International Journal of Innovative
Computing, Information and Control
Volume **10**, Number **2**, April **2014**

ICIC International ©2014 ISSN 1349-4198
pp. 437–458

IMPLEMENTING SELF-ORGANIZING INFORMATION DISSEMINATION INTO NETWORK-CENTRIC MACHINE-TO-MACHINE SYSTEMS

Damjan Katusic and Gordan Jezic

Faculty of Electrical Engineering and Computing
University of Zagreb
Unska 3, 10000 Zagreb, Croatia
{ damjan.katusic; gordan.jezic }@fer.hr

Received December 2012; revised April 2013

Abstract. *This paper explores the convergence of Machine-to-Machine (M2M) systems with Network-Centric Operations (NCO), and analyzes the perspective of integrating self-organizing gossip protocols as an information dissemination solution. An overview of the M2M communication paradigm and current standardization efforts regarding architecture are given. The paper includes an overview of the network-centric networking and analyses the idea of implementing NCO approach to achieve situational awareness and self-synchronization of autonomous and intelligent M2M devices in networked M2M environments. Two case studies involving M2M systems are given and discussed as a proof of concept for the implementation of a network-centric approach. Properties of self-organizing systems are briefly analyzed, and gossip protocols are identified as a viable support solution for the proposed convergence.*
Keywords: Machine-to-machine, Network-centric operations, Self-organization, Information dissemination, Gossip protocols

1. **Introduction.** Machine-to-Machine (M2M) systems' rapid growth and development in recent years have attracted much attention. Numerous companies and network operators have established specialized M2M departments extending their businesses and providing new types of automated services. Ubiquitous wireless and wired connectivity, and declining prices of communication modules are the main drivers of such a trend. The potential for further growth of the M2M market is enormous: European Telecommunications Standards Institute (ETSI) suggests that the number of connectable machines is five times greater than the amount of humans, although the number of currently connected machines is still significantly lower. However, even today the number of connected M2M devices is measured in hundreds of millions. Harbor Research expects 390 million cellular M2M connections in 2014 [1], while Mobile Market Development predicts a projected compound annual growth rate of 25% through 2014, and approximately 50 billion M2M devices worldwide by 2025 [2]. Ericsson's predictions reach 50 billion M2M devices even sooner, by 2020 [3]. According to Juniper Research, M2M market as a whole, including both fixed and mobile technologies, will by 2014 reach value of nearly $35 billion [4].

Both leading M2M standardization bodies (ETSI and Third-generation Partnership Project (3GPP)) publish similar definition of the M2M communication: it is the communication between two or more entities with little or no direct human intervention [5,6]. Similar definitions can be found in numerous other publications, books or articles dealing with the same matter. From the functional point of view, a communication system based on M2M interactions typically comprises of geographically dislocated devices, communication channels that connect them and a platform for management functions. Actors in

such an environment can include broad range of communication capable devices: computers, mobile phones, tablets, but also variety of sensors, smart grid networks, embedded processors, industrial and medical equipment, and countless other devices. M2M technology offers various applications and a vast potential for future development of new types of applications. One of the unofficial divisions proposed in [7] identifies six application areas: building management, transportation and logistics, healthcare, local communities and public safety, energy, manufacturing, and industrial applications.

As stated in [8], M2M technology is based on the idea that a machine has more value when it is networked and that the network becomes more valuable as more machines are connected. Operation and control in large and dynamic M2M systems, as is the case with distributed systems in general, is still an emerging area of research. This paper extends the ideas suggested in [9] where the convergence of network-centric networking approach into machine-to-machine environments was discussed. Network-centric operation and control offers a scalable decentralized alternative to centralized control and its typical issues (scalability, traffic congestion ("bottleneck"), transmission delays, energy wastage, etc.) [10]. Enabling qualitative information management between communicating machines is the necessary prerequisite for information sharing ("bringing the right information to the right destination at the right time"), stimulating machine cooperation, and generally improving individual and collective machine operations. Effective information dissemination enables faster machine operations and ultimately better performance of the M2M system as a whole. Self-organization principles based on the natural systems provide an attractive approach for handling requirements in dynamic distributed environments, especially for those M2M systems that emphasize machine autonomy and cooperation.

This paper is organized as follows. In Section 2, we give an overview of the current standardization efforts in the M2M domain, while Section 3 brings prominent considerations in the area of M2M architectures, with the prospect of implementing device-to-device communication in standardized architecture layouts. Section 4 focuses on the integration of network-centric approach into an M2M system and discusses its potential importance for M2M communication, particularly information sharing between M2M devices. In Section 5, we give an analysis of two M2M scenarios in the context of analyzed network-centric networking. Section 6 brings an overview and a brief analysis of the bio-inspired self-organization principles that can be applied in a network-centric M2M environment, with particular focus on the gossip algorithms developed for scalable information dissemination and aggregation. Finally, Section 7 concludes the paper.

2. **M2M Standardization Efforts.**

Current networks are optimized for Human-to-Human (H2H) interactions and data transfer, and communication patterns in such systems can greatly differ from those in M2M systems. It is important that communication technologies evolve and develop capabilities to efficiently support both human and machine solutions without impairing their capabilities.

An M2M concept is not a revolutionary idea since it has been present in various forms over the years. Early 1990s witnessed the development of Supervisory Control and Data Acquisition (SCADA) systems [11]. These primitive industrial management and telemetry systems are usually perceived as precursors of modern M2M systems. They include many connected sensors from which they gather data. However, their biggest disadvantage is high cost because they are based on proprietary communication technologies. Unlike SCADA, M2M systems work with standardized technologies [8] and are independent of the used access in a wide range of possible wired/wireless network solutions (Digital Subscriber Line (DSL), Wi-Fi, ZigBee, Bluetooth, cellular, satellite, etc.).

Many standardization bodies, including mentioned ETSI and 3GPP, have recently engaged in M2M standards development: International Telecommunication Union – Teleco mmunication Standardization Sector (ITU-T), Institute of Electrical and Electronics Engineers (IEEE), 3rd Generation Partnership Project 2 (3GPP2) and Telecommunications Industry Association (TIA) [12]. Considering the positive impulse of M2M standardization activities in recent years and learning on the experiences of 3GPP, ETSI is currently joining six other major standardization organizations from around the world (Association of Radio Industries and Businesses (ARIB) in Japan, Alliance for Telecommunications Industry Solutions (ATIS) and TIA in the USA, China Communications Standards Association (CCSA) in China, and Telecommunications Technology Association (TTA) in South Korea) to form a global M2M partnership: oneM2M [13]. Its agenda is to encourage the development of a common M2M Service Layer that can be embedded within various hardware and software, and relied upon to connect a variety of devices in the field with M2M application servers worldwide.

ETSI produces globally applicable standards for Information and Communications Technology (ICT) including fixed, mobile, and radio communications, Internet, and other areas, and continually strives to improve collaboration with other research bodies [14]. In 2007, a new ETSI Technical Committee (TC) for developing standards for M2M communication (Table 1) has been established [15]. The group aims to provide an end-to-end view of M2M standardization. Their work regarding M2M technology has begun with standards that analyze different use cases: smart metering [16], eHealth [17], connected consumer [18], automotive applications [19], and city automation [20]. The objective is to cover enough prevailing use cases to ensure that all of the important requirements of M2M systems are identified so that the associated architecture work provides the foundation for future M2M applications. Anyhow, they have also put some effort into defining basic M2M terminology [21], as well as its service requirements [5] and functional architecture [22]. ETSI's cooperation with other organizations has also resulted in few published standards. They closely co-operate with the work of the 3GPP [23] and 3GPP2 [24] standards initiatives for mobile communication, then with Open Mobile Alliance (OMA) [25] and Broadband Forum (BBF) [26] regarding their solutions for remote management, and with the ZigBee Alliance on the subject of interworking with their area networks [27].

3GPP produces highly successful reports and specifications that define 3GPP technologies, from Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), and Enhanced Data rates for GSM Evolution (EDGE) towards Universal Mobile Telecommunications System (UMTS), and recently Long Term Evolution (LTE) [28]. Most of its M2M (to avoid possible confusion it is important to mention that 3GPP uses term Machine-Type Communication or abbreviated MTC) standardization efforts (Table 1) are conducted within several Service and System Aspects Working Groups (SA WG): SA WG1[1], SA WG2[2] and SA WG3[3]. WG1 focuses on services [6,29-32], WG2 on architecture [33], and WG3 on problems regarding security [34,35]. Two additional groups are actively working on the improvements for radio access networks: GSM EDGE Radio Access Network (GERAN) WG2[4] on protocol aspects of GPRS/EDGE networks [36], and Radio Access Network (RAN) WG2[5] on Layer 2 and Layer 3 Radio Resource specification [37].

[1]TSG SA WG1 Services, http://www.3gpp.org/SA1-Services
[2]TSG SA WG2 Architecture, http://www.3gpp.org/SA2-Architecture
[3]TSG SA WG3 Security, http://www.3gpp.org/SA3-Security
[4]TSG GERAN WG2, http://www.3gpp.org/GERAN-2-Protocol-Aspects
[5]TSG RAN WG2, http://www.3gpp.org/RAN2-Radio-layer-2-and-Radio-layer

Table 1. ETSI and 3GPP M2M standards

Standardization body	***Description***	***Specification reference***
ETSI	*M2M Service Requirements*	*TS 102 689*
	M2M Functional Architecture	*TS 102 690*
	Smart Metering Use Cases	*TR 102 691*
	M2M Definitions	*TR 102 725*
	eHealth Use Cases	*TR 102 732*
	Connected Customer Use Cases	*TR 102 857*
	City Application Use Cases	*TR 102 897*
	Automotive Applications Use Cases	*TR 102 898*
	M2M Interfaces mIa, mId, dIa	*TS 102 921*
	Impact of Smart Grids on M2M Platform	*TR 102 935*
	Interworking with 3GPP Networks	*TR 101 603*
	Interworking with 3GPP2 Networks	*TR 103 107*
	Interworking with M2M Area Networks	*TR 102 966*
	OMA DM Compatible Objects	*TS 103 092*
	BBF TR-069 Compatible Data Model	*TS 103 903*
3GPP	*SA1 – M2M Study Report*	*TR 22.868*
	SA1 – MTC Service Requirements	*TS 22.368*
	SA1 – Alternatives to E.164 for MTC	*TR 22.988*
	SA1 – Man-machine Interface of the Mobile Station	*TS 02.30*
	SA1 – Man-machine Interface of the User Equipment	*TS 22.030*
	SA2 – System Improvements for MTC	*TR 23.888*
	SA3 – M2M Security Aspect for Remote Provisioning and Subscription Change	*TR 33.812*
	SA3 – Security Aspect of M2M	*TR 33.868*
	3GPP Study on RAN Improvements for MTC	*TR 37.868*
	3GPP Study on GERAN Improvements for MTC	*TR 43.868*

3. **M2M System Architecture Considerations.** Broad market potential of M2M systems is consequence of their numerous possible applications and use cases, as well as the variety of available access technologies that can be used in their implementation. These systems need to be reliable, scalable, secure, and manageable. The easiest way to accomplish this, and to solve set of unique challenges that differentiate them from H2H systems (large number of connected devices, specific traffic patterns, many types of devices, small energy requirements, etc.) is standardization. One of its main aspects is consideration regarding architecture of M2M systems.

3.1. **ETSI architecture standardization approach.** ETSI TC M2M published in [22] high-level architecture concept for M2M application support (Figure 1). It includes network (*Access Network*, *Core Network*, *M2M Service Capabilities*, *M2M Applications*, *Network Management*, and *M2M Management Functions*), and device and gateway domains (*M2M Devices*, *M2M Gateway*, and *M2M Area Network*, including *M2M Applications* and *M2M Service Capabilities*). M2M Devices include broad range of devices cited in the introduction, run M2M Application(s) using M2M Service Capabilities, and are capable to autonomously (without human intervention) exchange data with other devices. They connect to network domain in two different ways: directly or through M2M Gateway which serves as a network proxy. M2M Gateway using M2M Service Capabilities to ensure M2M Devices are interworking and interconnected to the underlying communication

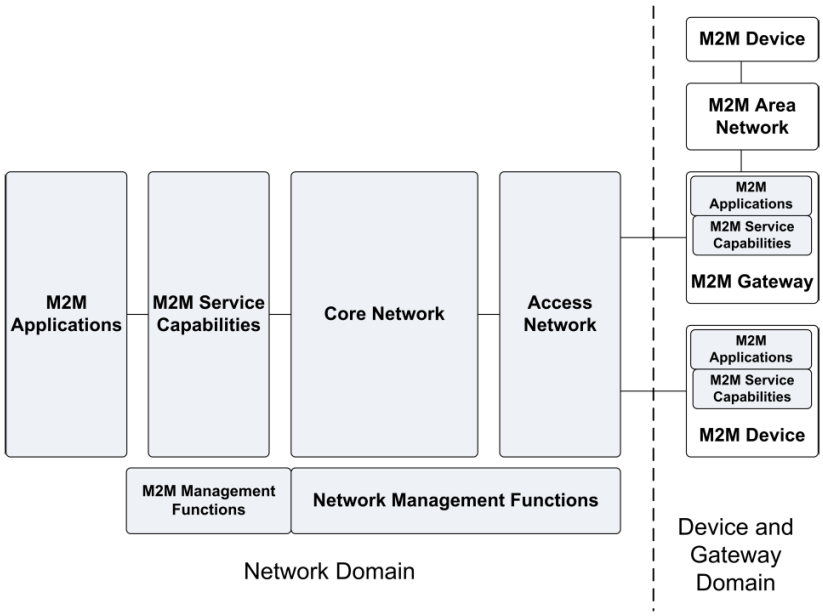

FIGURE 1. ETSI M2M system architecture

network, and can provide various services to them. M2M Area Network connects gateway and devices that lack service capabilities and are not capable to directly connect to Access Network. Network Domain comprises of Access and Core Networks, enables communication between M2M Gateways and M2M Applications, and includes Network and M2M Management Functions. Access Networks include (but are not limited to): DSL, satellite, GERAN, Universal Terrestrial Radio Access Network (UTRAN), evolved UTRAN (eUTRAN), Wireless Local Area Network (WLAN), and Worldwide Interoperability for Microwave Access (WiMAX). Core Networks (CN) include (but are not limited to): 3GPP CNs, ETSI Telecoms and Internet converged Services and Protocols for Advanced Networks (TISPAN) CN, and 3GPP2 CN. M2M Applications run the service logic and use M2M Service Capabilities accessible via an open interface.

There are three reference points between various node pairs (M2M Device, M2M Gateway, and Network (e.g., Application Server)) that define ETSI M2M functional architecture framework (Figure 2):

- The mIa reference point offers generic and extendable mechanism for Network Application (NA) interactions with the Network Service Capabilities Layer (NSCL).
- The dIa reference point offers generic and extendable mechanism for Device Application (DA)/Gateway Application (GA) interactions with the DSCL/GSCL. When between DA and GSC, typically over an Internet Protocol (IP) network, it is implemented over Constrained Application Protocol (CoAP) or Hypertext Transfer Protocol (HTTP).
- The mId reference point, between SCLs (DSCL/GSCL to NSCL), offers generic and extendable mechanism for SCL interactions. When between GSC and NSC, it is implemented over HTTP or Session Initiation Protocol (SIP).

It can be observed from the figure that M2M Device connects to Network Domain either directly (includes Service Capability Layer) or through the M2M Gateway (lacks SCL). ETSI so far in its standards does not assume direct device-to-device communication scenario (apart from the local interactions inside the M2M Area Network), but every communication involves Network Domain and associated servers who are then responsible for providing connectivity and/or other services to M2M Gateway(s)/Device(s).

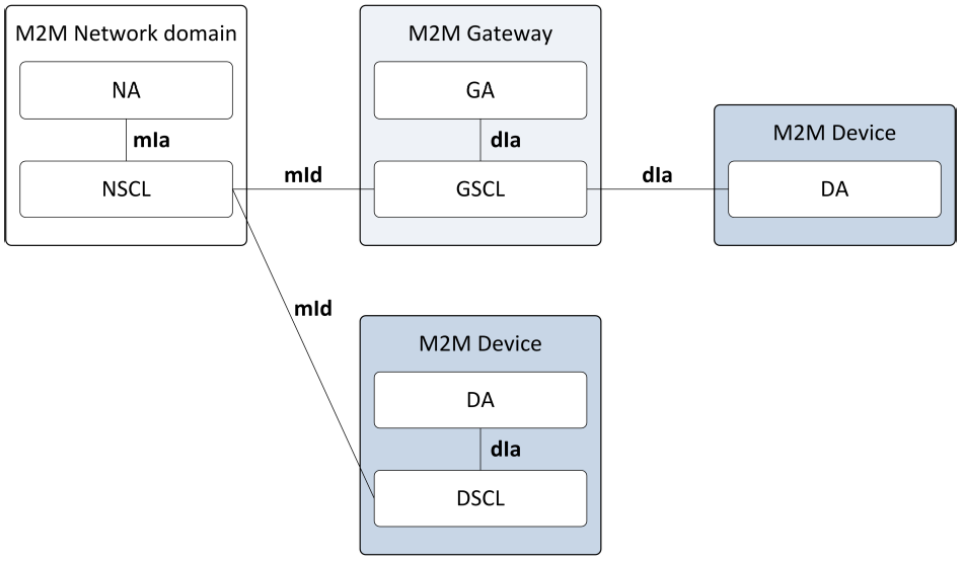

FIGURE 2. M2M functional architecture framework

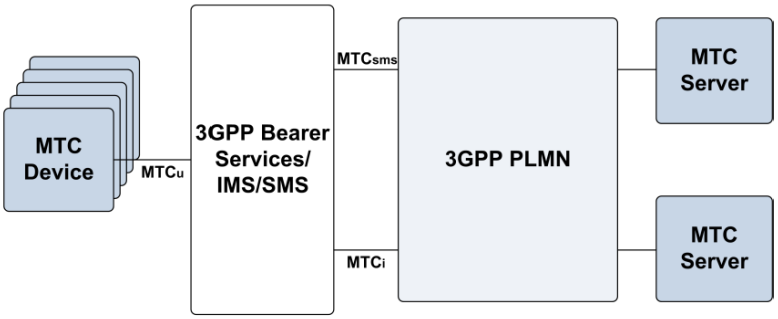

FIGURE 3. 3GPP M2M system architecture

3.2. **3GPP architecture standardization approach.** Recent developments in wireless industry such as widespread availability of wireless connectivity, declining prices of M2M modules, and regulatory incentives for certain industries (smart grid, e-Health) have attracted attention of potential M2M stakeholders [12]. With the merit of providing higher-layer connections, 3GPP network scenarios have been regarded as one of the most promising M2M solutions [11].

MTC Device comprises of variety of devices mentioned in the introduction and connects via MTC_u interface to the 3GPP network (GERAN, UTRAN, eUTRAN, etc.). Depending on the used access technology, MTC_u can be based on one of the following interfaces: U_u, U_m, W_w or LTE-U_u. The 3GPP network provides transport and communication services (including 3GPP bearer services, IP Multimedia Subsystem (IMS), and Short Message Service (SMS)) optimized for the MTC communication that connect MTC Device with an MTC Server or other MTC Devices. The MTC Server connects to the 3GPP network via MTC_i/MTC_{sms} interface and thus communicates with MTC Devices [29] (Figure 3).

There are three scenarios regarding the communication between MTC Servers and MTC Devices [6]. MTC Device indicates wireless MTC modules and terminals connected via an access network, included in the "machines in the field" domain. MTC Server stands for central servers that communicate with MTC Devices, and can be located inside or outside Mobile Network Operator (MNO) domain, or within public Internet. First communication scenario involves MTC Devices, distinguishable from each other, communicating with one

MTC Server (N to 1), while in second scenario there are several MTC Servers and several MTC Devices (N to N). In first scenario, one MTC module communicates with one server only, while second scenario involves more servers for load distribution. Third scenario consists of MTC Devices communicating directly with each other without the intermediate MTC Server. The latter scenario is not seen as the relevant within the scope of 3GPP's work on M2M, because most popular use cases involve some kinds of M2M device-to-server communication. Therefore, 3GPP and ETSI seem to have a rather similar standpoint regarding Machine-to-Machine communication between devices without intermediaries, and leave this area open to further discussion and research. However, there is no doubt that certain methods and principles, such as the ones discussed in the following chapters (e.g., network-centric approach), may greatly improve specific M2M applications.

4. **Network-Centric Approach in M2M Systems.** M2M systems are due to their diversity still faced with information management and coordination challenges. They can consist of various types and numbers of devices, local or wide area coverage, different level of mobility, autonomy, intelligence or energy constraints. Information management in such an environment that can be based on one of the two basic types, centralized or decentralized. Centralized information management system is continuously examining the environment using its sensor capabilities, transmitting the gathered data to the central node (M2M/MTC Server) for processing, and eventually decision making. Commands are distributed from centre to the edges [10]. This approach is correlated to the M2M/MTC Device(s)-M2M/MTC Server(s) 3GPP scenarios. In decentralized information management approach, inherent in the NCO principles, control and intelligence is shifted from one node to the whole network [10], or as it is in [38] called, "infostructure". The decentralization of control and intelligence among many nodes allows processing of gathered data within the network, which is in relation to the M2M/MTC Device-M2M/MTC Device 3GPP scenarios. NCO features motivate the idea of integrating some of its concepts in the perspective area of machine type communications.

4.1. **Network-centric operations.** Network-Centric Operations (NCO) refer to a continuously evolving, complex community of people, devices, information, and services interconnected by a communications network in order to optimize resource management and provide superior information on events and conditions needed to empower decision makers [39]. The term "network-centric" is attributed to the U.S. Admiral Jay Johnson who used it to describe what he has seen as a "fundamental shift from platform-centric warfare to network-centric warfare" [38]. Network-centric operations approach is in direct opposition to platform centricity, it shifts from viewing actors as independent to viewing them as part of a continuously adapting ecosystem, and emphasizes the importance of making strategic decisions to adapt or even survive in such a changing environment [38,40]. Its underlying framework has been influenced by certain command and control processes characterized by an iterative sequential series of steps, such as Observe, Orient, Decide and Act (OODA) loop cycle attributed to former United States Air Force (USAF) Colonel John Boyd, a model consisting of sense, process, compare, decide, and act steps, developed by Dr. J. S. Lawson, and the Headquarters Effectiveness Assessment Tool (HEAT) process developed by Dr. R. E. Hayes in 1984 [40].

Network-centric (sometimes also referred to as information-centric or knowledge-centric) approach seeks to achieve an information advantage, enabled in part by information and communication technologies, into a competitive advantage through the robust networking. Specifically, the NCO concept contains the following four tenets, as proposed in [41]:

- A robustly networked force improves information sharing.

- Information sharing enhances the quality of information and shared situational awareness.
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command.
- These, in turn, dramatically increase work (mission) effectiveness.

These tenets can be, with certain adjustments, applied to any networked environment. For a success, especially in a dynamic environment, it is critical to achieve information sharing that enables shared situational awareness and self-synchronization. This, simply speaking, means to deploy as much information about relevant aspects of the networked environment (e.g., the position and availability of critical resources, status of neighboring nodes, position of link/node failures, traffic congestions.) to nodes that need to know it in order to achieve better work performance in a dynamic distributed environment.

4.2. **Network-centric operations in M2M systems.** NCO paradigm described in the previous section mentioned several important features. However, despite the necessary technological basis that allows all of these features to fit together, the most important variable is behavior of a decision maker and its ability to make use of acquired information and knowledge. People, characterized by their cognitive processes and abilities, as well as their social interactions and organization, are the final destination of almost all of the acquired information and knowledge through networking. NCO results are ultimately driven and evaluated by human reasoning. Nodes in a network-centric environment are autonomous decision making units that can collaborate with other nodes (serve other units or be served by them). Some machines in M2M environment are capable of same type of behavior: function autonomously, without the direct human intervention, and are characterized by different cognitive and learning abilities. In such an environment they do not only support the network to process data for human decision makers, but are at some level decision makers themselves. They are driven to adapt to changes in their environments and reach goals through autonomous social interactions with other machines and autonomous decision making.

Information sharing. Information exchange is an important aspect of any networked environment. Nodes (i.e., people, connected machines) collect information through interactions with other nodes and use it to solve operational tasks and enrich their own knowledge. M2M systems with potentially large number of nodes offer large quantities of information that can be used for their own benefit. Establishing collaboration between connected machines assumes a bit more than interoperability, which is a fundamental technical ability to communicate. It is defined on a more abstract level than protocols that allow communication and adds semantic layer to the data that is being exchanged, encouraging "meaningful" conversations to take place. Semantic description of both data and networked M2M machines that exchange it is the first step to establishing machine autonomy and collaboration, although human level of thinking and understanding of exchanged knowledge will not be achieved for years to come. Standardization in M2M systems has started in this area as well [42], and it will be interesting to see how connected M2M machines, despite the fact that many of them are constrained by their processor and memory capabilities, will be able to "talk" and understand each other.

Further insight into the importance of information sharing is provided by Metcalfe's Law, which describes the potential value of a network. It states that as the number of nodes in a network (n) increases linearly, the potential "value" or "effectiveness" (v) of the network increases nonlinearly as the square number of nodes [40] (Figure 4). The source of potential network value is a function of the interactions between the nodes. For every $n = N$ nodes in a network, there are $N - 1$ potential interactions between them.

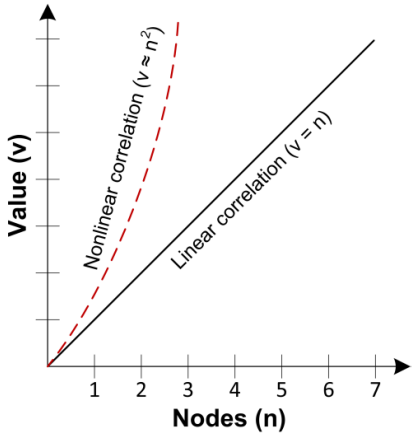

FIGURE 4. Metcalfe's law

Therefore, the potential value of the network is: $v = N \times (N-1) = N^2 - N$. For large N, the potential value scales with $v = N^2$.

Therefore, more nodes mean more information that can be used to achieve set goals. The NCO paradigm was devised in the first place to allow human users to extract qualitative information from the networked environment for better decision making. Situation is the same if M2M devices are the decision makers: network-centricity implies the necessity for better information connectivity between M2M network nodes in such an environment. There are numerous approaches for implementation of a decentralized information dissemination system, and some suggestions are going to be proposed in the following chapters of this paper.

Self-synchronization. Self-synchronization is the notion that highly complex groups, with accurate detailed information available at all levels, organize naturally (and optimally) from the bottom-up [43]. The term self-synchronization proposed in the network-centric literature is closely related to the more general term of self-organization which describes the class of processes that occur in a variety of different systems, and are all characterized by the bottom-up arising order through local interactions between the components of the system. Such an organizational principle is inherent in many aspects of human societies or numerous animal groups (e.g., ant colonies, swarms, flocks of birds), and can also be achieved in M2M systems. Then it creates new operational capabilities (machines are able to make decisions based on information gathered through sensors, from other machines, from databases, etc.) through autonomous cooperation of machines and allows better decision making.

Decision making. Finally, the last important aspect of NCO, and the desired consequence of all mentioned features, is the smart decision making. It implies that a node in a networked environment has access to underlying information and that it uses it for conducting both regular or out of the ordinary work activities. Human societies are accustomed to hierarchical organization and highly-centralized top-down commands. NCO changes that notion and pushes shared situational awareness to the edge of the network. This disrupts traditional practices in top-down command and control environments, especially military [44], which is in fact one of the pioneers of NCO research. Firstly, information non-attribution reverses the assumption that commands are issued from an individual entity to a particular individual entity: they are issued to a pool with rather undefined responsibilities. Secondly, as a consequence of such decentralization, decision making is migrating to the edges of a network, giving access to information of quality and quantity that is potentially equal to or better than that available at the centre. US

Army's restructuring into smaller units, such as formation of Stryker brigades [45], is on evidence that even strict hierarchical human organizations have started to accept benefits of such an approach. Decentralization can also be applied in M2M environment, nevertheless ETSI and 3GPP either so far prefer architectures with servers who act as the central points of control over the group of connected machines. Such an approach will allow machines to enrich their capabilities and achieve full utilization of the information available in the system. One of the main prerequisites for accomplishing this is an implementation of a robust information grid within the M2M system that fosters cooperation and allows sharing of structured data, information, and knowledge.

5. **Case Study: Network-Centric M2M Scenarios.** This chapter brings forward the analysis of integration of network-centric ideas into two possible M2M scenarios.

Healthcare M2M systems will be according to projections in [1] one of the main market drivers of the global M2M growth in the following years. Healthcare is an information rich and knowledge intensive environment, and in order to treat and diagnose even a simple condition, a physician must combine many varied data elements and information [46].

The analysis of the first scenario presumes that the architectural framework of the observed M2M e-Health scenario is largely based on the ETSI Remote Patient Monitoring model drafted in [17], with the inclusion of 3GPP cellular network as its underlying network access and core solution. Such a system includes remote patient monitoring M2M Devices connected via a Home Hub which acts as an M2M Gateway to the clinical side. Patient device gathers patient measurements, which may be communicated each time device gathers data, accumulated measurements may be communicated periodically (e.g., hourly or daily), or data may be delivered upon request or upon certain events. Clinical side involves care coordinator M2M services that monitor received patient data (M2M Server), and if measurements indicate that there has been a change in the patient's health status, or fall outside of a predetermined range, they alert clinician personnel (physician, nurse, etc.). This study for the more complete e-Health picture also involves some other healthcare stakeholders that are not crucial for the remote monitoring case, such as pharmacy and healthcare insurance (Figure 5).

Presently, many existing M2M e-Health initiatives represent distinctive and loosely connected entities whose operation is still largely platform-centric, that is, concentrates on the operations of a single subsystem (platform) with too little regard for the operational

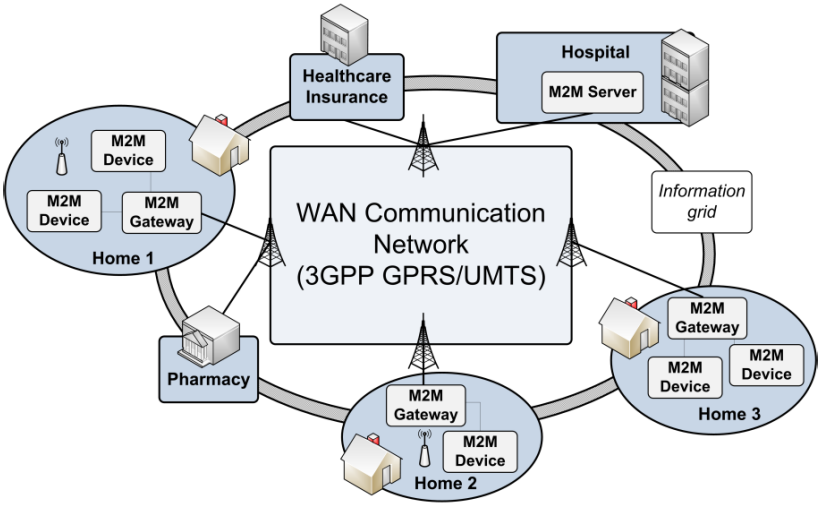

FIGURE 5. M2M-NCO e-Health scenario

interaction among different subsystems. The basic service of remote patient monitoring with remote M2M Devices and a central M2M Server is set up properly, so there is no need to change such an architectural decision. However, the inclusion of network-centric operations could improve analyzed scenario, stimulate better cooperation between various actors in such an environment (e.g., M2M remote monitoring devices, M2M Gateways, databases that maintain local measurement records), and include new types of services (e.g., automatically order new batch of medicines from pharmacy when current reserves become exhausted) without the need for an inclusion of a server side.

Second analyzed scenario involves a rather plausible system of M2M Devices equipped with various sensors scattered on a farming field. They could be used for measuring various farming relevant parameters such as soil temperature, moisture, chemical composition of the soil, and reporting it to the M2M coordinator service (M2M Server). One of the main prerequisites in such a system is the simplicity of its M2M end-devices, especially in the context of energy efficiency. Obviously, devices that would be put in soil should not be too big in dimensions, and they would need to be able to operate for a reasonable amount of time. Switching batteries is almost not applicable in this situation, and sensor capabilities that are the basis of a solution already consume an important part of available energy. The communication segment should be carefully designed: M2M Devices that are scattered on a possibly large field need to be able to establish a communication to server, gateway and each other. Solutions such as satellite or mobile cellular networks that offer large coverage are a possibility, but one has to take into account the energy cost. Also, fields can be located on remote and hardly accessible terrains with poor communication infrastructure that could have problems in supporting a very large number of end-devices. Nearby M2M Gateways would like in the previous scenario serve as proxies to the server side, and could be equipped with such communication technologies because they are not constrained as the end-devices. Next possibility is usage of Personal Area Network (PAN) ZigBee M2M modules. Such a solution is cheaper in the context of battery consumption than the latter proposals, especially when taking into account possibly large number of connected M2M end-devices. ZigBee offers a rather small coverage area, but end-devices can establish a mesh network between them that would support local interactions and eventually a connection to gateway, while gateway would be responsible for establishing the connection to the M2M Server (Figure 6). Each M2M Device is able to connect directly to its neighbors (full line), and indirectly to all other nodes (broken line). Each end-device serves as a relay for all other end-devices.

Farm field M2M scenario is very similar to the e-Health scenario described above. However, there are several important differences, apart from the fact that they are tied to different application domains. Cooperation between end-devices without the intermediary is because of the nature of used technology a necessity even for simple operations such as an exchange of data (e.g., between source and destination M2M Devices highlighted in Figure 6). This scenario is based on an ETSI proposed M2M Area Network template, and is still in accordance with its proposed architecture described earlier in the paper. However, it also offers a very good insight into the limitations of current ETSI and 3GPP standards: if observed sensors are replaced with a bit more complex M2M end-devices they would not fit in the proposed architectural models, i.e., current standardization efforts would not be able to properly explain and analyze them. It is important to emphasize that certain M2M services operate in a dramatically different way. Therefore, apart from the described M2M e-Health system where a network-centric networking, although not a completely natural fit, offers enrichment of the current system's operations, there are also M2M systems with inherently decentralized organizations that are so far mostly ignored by the standardization and would benefit even more from the inclusion of NCO ideas.

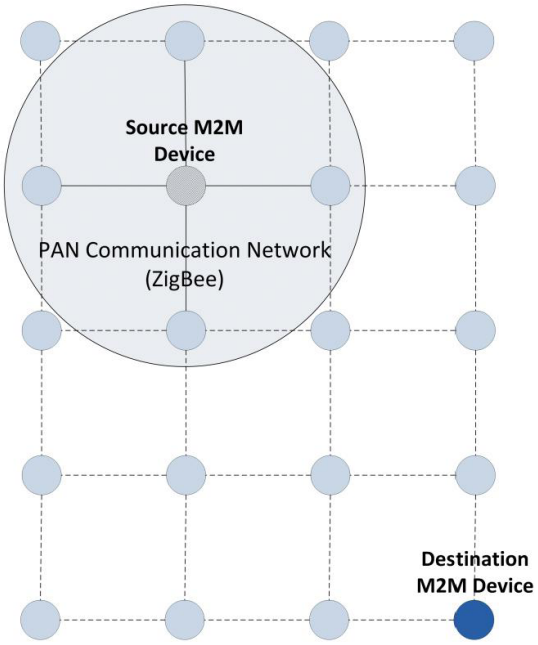

FIGURE 6. M2M farm field scenario

Mentioned platform-centricity has major influence on the access range and sharing of information stored among (or even within) the existing individual subsystems, and calls for another approach: implementing a network-centric system that facilitates information sharing among all participants within the operational space. Such an approach proposes the creation of an information exchange grid that will allow free flow of information, in observed cases among healthcare actors or sensors on a large farming field. This approach pushes critical information and shared situational awareness to nodes that need it to successfully accomplish tasks, no matter where are they located in the network.

Satisfying "right information to the right place at the right time" concept is not a trivial task. M2M systems are possibly heterogeneous and dynamic environments that could greatly benefit from the establishment of a network-centric and collaborative information management system. There are few important capabilities that such system should support: universal access to information (from a variety of sources), orchestrated information bus (that connects all M2M Devices and possibly aggregates, filters, and prioritizes information delivery), continuous adaptation to changes (to dynamic network topologies, M2M system membership changes, etc.), and support defined QoS policies and mechanisms [47].

6. **Self-Organization.** Self-organization has been a subject of numerous discussions and research since the time of ancient Greece. Various philosophy schools, and later branches of natural or social sciences have tried to introduce a precise definition of self-organization. Intuitively, self-organization refers to the autonomous arrangement of parts of a system in a non-random way. It is a result of local interactions and internal constraints that are not influenced or controlled by anything outside the system. As a result of these non-deterministic and local interactions occurs a phenomena known as emergence. Emergent phenomena as an externally (outside of a system) observable outcome can appear in the form of a particular pattern, property or a behavior. Although it can include rather complex patterns and behaviors, typically it is a result of simple interactions that occur within a system and without any apparent central control. Self-organizing systems are

encountered in many application areas, and because of the interesting properties they demonstrate, today they are a subject of numerous scientific efforts.

6.1. **Properties of self-organization.** Self-organizing systems are characterized by a number of mandatory and optional properties that define them [48]. Three mandatory properties are:

- Global organization: Process of self-organization brings system into relatively stable state in which it performs its functions. The resulting state can be either static or stationary. Static case presuming resulting organization positions in a system is fixed, while in the latter (stationary) case organizational components continuously change their position, but according to some ordered and stable pattern.
- Dynamic adaptation: Self-organizing systems are capable of dynamically reorganizing their organization in order to adapt to changes either in their functions or the conditions they face from the environment.
- Lack of external control: The dynamic reorganization and resulting order mentioned in the last entry is executed endogenously, i.e., without any external control.

Example of the static global organization is a fixed light bulb which serves its purpose of bringing light to the room when needed. Typical example of a stationary system are Benard cells [49] where pattern remains stable as long as the heating and cooling of the liquid are not altered, so an upward flow of the liquid on one side and a downward stream on the other side are in balance. Dynamic adaption is very clearly demonstrated in the example of insect populations that collect food, and behave differently according to the environmental conditions around them. Before mentioning some of the optional properties of self-organization, especially those important in the context of network-centric networking approach, it is important to distinguish its two subtypes: strong and weak self-organization. Strong self-organization systems' decisions are distributed among system components without any central control loop. Linking this discussion to the previous chapters, such properties can be achieved in systems that are so far outside of the current standardization efforts of ETSI and 3GPP, but we feel obliged to warn about their unattended potential. Weak self-organized systems, from an internal point of view, achieve self-organization as a consequence of a centralized planning and control. Scenario about M2M sensors distributed on a farm field is a very good fit for the latter. Although certain aspects of a system, such as its edge (area network of sensors) are decentralized, system as a whole still involves centralized control in a form of gateway(s) and server(s). Apart from the mandatory properties that determine if a system is self-organized, there are several other characteristics that can appear in it and determine its very important properties [48]:

- Nonlinearity and complex interactions: Self-organizing systems commonly display complex and nonlinear behavior that cannot be understood by separately examining its components. Such a nonlinear dynamics enables them to better adapt to a larger range of environmental conditions, and even a small fluctuation can cause a significantly different final result. Nonlinear systems' behavior can be achieved by adding up the nonlinear behaviors of the individual components of the system. An example of numerous water pipes flowing water into an irrigation bin is a good visualization. Each of them is characterized by a nonlinear behavior, which ultimately results that the overall flow of the system also exhibits nonlinear properties.
- Decentralized control: This property has already been discussed in the context of weak and strong self-organization. To summarize, in weak systems self-organization is a product of central control, while in the strong ones control is distributed over the whole system.

- Simple behaviors and local interactions: This property is one of the main reasons why self-organized systems are getting so much attention. It means that system components with simple behaviors, local interactions, and limited perception abilities (components do not have global view of the system, but rather local view with several of its neighbors) are able to achieve significantly more complex results. For example, molecule in the mentioned Benard example influences only several of its neighboring molecules it collides with.
- Robustness, resilience: Self-organizing systems consisting of large number of components can be robust, i.e., immune to errors or perturbations from the environment. If one ant is removed from the colony, the result of harvesting food will nevertheless be the same. Reason for robustness is a redundancy inherent in such systems, because the remaining components of the system cover for the ones that failed.
- Emergent properties: The emergent outcome of the system self-organizing processes can be a structure, pattern, behavior, or some other system properties that cannot be reduced to its basic elements. In the Benard example, resulting cells are created as a result of a direction of molecules' rotation. This emergent property cannot be observed in independent molecules.

6.2. **Self-organization in biological systems.** The focus of this paper are certain self-organizing principles observed in natural systems, particularly biological systems. Natural systems are dictated by nature in contrast to business and economic systems which are governed by business and market laws, and can be broadly divided into physical systems, biological systems, and social systems [48]. Research field that investigates models and methods inspired by nature is usually termed as natural computing. This highly interdisciplinary field connects biology and computing science, especially in terms of information processing.

The study of self-organizing systems has been initiated in 1953 with the work done by P. P. Grassé [50]. He studied insect societies and found out they achieve order without any central point of control. Self-organizing properties have over time been observed in many natural systems, from insect colonies to flocks of birds and schools of fish, and they have inspired solutions to many practical problems. S. Camazine et al. in [51] provide many outstanding examples of such self-organization in biological systems. Foraging ants [52] that explore their environment and seek food can be used to find the shortest possible path given the environmental constraints. Swarms find their appliance in fixed and mobile networks systems management [53], routing and load balancing [54], or security [55]. Self-organization in Peer-to-Peer (P2P) and Mobile ad hoc Network (MANET) including gossip-based overlay topology management [56] or decentralized techniques for routing, updates, and identity management are proposed in [57]. Network coordination problems have been solved using techniques inspired by swarm-based models [58] or mimicking insect foraging behavior [59]. Self-organizing sensor networks are used in numerous civil and military applications, and recent research in this area focuses on routing, synchronization, and power conservation [60] or decentralized collaborative detection of events [61]. There are numerous other areas and applications that have been the subject of self-organization themed research, so for more examples consult the associated references section.

6.3. **Gossip.** Insect social behavior and its self-organizing properties have inspired many research activities in various scientific areas. Some examples were given in the previous section. Human social interactions are also observed in the context of natural systems they belong to. People can be part of incredibly complicated social structures, many of which demonstrate self-organizing properties. Apart from the vertebrate neural and immures

systems, human social interactions have attracted much interest of the scientific community and have inspired various practical applications. Social networks have been a subject of an intensive sociological research for decades, and until only recently have linked up with mathematical and computational studies. Although initially not expected, research confirmed that networks which were a result of social interactions, although largely self-organizing, are not random graphs. Experiments inspired by the popular Erdős number (the number of collaborative links through scientific publications needed to connect to famous mathematician Paul Erdős) suggested that only six links were needed to connect almost everyone in the world [62]. Networks that describe human social interactions share distinct class of mathematical properties which positions them between random graphs and fully ordered networks. They have become known as the small-world networks and have inspired first important area of research based on human social interactions [63].

Simple interactions between humans known as gossip have inspired the second important research area based on human social behavior. Gossip is characterized by its high speed: information spreads very quickly, analogous to an epidemic infection. The difference in the latter case is that viruses play the role of disseminated information, but the underlying mechanics is the same. So, it is not uncommon when describing properties of a gossip protocol to accept and use epidemiologic terminology. More details on human gossip can be found in [64]. The use of epidemic (gossip) algorithms has been explored in applications such as information dissemination among a large number of nodes [65], failure detection [66], resource discovery and monitoring [67], data aggregation [68], and database replication [69]. The latter scenario represents the first practical application of gossip, and has introduced several basic variants of gossip-based information dissemination models.

In the context of this paper, our interest lies in studying various information dissemination techniques that can be implemented in computer and communication systems, their properties, advantages and disadvantages, and the possibility of using such protocols in the implementation of a network-centric networking in a decentralized environment.

Information dissemination. Distributed systems today are large-scaled and highly dynamic in nature [70]. The traditional client-server model is not an adequate solution to connect large number of nodes, enable information exchange between them, and handle failures or dynamic memberships in the system. The problem of reliability and scalability that occurs has to be tackled with radically different organization: P2P computing model. Each node there can potentially assume the role of either a client or a server. Scalability is achieved because the load is balanced between all nodes in the network, which prevents the occurrence of central point of failure and bottleneck. The problem of implementing information exchange on an application level is not straightforward, and in the context of M2M systems that are currently being standardized represents an active area of research.

Epidemic dissemination protocols are simple, scalable, and easy to deploy. Based on the same ideas as the spread of disease on a population, these protocols also show similar properties. Just the way epidemics shows resilience in case of failures (some infect people to die before they are able to spread a disease), epidemic protocols are also able to overcome link/node failures. Their scalability is based on the fact that there is not a single point of failure. In case of a node/link failure, other nodes will still be able to spread information through different routes. Each node in a system typically communicates only with its neighboring nodes because it lacks the global picture of the system. Complete view of all nodes in a system is not a realistic assumption in a large-scale network, especially in ad hoc networks which feature many joining and departures. Also, maintaining an up-to-date membership view without the irregularities is almost impossible, and brings unnecessary message overload in the network. However, some earlier implementations of epidemic protocols featured such an approach [69].

```
loop
    wait (Δ)
    p < random peer
    if push and in state I then
        send update to p;
    end
    if pull then
        send update-request to p;
    end
end

procedure onUpdate
    store m.update;     //switching to state I
end procedure

procedure onUpdateRequest
    if in state I then
        send update to m.sender;
    end
end procedure
```

FIGURE 7. SI gossip model (anti-entropy)

Two basic epidemic protocol variants known in the literature are the SI and SIR model. According to the terminology of epidemiology, each node can be in one of the following states [48]:

- Susceptible (S): The node is not yet infected, i.e., it does not know the update;
- Infected (I): The node knows the update and is trying to infect others around him, i.e., spread the update to other nodes;
- Removed (R): The node has developed immunity or died, i.e., it is no longer spreading the information.

The first, SI model (also called anti-entropy), includes only two possible states. Node is either susceptible or infected, and behaves accordingly. Spreading of information to its neighbors is happening according to the prototype showed in Figure 7. Node spreads information once in each Δ time units. This period is called a gossip cycle. It chooses a random node p out of the set of all available nodes. Next important choice is the selection of *push* or *pull* parameter. At least one of them has to be true, so the available combinations are *push*, *pull*, or *push-pull* gossip. In *push* gossip, susceptible nodes are passive, while in the two remaining cases each node is active. All the three variants eventually infect the entire network, but offer different performance while doing so. The *push-pull* model works faster than the other two variants.

A bit more complex model, the SIR epidemics model, was developed to cope with some of the problems encountered by the SI. Anti-entropy ignores one very important aspect of such systems: termination. SI *push* protocols never terminate, while *pull* have the ability to do so, but need to know the list of all available updates in advance which is rarely known in practice. Therefore, a more advanced epidemic model that solves this problem was developed. Algorithm showed on Figure 8. is very similar to the one of SI model. Major difference is the *onFeedback* procedure that allows a transition to the

```
loop
    wait (Δ)
    p < random peer
    if push and in state I then
        send update to p;
    end
    if pull then
        send update-request to p;
    end
end

procedure onFeedback(m)
    switch to state R with prob. 1/k;
end procedure

procedure onUpdate(m)
    if in state I or R then
        send feedback to m.sender;
    end
    else
        store m.update;      //now in state I
    end
end procedure

procedure onUpdateRequest
    if in state I then
        send update to m.sender;
    end
end procedure
```

FIGURE 8. SIR gossip model (rumor mongering)

removed state with the probability of $1/k$, where k stands for average number of times a node sends update to his peer that already has it. This mechanism, also called "rumor mongering", is based on "hot rumors". It means when a node receives a new update it is considered "hot", so it tries to send it to all nodes in his peer list. However, when his peer informs it that it already possesses this update, the sender switches its state to R with the mentioned probability. This behavior causes a rather important implication: depending on how fast the system converges to inactive state (all nodes are R), there is an explicit probability that the complete dissemination of information will not be achieved. In other words, rumor mongering does not assure that the sent updates will be received by all its intended destinations. For more details on SI and SIR epidemic models consult accompanied literature [48,69].

Based on the brief analysis, it is safely to assume that an actual distributed system information is spread using rumor mongering, but the occasional run of anti-entropy is necessary to take care of possible undelivered updates. In chapter 5, we discussed two M2M scenarios and analyzed their compatibility with the network-centric approach. The second one involves a possible farm field implementation and features decentralized network of M2M devices with sensors scattered on a possibly large area. The use of low-coverage technology such as ZigBee encourages the usage of self-organizing mechanisms for

information dissemination. Source node highlighted in the figure cannot send information to the highlighted destination directly as it does not possess the necessary technology to do so. It has an ability to send information to its neighboring nodes, and then rely on the fact that they will do the same. Obviously, self-organizing methods such as gossip (epidemic) protocols are almost a natural fit for these occasions. They offer a robust and scalable way of propagating information in distributed systems, and based on the brief overview of their basic features, are a compatible solution for implementing "information grid" of desired properties (universal access to information, information bus that connects all M2M devices, ability to continuously adapt to changes (dynamic network topologies, membership changes, etc.)) as proposed by the network-centric operations.

Applying gossip information dissemination in distributed systems. Epidemic algorithms have been studied theoretically because they are based on sound mathematical foundations [70]. There are several non-trivial issues that have to be carefully analyzed (e.g., analysis in [71] discovers that gossip's robustness crucially depends on a handful of assumptions that are often left unspoken) and resolved before epidemic algorithms can be applied in a practical distributed environment [72].

Every node in a network is a potential relay in a dissemination process and has a buffer of capacity b, sends messages limited number of times t to a randomly selected set of nodes of size f (fanout). Probabilistic guarantees of message delivery are directly related to the value of dissemination parameters, and epidemic algorithms in this sense display bimodal behavior: there is a clear threshold in the value of these parameters and the high probability of a reliable delivery. The reliability of message delivery is achieved with redundancy and randomization in order to bypass potential node and link failures. When implementing epidemic information dissemination in a practical setting, there are several important design constraints that need to be taken into account, and several important assumptions about the environment in which the protocols operate:

- Membership: The goal of the membership issue is to define how a node chooses nodes it knows, and then sends them information that is being disseminated. This has impact on the performance of the information dissemination process. The original ideas discussed in [69] assumed that every node in a network knows every other node. There are two important constraints for such an assumption. Firstly, membership information grows as the network grows. Secondly, maintaining consistent membership information about every node in a network imposes an extra network load, especially in dynamic environments (e.g., P2P networks). Therefore, because of the scalability requirements, each network node in a network in a practical example typically has only partial view of the network. The tradeoff between small and large views is also a tradeoff between scalability and reliability. Small views scale better, while large views reduce the chance that node becomes isolated.
- Network awareness: So far, discussions regarding epidemic algorithms assumed that all nodes are equally reachable, i.e., did not take into account the underlying network topology. In practice, such ignorance can be very costly: it is not an unlikely scenario where information is disseminated from one node to a very close node via a third remote node. Most solutions proposed to address this issue are based on hierarchical organizations which mimic the network topology [73] or use an administration system aware of the actual hierarchy [67].
- Buffer management: Simple epidemic protocol is based on the following sequence off steps: a node receives an update message and stores it in a buffer of capacity b, forwards that message a limited number of times t, each time to a randomly selected set of nodes of size f. Buffer's role is to ensure that every message is stored long

enough to enable it being sent a sufficient number of times to achieve an acceptable reliability of information dissemination. Strategies on what to do when the buffer is full: nodes in a conservative strategy simply reject and drop new messages, while a dynamic strategy drops old messages (those that have been forwarded a sufficient number of times) according to certain criteria. The goal of these strategies is to ensure memory usage optimization and/or resource scalability, while maintaining an acceptable reliability. An example is a strategy which classifies messages according to their age, i.e., the number of times a message has been sent to another node. When a buffer is full, instead of dropping a new message, node chooses to drop the oldest one. Similar result can be achieved using application semantics [74] that defines an obsolescence relation: message m_1 makes message m_2 obsolete in a sense a node that receives m_1 does not need m_2 anymore. This approach can be combined with the age-based priority.

- Message filtering: So far, all discussions assumed that every node in a network is equally interested to receive all messages. However, nodes could be partitioned into distinct groups according to their interest, and messages disseminated accordingly. Epidemic dissemination scheme can be enhanced with filtering capabilities that switch randomized neighbor selection scheme with a heuristic to privilege only interested nodes. The goal is to increase probability that a node receives a message only it is interested in. Non-randomized solutions take into account node's interests and dynamically evaluate exchanged messages based on their contents. The design of such a filtering mechanism is not a trivial problem. Providing knowledge on node's interest in a decentralized manner is a first major issue. Secondly, even when a node knows that a certain message is not interesting to its neighboring node, there is still a genuine possibility that this node might be critical in reaching message's intended destination. Obviously, making nodes communicate only with nodes of the same interest is hard, because nodes only know subsets of the other nodes in the network. In addition, achieving network awareness together with message filtering is even a more complex problem. Approach presented in [75] arranges nodes in a form of a hierarchy according to their geographical distances, while their interests are grouped at each level of hierarchy at the same time, and achieves very good performance.

7. **Conclusion.** M2M systems due to their diversity still faced with management and coordination challenges. NCO as an information management concept is a way of maximizing the value of M2M solutions, moving from centralized to decentralized control and reaching the maximum utilization of available information. It is shown that M2M environment is capable of implementing key features of such an approach. Apart from the described M2M e-Health system where a network-centric networking, although not a completely natural fit, offers enrichment of the current system's operations, there are also M2M systems with inherently decentralized organizations that are so far mostly ignored by the standardization efforts and would benefit even more from the inclusion of NCO ideas. Implementing such an approach proposes the development of an interconnected, robust and dynamic information grid within the M2M system network infrastructure that will increase shared situational awareness and allow self-synchronization of connected smart devices. As it was discussed in the paper, natural self-organizing systems offer a viable solution: gossip (epidemic) protocols. They have already been implemented in various distributed systems and display many desired properties. However, there are several non-trivial issues that have to be carefully analyzed before initiating their customization for specific practical purposes.

Future work, according to the presented material, offers many possibilities. Further research on the topic of information dissemination, customization of gossip protocols that would be able to take advantage of the specific properties of M2M applications, or the development of semantic support for information exchange and social interactions between M2M machines are just few of the many available options.

Acknowledgment. This work was supported by two research projects: "Content Delivery and Mobility of Users and Services in New Generation Networks" (036-0362027-1639), funded by the Ministry of Science, Education and Sports of the Republic of Croatia and "Looking to the Future", funded by Croatian Post and Electronic Communications Agency. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] *Smart Devices and Services Connected by CDMA2000*, Harbor Research, Inc., 2010.
[2] *M2M: Growth Opportunities for MNOs in Developed Markets (Sample Pages)*, Mobile Market Development Ltd., 2010.
[3] M. Alendal, Operators need an ecosystem to support 50 billion connections, *Ericsson Review*, no.3, 2010.
[4] A. Cox, M2M: Connecting the devices, M2M & embedded strategies, telematics, CE, mHealth, metering & smart buildings 2011-2016, *Juniper Research*, 2011.
[5] *ETSI Technical Specification 102 689: M2M Service Requirements, v2.0.3, ETSI*, 2012.
[6] *3GPP Technical Report 22.868: Study on Facilitating M2M Communication in 3GPP Systems, v8.0.0, 3GPP*, 2007.
[7] N. Tekbiyik and E. Uysal-Biyikoglu, Energy efficient wireless unicast routing alternatives for machine-to-machine networks, *Journal of Network and Computer Applications*, vol.34, no.5, pp.1587-1614, 2011.
[8] G. Lawton, Machine-to-machine technology gears up for growth, *IEEE Computer*, vol.37, no.9, pp.12-15, 2004.
[9] D. Katusic and G. Jezic, Network-centric operations in machine-to-machine networks, *Lecture Notes in Computer Science*, vol.7327, pp.474-483, 2012.
[10] F. Dressler, Network-centric actuation control in sensor/actuator networks based on bio-inspired technologies, *Proc. of the 2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, pp.680-684, 2006.
[11] S.-Y. Lien, K.-W. Chen and Y. Lin, Towards ubiquitous massive accesses in 3GPP machine-to-machine communications, *IEEE Communications Magazine*, vol.49, no.4, pp.66-74, 2011.
[12] K. Chang, A. Soong, M. Tseng and Z. Xiang, Global wireless machine-to-machine standardization, *IEEE Internet Computing*, vol.15, no.2, pp.64-69, 2011.
[13] *oneM2M*, http://www.onem2m.org/, 2012.
[14] *ETSI*, http://www.etsi.org/website/homepage.aspx, 2012.
[15] *ETSI M2M Technical Committee*, http://www.etsi.org/Website/Technologies/M2M.aspx, 2012.
[16] *ETSI Technical Report 102 691: Smart Metering Use Cases, v1.1.1, ETSI*, 2010.
[17] *ETSI Technical Report 102 732: Use Cases of M2M Applications for eHealth, v0.4.1, ETSI*, 2011.
[18] *ETSI Technical Report 102 857: Use Cases of M2M Applications for Connected Consumer, v0.3.0, ETSI*, 2010.
[19] *ETSI Technical Report 102 898: Use Cases of Automotive Applications in M2M Capable Networks, v0.4.0, ETSI*, 2010.
[20] *ETSI Technical Report 102 897: Use Cases of M2M Applications for City Automation, v0.1.1, ETSI*, 2010.
[21] *ETSI Technical Report 102 725: M2M Definitions, v0.8.0, ETSI*, 2012.
[22] *ETSI Technical Specification 102 690: M2M Functional Architecture, v2.0.9, ETSI*, 2012.
[23] *ETSI Technical Report 101 603: 3GPP Interworking, v0.0.5, ETSI*, 2012.
[24] *ETSI Technical Report 103 107: 3GPP2 Interworking, ETSI*, 2012.
[25] *ETSI Technical Specification 103 092: OMA DM Compatible Management Objects for ETSI M2M, v1.2.1, ETSI*, 2013.
[26] *ETSI Technical Specification 103 903: BBF TR-069 Compatible Data Model, v2.0.3, ETSI*, 2012.

[27] *ETSI Technical Report 102 966: Interworking between the M2M Architecture and M2M Area Network Technologies, v0.2.0, ETSI*, 2012.
[28] *3GPP*, http://www.3gpp.org/About-3GPP, 2012.
[29] *3GPP Technical Specification 22.368: Service Requirements for MTC, v11.3.0, 3GPP*, 2011.
[30] *3GPP Technical Report 22.988: Study on Alternatives to E.164 for MTC, v2.0.0, 3GPP*, 2012.
[31] *3GPP Technical Specification 02.30: Man-machine Interface of the Mobile Station, v7.1.1, 3GPP*, 2002.
[32] *3GPP Technical Specification 22.030: Man-machine Interface of the User Equipment, v12.0.0, 3GPP*, 2012.
[33] *3GPP Technical Report 23.888: System Improvements for MTC Communication, v1.6.0, 3GPP*, 2011.
[34] *3GPP Technical Report 33.812: Feasibility Study on the Security Aspects of Remote Provisioning and Change of Subscription for M2M Equipment, v9.2.0, 3GPP*, 2010.
[35] *3GPP Technical Report 33.868: Security Aspects of Machine-Type Communications, v0.10.0, 3GPP*, 2012.
[36] *3GPP Technical Report 37.868: RAN Improvements for Machine-Type Communications, v11.0.0, 3GPP*, 2011.
[37] *3GPP Technical Report 43.868: GERAN Improvements for Machine-Type Communications, v12.0.0, 3GPP*, 2012.
[38] A. K. Cebrowski and J. J. Garstka, Network-centric warfare: Its origin and future, *Proceedings Magazine*, pp.28-35, 1998.
[39] NIS23, *Net-Centric Information & Integration Services for Security System*, 2009.
[40] D. S. Alberts, J. J. Garstka and F. P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition, CCRP, 2001.
[41] *Network Centric Warfare*, Department of Defense Report to Congress, 2001.
[42] *ETSI Technical Report 101 584: Study on Semantic support for M2M Data, v0.5.0, ETSI*, 2012.
[43] N. J. Wesensten, G. Belenky and T. J. Balkin, Cognitive readiness in network-centric operations, *Parameters*, vol.35, no.1, pp.94-105, 2005.
[44] J. S. Bay, Disruptive effects of net-centricity on command and control, *Proc. of the 13th ICCRTS "C2 for Complex Endeavors"*, 2008.
[45] J. L. Groh, Network-centric warfare: Leveraging the power of information, *USAWC Guide to National Security Issues*, vol.1, pp.323-338, 2008.
[46] D. von Lubitz and N. Wickramasinghe, Healthcare network centric operations: The confluence of E-Health and E-Government, *Global E-Government: Theory, Applications and Benchmarking*, pp.127-147, 2007.
[47] D. C. Schmidt, A. Corsaro and H. van't Hag, Addressing the challenges of tactical information management in net-centric systems with DDS, *PrismTech Corporation*, 2008.
[48] G. D. M. Serugendo, M.-P. Gleizes and A. Karageorgos, *Self-Organising Software: From Natural to Artificial Adaptation*, Springer-Verlag, Berlin, 2011.
[49] F. Heylighen, The science of self-organization and adaptivity, *Knowledge Management, Organizational Intelligence and Learning, and Complexity*, pp.253-280, 2001.
[50] P. P. Grassé, La reconstruction du nid et les coordinations interindividuelles chezbellicositermes natalensis ectubitermes sp la théorie de la stigmergie: Essai d'interprétation du comportement des termites constructeurs, *Insectes Sociaux*, vol.6, no.1, pp.41-80, 1959.
[51] S. Camazine, J. L. Deneubourg, N. R. Franks, J. Sneyd, G. Theraulaz and E. Bonabeau, *Self-Organization in Biological Systems*, 2nd Edition, Princeton University Press, 2003.
[52] J. L. Deneubourg, S. Goss, N. Franks, A. Sendova-Franks, C. Detrain and L. Chretien, The dynamics of collective sorting robot-like ants and ant-like robots – Simulation of animal behaviour, *Proc. of the 1st International Conference of Simulation of Adaptive Behaviour*, pp.356-363, 1991.
[53] S. Brueckner and H. V. D. Parunak, Self-organising MANET management, *Lecture Notes in Artificial Intelligence*, vol.2977, pp.20-35, 2004.
[54] A. Montresor, H. Meling and O. Babaoglu, Messor: Load-balancing through a swarm of autonomous agents, *Lecture Notes in Artificial Intelligence*, vol.2530, pp.125-137, 2003.
[55] N. Foukia, IDReAM: Intrusion detection and response executed with agent mobility, *Proc. of International Conference on Autonomous Agents and Multi-Agent Systems*, New York, USA, pp.264-270, 2005.
[56] M. Jelasity and O. Babaoglu, T-man: Gossip-based overlay topology management, *Lecture Notes in Computer Science*, vol.3910, pp.1-15, 2006.

[57] K. Aberer, A. Datta and M. Hauswirth, P-grid: Dynamics of self-organizing processes in structured peer-to-peer systems, *Lecture Notes in Computer Science*, vol.3485, pp.137-153, 2005.
[58] G. D. Caro and M. Dorigo, Ant colonies for adaptive routing in packet switched communication networks, *Proc. of the 5th International Conference on Parallel Problem Solving from Nature*, London, UK, pp.673-682, 1998.
[59] R. Schoonderwoerd, O. Holland and J. Bruten, Ant-like agents for load balancing in telecommunications networks, *Proc. of the 1st International Conference on Autonomous Agents*, Los Alamitos, USA, pp.209-216, 1997.
[60] K. Mills, A brief survey of self-organization in wireless sensor networks, *Wireless Communications and Mobile Computing*, vol.7, pp.823-834, 2007.
[61] J. L. Fernandez-Marquez, J. L. Arcos and G. D. M. Serugendo, A decentralized approach for detecting dynamically changing diffuse event sources in WSN environments, *Proc. of the 4th International Conference on Self-Adaptive and Self-Organising Systems*, Los Alamitos, USA, 2010.
[62] D. Watts, *Six Degrees: The Science of a Connected Age*, Vintage, London, 2004.
[63] D. Watts, *Small Worlds: The Dynamics of Networks Between Order and Randomness*, Princeton University Press, 1999.
[64] A. J. Kimmel, Rumors and rumor control: A manager's guide to understanding and combating rumors, *Taylor & Francis Group*, 2004.
[65] R. M. Karp, C. Schindelhauer, S. Shenker and B. Vocking, Randomized rumor spreading, *Proc. of the 41st Annual Symposium on Foundations of Computer Science*, Berkeley, USA, pp.565-574, 2000.
[66] R. van Renesse, Y. Minsky and M. Hayden, A gossip-style failure detection service, *Proc. of the IFIP International Conference on Distributed Systems Platforms and Open Distributed Processing*, London, UK, pp.55-70, 1998.
[67] R. van Renesse, K. P. Birman and W. Vogels, Astrolabe: A robust and scalable technology for distributed system monitoring, management, and data mining, *ACM Transactions on Computer Systems*, vol.21, no.2, pp.164-206, 2003.
[68] M. Jelasity, A. Montresor and O. Babaoglu, Gossip-based aggregation in large dynamic networks, *ACM Transactions on Computer Systems*, vol.23, no.3, pp.219-252, 2005.
[69] A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart and D. Terry, Epidemic algorithms for replicated database management, *Proc. of the 6th Annual ACM Symposium on Principles of Distributed Computing*, Vancouver, Canada, pp.1-12, 1987.
[70] N. T. J. Bailey, *The Mathematical Theory of Infectious Diseases and Its Applications*, 2nd Edition, Griffin, London, 1975.
[71] L. Alvisi, J. Doumen, R. Guerraoui, B. Koldehofe, H. Li, R. von Renesse and G. Tredan, How robust are gossip-based communication protocols? *ACM SIGOPS Operating Systems Review – Gossip-Based Computer Networking Archive*, vol.41, no.5, pp.14-18, 2007.
[72] P. T. Eugster, R. Guerraoui, A.-M. Kermarrec and L. Massoulié, From epidemics to distributed computing, *IEEE Computer*, vol.37, no.5, pp.60-67, 2004.
[73] A.-M. Kermarrec, L. Massoulié and A. J. Ganesh, Probabilistic reliable dissemination in large-scale systems, *IEEE Transactions on Parallel and Distributed Systems*, vol.14, no.3, pp.248-258, 2003.
[74] J. Pereira, L. Rodrigues and R. Oliveira, Semantically reliable multicast algorithms, *IEEE Transactions on Computers*, vol.52, no.2, pp.150-165, 2003.
[75] P. T. Eugster and R. Guerraoui, Probabilistic multicast, *Proc. of the 2002 International Conference on Dependable Systems and Networks*, pp.313-324, 2002.