

# Realizing the Internet of Nano Things: Challenges, Solutions, and Applications

**Sasitharan Balasubramaniam**, *Tampere University of Technology, Finland,*  
and *Waterford Institute of Technology, Ireland*

**Jussi Kangasharju**, *University of Helsinki, Finland*

**Embedding nanosensors in the environment would add a new dimension to the Internet of Things, but realizing the IoNT vision will require developing new communication paradigms and overcoming various technical obstacles.**

**T**he Internet of Things has transformed the use of the Internet. Through the IoT, various types of objects, sensors, and devices can interact and form pervasive networks that enhance our daily lives.<sup>1</sup> In the healthcare domain, for example, body area networks collect vital patient information and feed it to service providers' computing systems, making it possible to more accurately and efficiently monitor a large number of people. Sensors embedded in the environment also provide ambient assisted living care for the elderly and disabled.

Advances in nanotechnology have paralleled developments in Internet and sensing technology. Since Richard Feynman's famous Nobel Lecture on nanotechnology in 1959, the field has rapidly progressed, producing sophisticated devices with numerous applications, such as improved sensing at the molecular level to facilitate targeted drug delivery to patients. In recent years, the discipline of nanocommunication has emerged, with

the objective of creating new interaction paradigms for nanodevices to improve their capabilities and applications.<sup>2</sup>

However, nanodevices need not be limited to peer-to-peer communication. Embedding nanosensors in the various objects and devices that surround users would add a new dimension to the IoT: the Internet of Nano Things (IoNT). Such miniature sensors, interconnected through nanonetworks, could obtain fine-grained data within objects and from hard-to-access areas, leading to the discovery of novel insights and applications. For example, on-body nanosensors could provide electrocardiographic and other vital signals, while environmental nanosensors could collect information about pathogens and allergens in a given area. Combining these two data sources through the IoNT could make it easier to more accurately diagnose and monitor a patient's condition.

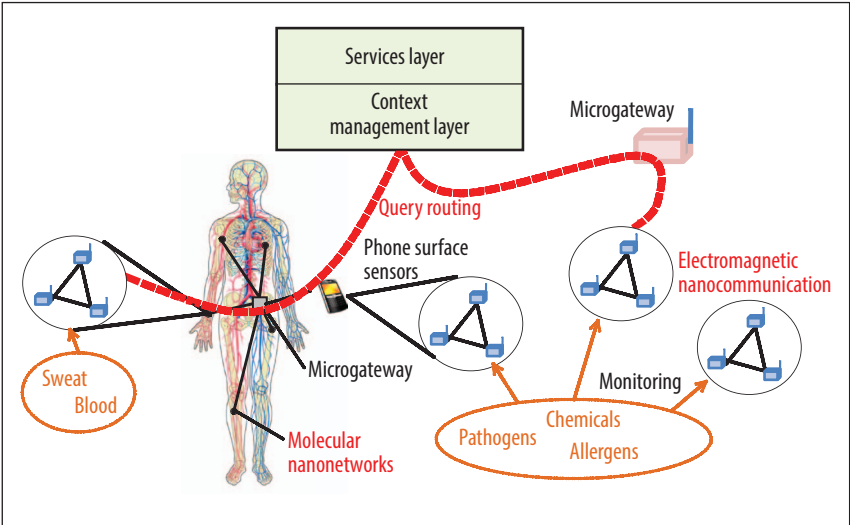
The IoNT concept was introduced by Ian Akyildiz and Josep Jornet,<sup>3</sup> who outlined a general architecture for electromagnetic (EM) nanodevice communication, including channel modeling, information encoding, and protocols. These researchers described the components most suitable for nanoscale communication, focusing on graphene-based nanoantennas. Such antennas are most energy efficient in the terahertz band. However, this leads to unique and sensitive properties such as path loss and noise resulting from molecular absorption, which affects the attenuation of propagating waves. Akyildiz and Jornet also addressed new forms of routing as well as service discovery that would be required for EM-based nanocommunication.

Here, we consider two major challenges to realizing the IoNT: creating data collection and routing mechanisms in nanonetworks, and developing middleware that connects conventional microsenors to nanonetworks. We also look at the requirements for extending current context and service management systems to support the IoNT, as well as some possible IoNT applications.

### THE INTERNET OF NANO THINGS

As Figure 1 shows, the envisioned IoNT includes underlying nanoscale networks connecting a multitude of nanosensors, devices that interact with the nanonetworks and process their information in a distributed manner, and context and service management systems. While researchers have proposed numerous nanocommunication approaches, here we consider the two most practical: *molecular communication* and *EM communication*.<sup>2</sup>

Nanodevices could interact in a biological environment such as the human body by overriding the existing organic communication system or utilizing biomolecules such as nucleotides, amino acids, and peptides for communication—for example, reprogramming cells to function as sensors. Researchers have proposed numerous ways to convert information into biomolecules and then transport them to recipient nanodevices for decoding, including molecular diffusion, calcium signaling, bacteria and virus nanonetworks, and the use of neurons.<sup>2,4-7</sup> Bacteria and viruses can carry genetic data, which is suited for sensors that encode information in DNA form.

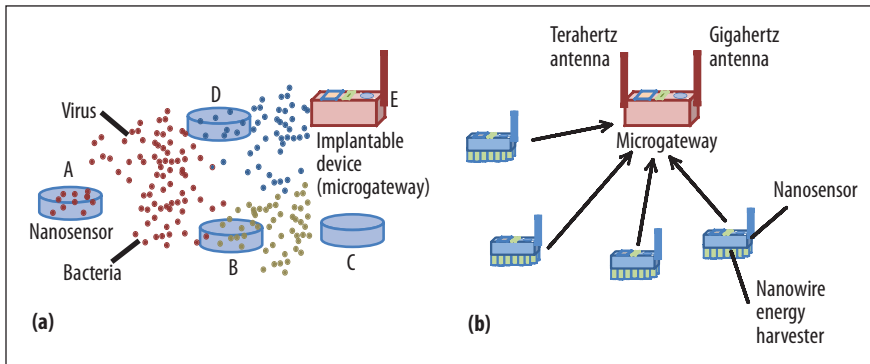


**Figure 1. The Internet of Nano Things.** The envisioned IoNT includes underlying nanoscale networks connecting a multitude of nanosensors, devices that interact with the nanonetworks and process their information in a distributed manner, and context and service management systems.

Nanodevices could also interact through EM communication, which is more conventional than molecular communication. Each device would resemble a micro-sensor mote, ranging in size from 2 to 6 micrometers. The components—including antennas, EM transceivers, and processors—would all be built at nanoscale.<sup>3</sup> As indicated, the antennas would likely be built from graphene materials and communicate in the THz band.<sup>3</sup>

Protocol design for the IoNT will require revised thinking to accommodate nanocommunication properties. In the case of molecular communication, these properties might include slow or unreliable message transmission between nanodevices due to a high level of noise in the biological environment, slow propagation of molecules, or the motility of bacteria or viruses. In the case of EM communication, nanoscale devices must self-power or

Table 1. Data collection challenges to realizing the IoNT.		
Category	Challenge	Proposed solution
System architecture	High ratio of nanosensors to microgateways could lead to swift energy depletion if microgateways must process information from every nanosensor.	Distribute the sink architecture and develop a two-layered hierarchy consisting of microgateways and nanonetworks.
Routing technology	Molecular nanonetworks: Information-carrying molecules could move very slowly between nodes as well as become lost.	Opportunistic routing through multihop relays of nanodevices; base the topology on random or unstructured graphs.
	EM nanonetworks: Limited memory, computational power, and energy will constrain data transmission between nodes.	Single-hop transmission to microgateways through a star topology; incorporate query-based routing, with queries routed between microgateways.
	With only one microgateway per nanonetwork, bulk data transmission could be difficult.	Incorporate unconventional routing technologies such as mobile delay-tolerant networks to carry bulk data.



**Figure 2.** Examples of molecular (a) and EM (b) nanonetworks interfacing to a microgateway.

harvest energy, adapt to timing differences between the harvesting and transmission periods, and cope with molecular absorption on graphene antennas that can affect transmission reliability.

## DATA COLLECTION

An important factor in realizing the IoNT is the need to collect the large quantities of data that nanodevices in the environment generate. Table 1 summarizes the challenges and proposed solutions with respect to the system architecture and routing technology.

## System architecture

Sensor network architectures traditionally use a certain number of sinks to collect data from the sensors, but this might not be feasible for nanonetworks. A possible solution is to use *microgateways*—conventional microsensors that can connect to nanosensors—as an intermediate layer of devices. Figure 2 illustrates the hierarchical structure that enables microgateways to interact with molecular and EM nanonetworks. In the case of EM nanonetworks, each microgateway will require dual transceivers: one to communicate with nanonetworks in the THz band and another to communicate with peer microgateways in the GHz band.

## Routing technology

Routing is an essential requirement for information transmission through communication networks. Most sensor network routing algorithms focus on optimizing energy-efficiency capabilities as well as scalability. However, there are key differences between nanosensors and traditional microsensors that impact IoNT algorithm design.

First, nanosensors use considerably less energy than microsensors, which require energy harvesting to power the devices. For example, biochemicals in the environment fuel molecular nanosensors, while EM nanosensors use nanowire vibrations to generate energy.

Second, nanodevices have relatively limited memory storage and computational processing capabilities and thus little topology knowledge of the communication en-

vironment. This means that they cannot look up addresses or perform path calculations.

### Molecular nanonetworks.

These nanonetworks can represent the transmitted information as data stored within a DNA component (similar to an IP packet) or in binary form. The binary value usually represents a concentration of molecules that are transmitted between the nodes—for example, 1 represents a specific concentration, while 0

represents no molecular transmission. Due to the limited range of molecules or other components carrying the message, routing within molecular nanonetworks can be multihop. A relay nanodevice will not have a routing table that can compute routes to a destination point, so the routing mechanism will be opportunistic.

Routing in molecular nanonetworks can be query based or rely on polling at the microgateway to collect data. Since multihop routing is an option, topologies deployed for molecular nanonetworks could assume various shapes and sizes: scale-free, grid, and so on. For example, one study used various simple topologies to simulate a multihop routing scheme for bacteria carrying DNA-based messages.<sup>8</sup> On the other hand, the probability of information loss in molecular nanonetworks is very high. For example, molecules diffused by environmental fluid motion could become lost, while external chemical agents such as antibiotics can kill viruses or bacteria.

**EM nanonetworks.** Although devices in EM nanonetworks will have dedicated nanomemory, they might not be able to store protocol code and thus will be incapable of calculating routes to a destination node. This limitation extends to cooperation between devices. We therefore expect the routing architecture to be hierarchical, with nanodevices communicating in a single hop to a microgateway—that is, a star topology. Because the devices have limited memory and can only produce packets with a small number of bits, which will be transmitted within nanoseconds, data transmissions between nanodevices and microgateways should not experience packet collision. Due to nanodevices' limited energy, the communication protocol will be query based, with queries routed between the microgateways to reach specific devices.

**Unconventional routing.** With only one microgateway per nanonetwork, routing bulk data could be difficult. A possible solution is to incorporate unconventional routing technologies such as mobile delay-tolerant networks, which opportunistically use people or vehicles equipped with mobile devices to transport data to a destination

**Table 2. Middleware challenges to realizing the IoNT.**

Category	Challenge	Proposed solution
System management	Unstable and unreliable environment—for example, fluid motion in molecular nanonetworks and water vapor in EM nanonetworks.	Integrate self-awareness mechanisms at the microgateway to learn environmental conditions.
Data analysis	Dynamic changes in the environment could lead to transmitting a large quantity of data along microgateway routes, making traditional static data collection trees impractical.	Incorporate a dynamic tree structure for distributed, node-to-node interactions between microgateways.
	Timing difference in data propagation between nanosensors could result in long delays for messages before they reach the sink.	Implement a time-delayed data fusion process so that microgateways wait for all messages to arrive before routing them to peer microgateways.
Energy conservation	Microgateways could quickly deplete their energy while interfacing with nanonetworks.	Through awareness of the environment, the microgateway synchronizes its sleep pattern to latency in molecular transmission (molecular nanonetworks) or charging patterns (EM nanonetworks).

point. In EM nanonetworks, each device could be equipped with a transceiver that receives signals from sensors (in the THz band) when it comes within close proximity. In molecular nanonetworks, an intermediate microgateway would be required to fuse and collect data before transmitting it to the mobile carrier. This approach is similar to “data mules” moving through an environment collecting data from sensors.

## MIDDLEWARE

Researchers have proposed various middleware for sensor networks in recent years.<sup>9</sup> This middleware is designed to abstract the underlying network functionalities from the services that utilize the sensor information. To support the IoNT, however, current middleware must address challenges with respect to system management, data analysis, and energy conservation. Table 2 summarizes the challenges and proposed solutions.

Figure 3 illustrates an architecture for distributed microgateway middleware that could support the IoNT. Microgateways contain system management and data analysis modules. On the user end, programming abstractions link to the microgateway middleware, and application services use data from the nanonetworks.

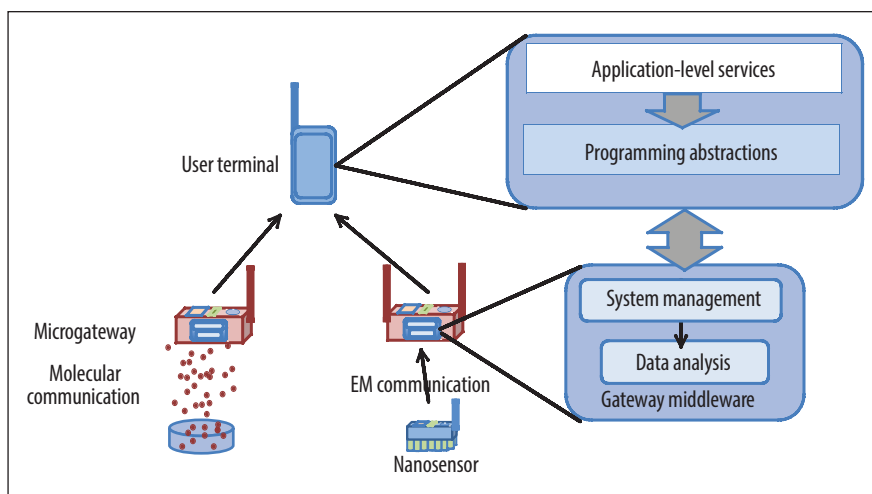
### System management

Similar to current wireless sensor networks middleware, the microgateway system management module manages the

gateway’s internal operation. In addition to resource and quality-of-service management, one of its main functions is self-awareness.

Nanonetwork environments are often harsh and variable, which can interfere with the efficient and reliable transmission of nanosensor data. For example, fluid motion can disturb molecular diffusion, while water vapor can interfere with EM signals. Because network topologies might be random and dynamic, depending on environmental conditions, nanodevices within the network might not have the requisite topology knowledge.

In both types of nanonetworks, there is a master-slave relationship between the microgateway and the nanonetwork: only the microgateway has full knowledge of the network and environment and the ability to reconfigure network behavior. To attain a high degree of self-awareness,



**Figure 3. IoNT middleware system architecture. Microgateways contain system management and data analysis modules. On the user end, programming abstractions link to the microgateway middleware, and application services use data from the nanonetworks.**



**Table 3. Other challenges to realizing the IoNT.**

Category	Challenge	Proposed solution
Context management	Nanonetworks will generate a wide range of extremely fine-grained data that requires contextual processing.	Integrate specialized conceptual models, such as smart space and gene ontologies, and enhance cross-domain reasoning.
Security and privacy	Information collected from nanosensors might include individuals' molecular and genetic data.	Implement safeguards to ensure that sensitive IoNT data does not fall into the wrong hands.
Service composition and discovery	Current service-oriented architectures cannot adequately deal with nanonetworks' large quantity and variety of data.	Subdivide services into two layers, application and data collection services, each with clustered service composition and discovery models.

a microgateway must be able to infer the topology of nanonetworks with which it is interfaced, assess the condition of the environment (which could vary with time), and identify and adjust for fluctuations that might affect the reliability of message transmission.

### Data analysis

In traditional sensor networks, data collection usually occurs via a static tree. Each node along the tree senses the data and then passes it along the tree to the sink node at the root. However, since each microgateway interfaces to numerous nanosensors, this approach could lead to large data traffic, especially if sensing is periodic. A dynamic data collection tree is therefore required for node-to-node interactions between microgateways.

In both molecular and EM nanonetworks, the microgateway must integrate data from various nanosensors before sending it down the tree. However, the timing difference in data propagation between nanodevices could result in long delays for messages before they reach the sink. In molecular nanonetworks, the transmission of information could take considerable time, especially when queries expect feedback. In EM nanonetworks, energy harvesting is a major constraint, as the harvesting process can take up to a minute before transmission can occur. An optimal time-delayed data fusion process must therefore be implemented at the microgateway to process all information before further transmission along the data collection tree.

### Energy conservation

Microgateways could quickly deplete their energy while interfacing with nanonetworks. Dynamic timing synchronization of microgateways with nanodevices could make it possible to determine when to put microgateways to sleep to conserve energy. In molecular nanonetworks, for example, if a high quantity of foreign fluids could delay molecules' arrival at their destination, the microgateway could go to sleep and awake once the molecules are estimated to arrive. In EM nanonetworks, microgateways could go to sleep while nanodevices are harvesting energy.

## OTHER CHALLENGES

In addition to data collection and middleware, IoNT researchers must address issues related to context management, security and privacy, and service composition and discovery. Table 3 summarizes these issues and proposed solutions.

The IoNT will make it possible to collect data at extremely fine-grained (microscopic) levels from various sources, and context models will be needed to process this data. While researchers have developed numerous context models and reasoning techniques for pervasive computing applications,<sup>10</sup> the wide range of data collected by nanonetworks will require cross-domain reasoning that spans multiple specialized ontologies. Figure 4 illustrates a context model that uses gene and smart-space ontologies to process data from molecular and EM nanonetworks.

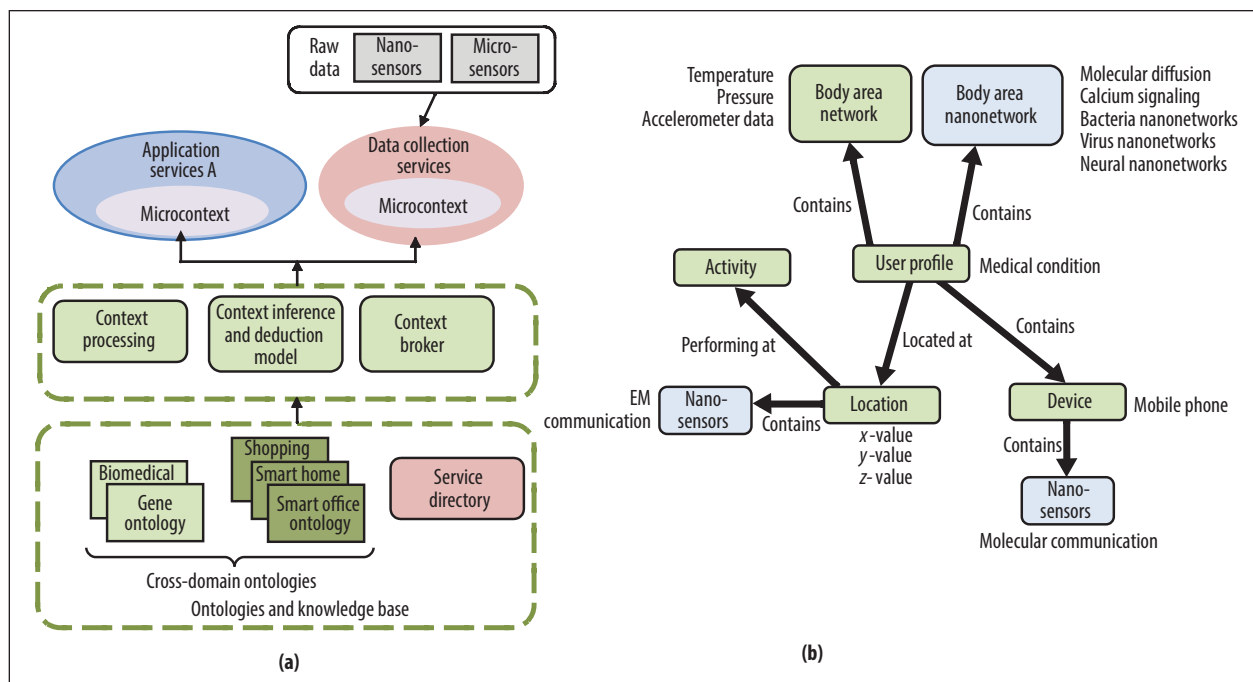
New security and privacy mechanisms will also be needed to protect sensitive data gathered by nanosensors, which can include detailed chemical and biological samples from individuals. For example, molecular nanonetworks could gather data about people infected with a harmful virus to shed light on the nature and severity of the disease. Safeguards must be in place to ensure that such data does not fall into the wrong hands.

Services are also an essential aspect of the IoNT. Current service-oriented architectures cannot adequately deal with nanonetworks' large quantity and variety of data. One way to address this problem is to subdivide services into application and data collection layers, each with clustered service composition and discovery models. Figure 5 provides an example of distributed interaction between these two types of services.

## APPLICATIONS

The fine granularity of data collected by nanonetworks will enable the IoNT to extend existing applications and provide new applications that are limited or unavailable in the IoT. In the immediate future, we envision IoNT applications in healthcare, environmental and agricultural monitoring, and certain cross-domain scenarios.

The most obvious IoNT application is using networked in-body nanosensors to collect and monitor



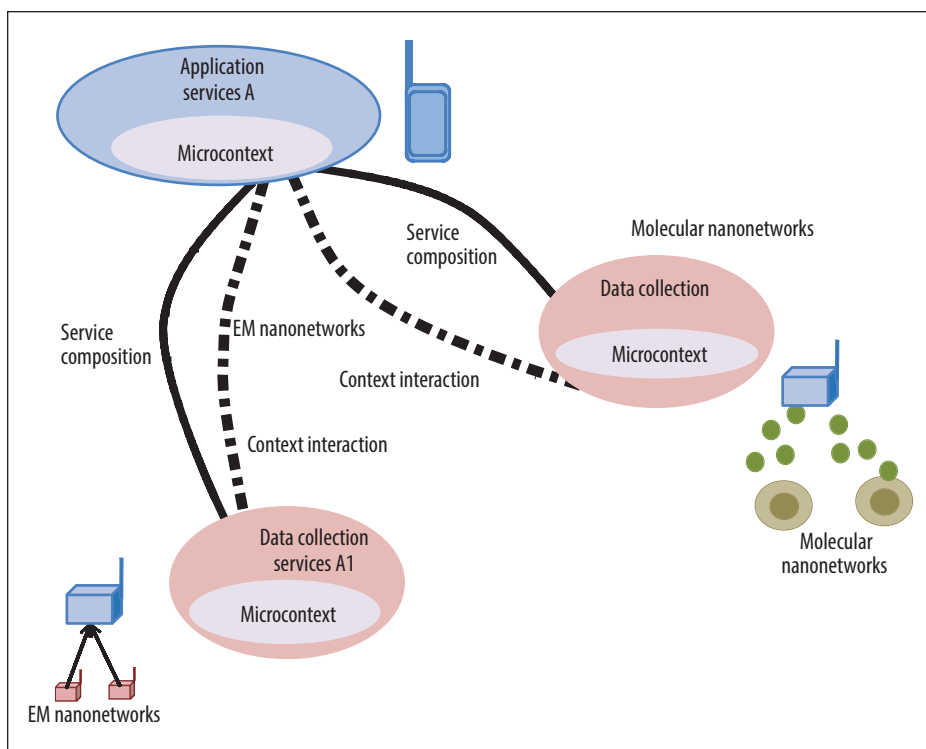
**Figure 4.** The wide range of data collected by nanonetworks will require cross-domain reasoning that spans multiple specialized domains. (a) Example context model that uses smart-space and gene ontologies to process data from molecular and EM nanonetworks. (b) Example definition of integrated IoNT ontology.

vital biological activity, including disease processes, in patients. Such sensors could provide near-real-time data to an on-body microgateway in a wearable device, which in turn would transmit the data to a patient's doctor. In-body nanonetworks could also analyze body fluid and breath and perform other types of medical tests, obviating the need for a patient to go to a laboratory.

Another possible application is the placement of nanosensors in high-density public locations, such as hospitals, airports, and restaurants, to track the propagation of viral diseases and better understand how different types of people are affected.

Networked nanosensors could also be used to monitor the environment, including pollution, greenhouse gasses, and radiation. The agricultural sector


would likewise benefit from the use of nanosensors to help detect harmful bacteria, viruses, and other infec-



**Figure 5.** To deal with nanonetworks' large quantity and variety of data, IoNT services can be subdivided into application and data collection layers, each with clustered service composition and discovery models.

tious agents such as *E. coli* and mad cow disease in crops or livestock.

The IoNT could extend across multiple domains. For example, a link could be formed between dairy products and healthcare sectors to eliminate or minimize production conditions that impact people with certain types of allergies.

**N**anotechnology has transformed traditional approaches to solving a wide variety of problems, especially in the manufacturing and healthcare domains. To date, however, researchers have given little attention to using nanodevices embedded in the environment to support computing for end users. The IoNT vision could be realized by incorporating new communication paradigms between nanodevices, as well as between nano- and microdevices used on a daily basis, along with overcoming some other technical hurdles. The time is ripe to develop a truly pervasive computing environment that can better serve humankind. 

## IEEE STC 2013

25th IEEE Software Technology  
Conference

8-11 April 2013

Salt Lake City, Utah, USA

Register today!  
<http://www.sstc-online.org/>



## Acknowledgments

This work received support from the Academy of Finland FiDiPro program "Nanocommunication Networks," 2012-2016, as well as Science Foundation Ireland under grant number 09/SIRG/I1643, "A Biologically Inspired Framework Supporting Network Management for the Future Internet."

## References

1. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, 2010, pp. 2787-2805.
2. I.F. Akyildiz, F. Brunetti, and C. Blázquez, "Nanonetworks: A New Communication Paradigm," *Computer Networks*, vol. 52, no. 12, 2008, pp. 2260-2279.
3. I.F. Akyildiz and J.M. Jornet, "The Internet of Nano-Things," *IEEE Wireless Comm.*, vol. 17, no. 6, 2010, pp. 58-63.
4. T. Nakano and J.-Q. Liu, "Design and Analysis of Molecular Relay Channels: An Information Theoretic Approach," *IEEE Trans. NanoBioscience*, vol. 9, no. 3, 2010, pp. 213-221.
5. L.C. Cobo and I.F. Akyildiz, "Bacteria-Based Communication in Nanonetworks," *Nano Comm. Networks*, vol. 1, no. 4, 2010, pp. 244-256.
6. F. Walsh et al., "Synthetic Protocols for Nano Sensor Transmitting Platforms Using Enzyme and DNA Based Computing," *Nano Comm. Networks*, vol. 1, no. 1, 2010, pp. 50-62.
7. A. Guney, B. Atakan, and O.B. Akan, "Mobile Ad Hoc Nanonetworks with Collision-Based Molecular Communication," *IEEE Trans. Mobile Computing*, vol. 11, no. 3, 2012, pp. 353-366.
8. P. Liò and S. Balasubramaniam, "Opportunistic Routing through Conjugation in Bacteria Communication Nanonetwork," *Nano Comm. Networks*, vol. 3, no. 1, 2012, pp. 36-45.
9. C.-L. Fok, G.-C. Roman, and C. Lu, "Agilla: A Mobile Agent Middleware for Self-Adaptive Wireless Sensor Networks," *ACM Trans. Autonomous and Adaptive Systems*, vol. 4, no. 3, 2009, article no. 16.
10. C. Bettini et al., "A Survey of Context Modeling and Reasoning Techniques," *Pervasive and Mobile Computing*, vol. 6, no. 2, 2010, pp. 161-180.

**Sasitharan Balasubramaniam** is a research fellow at Tampere University of Technology, Finland, and Waterford Institute of Technology, Ireland. His research interests include the bioinspired future Internet and molecular communications. Balasubramaniam received a PhD in computer science from the University of Queensland, Australia. He is a member of IEEE. Contact him at [sasib@tssg.org](mailto:sasib@tssg.org).

**Jussi Kangasharju** is a professor in the Department of Computer Science at the University of Helsinki, Finland. His research interests include information-centric networks, content distribution, opportunistic networks, and green ICT. Kangasharju received a PhD in computer science from the University of Nice Sophia Antipolis/Institut Eurécom. He is a member of IEEE and ACM. Contact him at [jussi.kangasharju@cs.helsinki.fi](mailto:jussi.kangasharju@cs.helsinki.fi).