously established. However, there are still no actual proposals for architectural solutions or procedures for establishing social relations among objects.

6. Conclusion

Currently, network-aware machines in the form of Wireless Sensor Networks (WSNs) and Machine-to-Machine (M2M) prevail, but Cyber-Physical Systems (CPSs) are slowly becoming a reality. The ultimate goal in this evolution is creating the Internet of Things (IoT) and social networks among machines, allowing the entire system to establish the Social Internet of Things (SIoT) paradigm. The concept of socially connected machines poses questions such as how a machine will be represented in an M2M network, that is, what a machine profile will look like, what its "context awareness" and "network awareness" will imply, how they can be modelled, and what their impact is on the emergence of vertical applications and smart services. Parallel to the evolution of IoT is another evolution line in the making, and its goal is achieving Human-Agent Collectives (HAC). HAC and IoT are very similar concepts, but they differ on human involvement. While IoT strides towards almost absolute human exclusion, except for sensor carrying purposes, HAC is based on cooperation between humans and the system, even in data processing. However, both of these evolutions favour machines because they demand the development of machines. Consequently, regardless of which of these paradigms prevails or should they cohabit on equal footing, the future appears to be bright for machines.

Despite the possibility of a bright future, researchers still have a long way to go before machine social networks become a reality for businesses and society. Most network-aware machines still require great human effort for configuring and deploying applications. The human factor impedes large-scale deployment of the system in the field, as well as long-term sustainability. By embedding more autonomy and intelligence into these networks, that is, socially connected machine networks, the human factor could be eliminated almost completely. Nevertheless, there is a long way to go before achieving true social connectedness. One of the problems is the infrastructure, which is not optimized for machine-like communications. Another problem is fragmentation of the value chain for the IoT. The deployment of a value-added service, coordination, and compatibility of many technologies, hardware, software, supply chain, and service providers is necessary for a broad market. The solution to these problems lies partially in standardization, and efforts have been made in that direction, especially with the oneM2M initiative. Finally, the devices out in the field are also a part of the problem because they cannot be easily (and financially affordable) improved to offer new services due to their remoteness. In essence, the M2M concept is service-driven and requires devices to be extensible and to act as a platform for future services. Current devices generally lack the computing power and upgradeability for new services.

When all of this is taken into account, we identify three key open research challenges faced by machine social networking: (i) *heterogeneity* of smart machines, (ii) *applications* for social networking of machines, and (iii) *interfaces* for humans. In the forthcoming years, scientists from areas of Wireless Sensor Networks, Machine-to-Machine, Internet of Things, Cyber-Physical Systems, Human-Agent Collectives, and many other fields will need to work together to further pursue and build sustainable (from a technical, economic, and societal perspective) machine social networking systems.

Heterogeneity of (Smart) Machines. Machine social networks will be complex eco-systems consisting of thousands, millions, or even billions of interconnected machines. Although this brings up the requirement for scalable algorithms and mechanisms to implement such systems, the already designed human Web 2.0 approaches could possibly be replicated. The largest human Web 2.0 service today, the Facebook social network, has more than 1.6 billion active users and supports real-time dynamics of network interactions. Nevertheless, an important difference between Facebook today and a future machine social network of 1.6 billion connected devices is the fact that connected people are much more similar to each other than connected devices. All humans have the same functionalities (e.g., they can speak and write) and they differ only as to how their functionalities are implemented (e.g., which language(s) they speak and which alphabet(s) they use). As described in this paper, the differences between machines could be substantial in functionalities as well, which will increase remarkably the heterogeneity of social networks and challenge researchers to design new algorithms and mechanisms to preserve the scalability and robustness of such networks.

Machine Social Networking Applications. Human social networking services such as Facebook, Twitter, or Instagram are popular because of the applications built on top of them as platforms. For example, Facebook is today used for real-time communication (Facebook Messenger application) and as a news aggregator (Facebook Wall application), among other things. In 2004, when launching Facebook, Mark Zuckerberg certainly did not think that millions of people from around the world will be using Facebook as their cookbooks. Nevertheless, today almost 50 million people regularly prepare food using Facebook's Tasty recommendations (https://www.facebook.com/buzzfeedtasty). The way that human social networks have transformed World Wide Web services into Internet platforms in only a decade is fascinating. Due to machine heterogeneity, the theoretical possibilities of different machine social network applications are becoming even broader. However, these possibilities are still in the early stage of research and as such represent an exciting area for researchers.

Human Interfaces. Not only is the relationship between man and machine a hot topic among researchers, but businesses and governments are also very interested in the topic. Although some of leading scientists (e.g., Stephen Hawking) and entrepreneurs (e.g., Elon Musk) have expressed concerns that developments in smart machines "run" by artificial intelligence could "spell the end of the human race," researchers should direct their activities to creating systems where humans and machines are "partners." An important step towards this goal will be designing interfaces between machine social networks and humans or, more generally, enabling integration of machine social networks and human social networks. This challenge goes far beyond the technical domain of interconnecting humans and machines in a common ICT system and represents transdisciplinary research problem where expertise not only from technical but social (e.g., legal and psychological perspective) sciences is needed. The research on HAC, one of the paradigms analysed in this paper, is an example of research directed towards building sociotechnical systems that interleave humans and machines. However, it is only the beginning of what should be an exciting playground for transdisciplinary collaboration of researchers, businesses, and governments for at least the next decade.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

The authors acknowledge the support of the research project "Managing Trust and Coordinating Interactions in Smart Networks of People, Machines, and Organizations," funded by the Croatian Science Foundation under Project UIP-11-2013-8813, as well as research projects "Machine-to-Machine Communication Challenges (M2MCC)" and "A Platform for Context-Aware Social Networking of Mobile Users (SmartSocial)," funded by Ericsson Nikola Tesla, Croatia.

References

[1] D. Hussein, S. N. Han, X. Han, G. M. Lee, and N. Crespi, "A framework for social device networking," in *Proceedings of the 9th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS '13)*, pp. 356–360, Cambridge, Mass, USA, May 2013.

[2] D. Evans, "How the Internet of things Will Change Everything Including Ourselves," Web blog post. *Internet of Everything*. Cisco Blogs. May 2011–Sep. 2015.

[3] B. Emerson, "M2M: the internet of 50 billion devices," *Huawei Win-Win*, no. 4, pp. 19–22, 2010.

[4] M. Hatton and J. Morrish, "Press release—machine-to-machine connections to hit 18 billion in 2022, generating USD1.3 trillion revenue," *Machina Research*, December 2013.

[5] The Networking Exchange Blog Team, "The Emerging M2M Ecosystem—20 Billion Devices by 2020," Web blog post. *Networking Exchange Blog*, April 2011–June 2015.

[6] J. Rivera and R. van der Meulen, *Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units by 2020*, Gartner, Stamford, Conn, USA, 2013.

[7] G. Jelen, *Health Organizations in a Networked Society*, University of Zagreb Faculty of Electrical Engineering and Computing, Zagreb, Croatia, 2015.

[8] E. Brynholfsson and A. McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, W. W. Norton & Company, New York, NY, USA, 1st edition, 2014.

[9] Y. Chen and W. Wang, "Machine-to-machine communication in LTE-A," in *Proceedings of the IEEE 72nd Vehicular Technology Conference Fall (VTC-Fall '10)*, pp. 1–4, Ottawa, Canada, September 2010.

[10] S. Abdul Salam, S. A. Mahmud, G. M. Khan, and H. S. Al-Raweshidy, "M2M communication in smart grids: implementation scenarios and performance analysis," in *Proceedings of the IEEE Wireless Communications and Networking Conference Workshops (WCNCW '12)*, pp. 142–147, Paris, France, April 2012.

[11] 3GPP, "3rd generation parthership project; technical specification group services and system aspects; study on facilitating machine to machine communication in 3GPP systems; (Release 8)," Tech. Rep. TR 22.868 V8.0.0., 3GPP, 2007.

[12] J. M. Costa and G. Miao, "Context-aware machine-to-machine communications," in *Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS '14)*, pp. 730–735, IEEE, Toronto, Canada, May 2014.

[13] R. Ratasuk, J. Tan, and A. Ghosh, "Coverage and capacity analysis for machine type communications in LTE," in *Proceedings of the IEEE Vehicular Technology Conference (VTC 12)*, pp. 1–5, Yokohama, Japan, May 2012.

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

[15] D. Niyato, L. Xiao, and P. Wang, "Machine-to-machine communications for home energy management system in smart grid," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 53–59, 2011.

[16] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson, "M2M: from mobile to embedded internet," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 36–43, 2011.

[17] M. Chen, J. Wan, and F. Li, "Machine-to-machine communications: architectures, standards and applications," *KSII Transactions on Internet and Information Systems*, vol. 6, no. 2, pp. 480–497, 2012.

[18] E. Darmois and O. Elloumi, "Introduction to M2M," in *M2M Communications: A Systems Approach*, chapter 1, section 1.1, John Wiley & Sons, New York, NY, USA, 1st edition, 2012.

[19] S. Pandey, M.-J. Choi, M.-S. Kim, and J. W. Hong, "Towards management of machine to machine networks," in *Proceedings of the 13th Asia-Pacific Network Operations and Management Symposium (APNOMS '11)*, pp. 1–7, Taipei, Taiwan, September 2011.

[20] G. Steimel, "What are the drivers and obstacles in GSM-M2M market?" (German), M2M Alliance publications on M2M Beratung, 2006.

[21] D. S. Watson, M. A. Piette, O. Sezgen, N. Motegi, and L. ten Hope, "Machine to machine (M2M) technology in demand responsive commercial buildings," in *Proceedings of the Summer Study on Energy Efficiency in Buildings: Breaking out of the Box (ACEEE '04)*, pp. 351–363, Pacific Grove, Calif, USA, August 2004.

[22] Y. Chen and Y. Yang, "Cellular based machine to machine communication with un-peer2peer protocol stack," in *Proceedings of the IEEE 70th Vehicular Technology Conference (VTC '09)*, pp. 1–5, Anchorage, Alaska, USA, September 2009.

[23] *Trends in Machine-to-Machine Communications: Technology Scan and Assessment Final Report—October 2011*, Intelligent Transportation Systems Joint Program Office, United States Department of Transportation, 2015.

[24] I. Bojic, T. Lipic, and V. Podobnik, "Bio-inspired clustering and data diffusion in machine social networks," in *Computational Social Networks: Mining and Visualization*, A. Abraham, Ed., chapter 3, pp. 51–79, Springer, London, UK, 2012.

[25] M. Weiser, "The computer for the 21st century," *Scientific American*, vol. 265, no. 3, pp. 94–104, 1991.

[26] S. Poslad, *Ubiquitous Computing: Smart Devices, Environments and Interactions*, John Wiley & Sons, Chichester, UK, 2009.

[27] ETSI, "Machine-to-Machine communications (M2M); Definitions," Tech. Rep. TR 102 725 V1.1.1, ETSI, Sophia Antipolis, France, 2013.

[28] oneM2M, "oneM2M technical specification: common terminology (TS-0011-V1.2.1)," Tech. Rep. oneM2M-TS-0011-V1.2.1, oneM2M, 2015.

[29] P. Papageorgiou, *Wireless Sensor Networks—An Overview*, University of Maryland, College Park, Md, USA, 2003.

[30] J. Holler, V. Tsiatsis, C. Mulligan, S. Avesand, S. Karnouskos, and D. Boyle, "M2M to IoT—the vision: from M2M to IoT," in *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*, chapter 2, section 2.2, pp. 14–18, Academic Press, Oxford, UK, 1st edition, 2014.

[31] *Internet of Things Global Standards Initiative*, ITU: Committed to connecting the world, Geneva, Switzerland, 2015.

[32] J. Williams, "Internet of Things: Science Fiction or Business Fact?" Harvard Business Review Analytic Services Report, December 2014.

[33] Harbor Research, "Shared destinies: how the internet of things, social networks, & creative collaboration will shape future market structure," White Paper, Harbor Research, San Francisco, Calif, USA, 2009.

[34] M. Rouse, "Pervasive Computing (Ubiquitous Computing)," *IoT Agenda. IoT analytics guide: Understanding Internet of Things data*, TechTarget. December 2010, March 2016 .

[35] J. Lingli, "Smart city, smart transportation: recommendations of the logistics platform construction," in *Proceedings of the International Conference on Intelligent Transportation, Big Data and Smart City (ICITBS '15)*, pp. 729–732, Halong Bay, Vietnam, December 2015.

[36] J. Van Den Bergh and S. Viaene, "Key challenges for the smart city: turning ambition into reality," in *Proceedings of the 48th Annual Hawaii International Conference on System Sciences (HICSS '15)*, pp. 2385–2394, January 2015.

[37] Y. Wenbo, W. Quanyu, and G. Zhenwei, "Smart home implementation based on internet and WiFi technology," in *Proceedings of the 34th Chinese Control Conference (CCC '15)*, pp. 9072–9077, IEEE, Hangzhou, China, July 2015.

[38] R. S. H. Istepanian, "The potential of Internet of Things (IOT) for assisted living applications," in *Proceedings of the IET Seminar on Assisted Living*, pp. 1–40, London, UK, April 2011.

[39] B. Morvaj, L. Lugaric, and S. Krajcar, "Demonstrating smart buildings and smart grid features in a smart energy city," in *Proceedings of the 3rd International Youth Conference on Energetics (IYCE '11)*, pp. 1–8, Leiria, Portugal, July 2011.

[40] B. Chowdhury and M. U. Chowdhury, "RFID-based real-time smart waste management system," in *Proceedings of the Australasian Telecommunication Networks and Applications Conference (ATNAC '07)*, pp. 175–180, Christchurch, New Zealand, December 2007.

[41] M. Marjanovic, L. Skorin-Kapov, K. Pripuzic, A. Antonic, and I. Podnar Zarko, "Energy-aware and quality-driven sensor management for green mobile crowd sensing," *Journal of Network and Computer Applications Archive C*, vol. 59, pp. 95–108, 2015.

[42] A. Antonić, M. Marjanović, K. Pripužić, and I. P. Žarko, "A mobile crowd sensing ecosystem enabled by CUPUS: cloud-based publish/subscribe middleware for the Internet of Things," *Future Generation Computer Systems*, vol. 56, pp. 607–622, 2016.

[43] Y.-K. Chen, "Challenges and opportunities of internet of things," in *Proceedings of the 17th Asia and South Pacific Design Automation Conference (ASP-DAC '12)*, pp. 383–388, Sydney, Australia, February 2012.

[44] J. Holler, V. Tsiatsis, C. Mulligan, S. Avesand, S. Karnouskos, and D. Boyle, "M2M to IoT—the vision: implications for IoT," in *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*, chapter 2, section 2.3, pp. 30–31, Academic Press, Oxford, UK, 1st edition, 2014.

[45] R. Alur, *Principles of Cyber-Physical Systems*, The MIT Press, Cambridge, Mass, USA, 2015.

[46] S. Engell, "Cyber-physical systems of systems—definition and core research and innovation areas," Working Paper of the Support Action CPSoS, 2014.

[47] N. R. Jennings, L. Moreau, D. Nicholson et al., "Human-agent collectives," *Communications of the ACM*, vol. 57, no. 12, pp. 80–88, 2014.

[48] V. Podobnik and I. Lovrek, "An agent-based platform for ad-hoc social networking," *Lecture Notes in Computer Science*, vol. 6682, pp. 74–83, 2011.

[49] E. Kamar, Y. (Kobi) Gal, and B. J. Grosz, "Modeling information exchange opportunities for effective human-computer teamwork," *Artificial Intelligence*, vol. 195, pp. 528–550, 2013.

[50] R. H. Thaler and C. R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Revised & Expanded, Penguin Books, New York, NY, USA, 2009.

[51] Team Litmus, *Iot vs M2M: A Subset, Intersection or a Value Addition*, Litmus Automation, 2014.

[52] M. Pticek, V. Cackovic, M. Pavelic, M. Kusek, and G. Jezic, "Architecture and functionality in M2M standards," in *Proceedings of the 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO '15)*, pp. 413–418, IEEE, Opatija, Croatia, May 2015.

[53] S. Manley, "The social network of machines. Software-defined storage, & the data protection continuum," Reflections: EMC Executives Report from the Road, EMC^2 Reflections Blog, 2014.

[54] O. Vermesan, P. Friess, P. Guillemin et al., *Internet of Things Strategic Research Roadmap*, IERC Cluster SRA Publications, 2011.

[55] V. Podobnik, D. Ackermann, T. Grubisic, and I. Lovrek, "Web 2.0 as a foundation for Social Media Marketing: global perspectives and the local case of Croatia," in *Cases on Web 2.0 in Developing Countries: Studies on Implementation, Application, and Use*, pp. 342–379, IGI Global, Hershey, Pa, USA, 2013.

[56] V. Podobnik and I. Lovrek, "Transforming social networking from a service to a platform: a case study of ad-hoc social networking," in *Proceedings of the 13th International Conference on Electronic Commerce (ICEC '11)*, ACM, August 2011.

[57] V. Podobnik and I. Lovrek, "Implicit social networking: discovery of hidden relationships, roles and communities among consumers," *Procedia Computer Science*, vol. 60, pp. 583–592, 2015.

[58] J. Bughin, M. Chui, and J. Manyika, *An Executive's Guide to the Internet of Things*, McKinsey Quarterly, McKinsey & Company, 2015.

[59] K. D. Johnson, "Reinventing embedded devices for smarter services," *Connected Intelligence*, vol. 1, no. 1, pp. 38–39, 2012.

[60] Harbor Research, "The emergence of smart business: machine-to-machine (M2M) & smart systems forecast 2010–2014," Harbor Research Report, 2010.

[61] L. Atzori, A. Iera, and G. Morabito, "From 'smart objects' to 'social objects': the next evolutionary step of the internet of things," *IEEE Communications Magazine*, vol. 52, no. 1, pp. 97–105, 2014.

[62] V. Smailovic, D. Striga, and V. Podobnik, "Advanced user profiles for the smartsocial platform: reasoning upon multi-source user data," in *Web Proceedings of the 6th ICT Innovations Conference*, pp. 258–268, ICT-ACT, Ohrid, Macedonia, September 2014.

[63] S. Duquennoy, G. Grimaud, and J.-J. Vandewalle, "The web of things: interconnecting devices with high usability and performance," in *Proceedings of the International Conference on Embedded Software and Systems (ICESS '09)*, pp. 323–330, Zhejiang, China, May 2009.

[64] A. Sleman and R. Moeller, "Integration of wireless sensor network services into other home and industrial networks using Device Profile for Web Services (DPWS)," in *Proceedings of the 3rd International Conference on Information and Communication Technologies: From Theory to Applications (ICTTA '08)*, pp. 1–5, April 2008.

[65] G. Moritz, E. Zeeb, S. Prüter, F. Golatowski, D. Timmermann, and R. Stoll, "Devices profile for web services in wireless sensor networks: adaptations and enhancements," in *Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation (ETFA '09)*, pp. 1–8, IEEE, Mallorca, Spain, September 2009.

[66] P. Swabey, "Pachube opens the internet of things to end users," *Information Age. Vitesse Media*, 2011.

[67] J. Formo, *Ericsson User Experience Lab Blog*, Ericsson, 2012.

[68] T. Schmid, Y. Cho, and M. B. Srivastava, "Exploiting social networks for sensor data sharing with SenseShare," in *Proceedings of the CENS 5th Annual Research Review*, Los Angeles, Calif, USA, October 2007.

[69] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H.-W. Gellersen, "Smart-its friends: a technique for users to easily establish connections between smart artefacts," in *Proceedings of the International Conference on Ubiquitous Computing (Ubicomp '01)*, G. D. Abowd, B. Brumitt, and S. Shafer, Eds., vol. 2201, pp. 116–122, Springer, Atlanta, Ga, USA, 2001.

[70] L. Atzori, A. Iera, and G. Morabito, "SIoT: giving a social structure to the internet of things," *IEEE Communications Letters*, vol. 15, no. 11, pp. 1193–1195, 2011.

[71] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (SIoT)—when social networks meet the internet of things: concept, architecture and network characterization," *Computer Networks*, vol. 56, no. 16, pp. 3594–3608, 2012.