Chapter 6
Internet of Things for Advanced Targeted Nanomedical Applications

6.1 Introduction

The fundamental idea behind nanomedicine is to improve the efficiency of medical and healthcare systems using nanotechnology concepts, devices, tools, technologies and techniques. On the other hand, another nanotechnology offshoot, molecular communication engineering, considers the design and development of nano-scale devices and machines that can communicate by means of biochemical information exchange. By integrating the concept of molecular communication into nanomedicine [1], the coordination of activities and information sharing among several nanomedical devices and machines can be achieved, which results in expanded potentials in the medical and healthcare systems. The concept of ATN takes advantages of the MC-nanomedicine synergy by incorporating historical information of the patient as well as real-time biosignal information to personalise disease treatment, as well as monitor/control the therapeutic process. The interconnection of the network of nanosystems and the body area network of biosignal sensors [2], as well as the off-body processing unit, forms the basic heterogeneous network of an ATN solution.

With the rise in global population, coupled with the low number and uneven distribution of medical personnel, the need for a new approach to global healthcare delivery that will ensure that medical aids get to wherever and whenever it is needed, is necessary. Over the years, the concept of the Internet of Things (IoT) [3, 4], which enables the connection and communication of physical objects with anything, anywhere, at any time using embedded wireless capabilities [5], has become the focus of research and industrial interest. It has been predicted that the IoT will create opportunities for more direct integration of the physical world into computer-based systems, resulting in improvements in many facets of life, economic benefits and reduced human intervention. With regard to nanotechnology and healthcare delivery, the concept of the IoT has ushered in related concepts such as the Internet of NanoThings (IoNT) [6], the Internet of Bio-NanoThings (IoBNT) [7], and Internet of Bio-NanoThings for Ambient Assisted Living (IoBNTAAL) [8] into the research and industrial domain. The IoNT considers the potential of making nanomachines

U. Chude-Okonkwo et al., *Advanced Targeted Nanomedicine*, Nanomedicine and Nanotoxicology, https://doi.org/10.1007/978-3-030-11003-1_6

to communicate using the Internet platform. The IoBNT projects the prospective application domain where the activities of nanosystems operating in an in-body nanonetwork can be monitored and controlled through the Internet. The IoBNTAAL specialises the IoBNT to ambient assisted living. By synergising nanotechnology and the Internet on a platform, these technologies aim at ensuring that medical aids get to people wherever and whenever they are needed. These technologies have the potential to also offer remote fitness programmes, epidemic control and elderly care.

The ATN can greatly benefit from the promises of the IoT. In this sense, the IoT-ATN synergy, which is simply referred in this book as IoT-ATN, taps into the benefits of the IoNT, IoBNT and IoBNTAAL to provide personalised nanomedical therapy, monitoring and control anywhere, anytime and for anyone. The resources, knowledge and expertise that are not available at the patient's physical location can be accessed through the Internet by the ATN solution.

6.2 Layered Architecture and Essential Components of IoT-ATN Solution

In the IoT-ATN system, ATN considers tapping into the capabilities of the IoT to query the states of a set of living and non-living systems and to change their states as required in order to tackle medical challenges in an unprecedented way. To be able to query and alter the states of the living and non-living systems in the network, there is a need for embedded sensors, actuators, processors and transceivers, which have to work in harmony. In this chapter, the conceptual layered architecture of the IoT-ATN solution that ensures effective connectivity among the IoT-ATN devices and services is introduced. This layered architecture will facilitate the identification of opportunities in each layer and across the layers.

6.2.1 Layered Architecture

Just like for the IoT [10], the devices, nodes and firmware/software applications that are connected together in an IoT-ATN system require a de facto standard to ensure seamless interoperation. A layered architecture for the IoT-ATN application is presented in Fig. 6.1.

6.2.1.1 Environment of Things Layer

This layer comprises the objects or places where the observations and activities of the nanosystems and sensors take place. The basic object is the patient or patients (in the case where multi-patient response is required) in whose body the nanosystems and

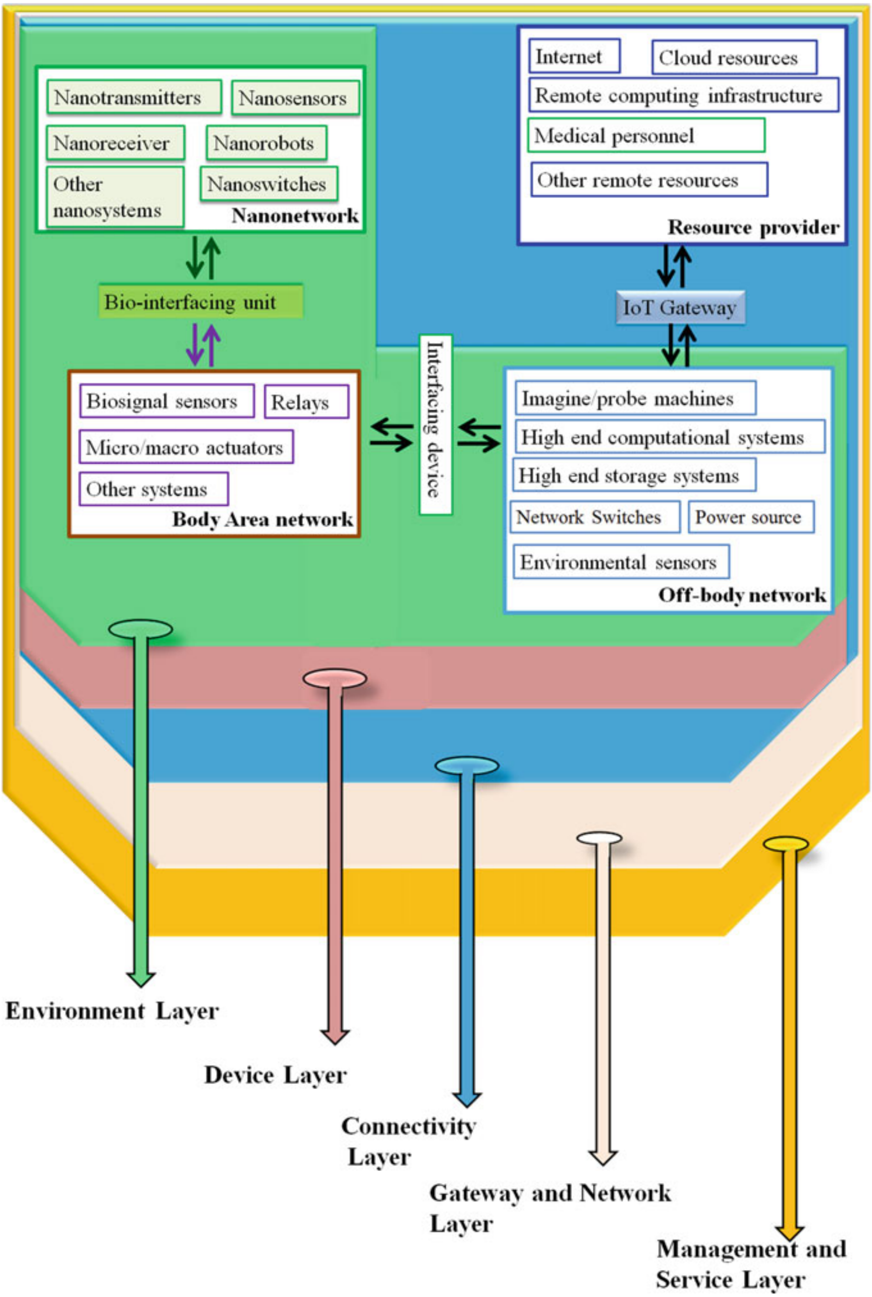

Fig. 6.1 IoT-ATN layered architecture

sensors/other devices work. The ‘places’ can be the immediate environment where the patient is at the time of observation.

6.2.1.2 Device Layer

This is a physical layer where hardware such as nanosystems, body area sensors, relays, environmental sensors, tags, readers and embedded systems are considered. In the IoT-ATN, the nanosystems form an in-body nanonetwork, while the body area sensors/actuators and other devices form the body area network. The nanosensors in the nanonetwork work inside the body to acquire information on the various states of the patient’s internal environment, cells, tissues and organs, as well as of the activities of other nanosystems in the nanonetwork. The body area sensors/actuators and other devices form the body area network in the IoT-ATN and acquire some biosignal information of the patient, externally. Sensory information on environmental conditions like temperature, humidity, air quality and movement can also be acquired using environmental sensors that are resident in the off-body network. Tags may be located in the body area network or off-body network for information storage. And embedded edge processors (centralised or distributed) will usually be employed to process acquired information.

6.2.1.3 Connectivity and Data Processing Layer

This layer takes care of the communication connectivity and data processing among the various nanosystems in the nanonetwork, the devices in the body area network and those in the off-body networks. The diversity in the communication formats among the different networks necessitates that this layer be separate from the gateway and network layer discussed below. Concerns at this layer include the physical placement and configuration of the network devices to achieve the desired goals. The achievement of good connectivity among the nanonetwork nanosystems requires the development of network technologies that depend on biological signalling and other appropriate signalling functions for information exchange in an in-body nanonetwork. For the body area and off-body networks, technologies such as Wi-Fi, ZigBee, ultrawideband (UWB) and Bluetooth can be used to connect the devices. Furthermore, this layer takes care of the processing of the information that is passed around the respective networks in a way that enables real-time information collection and processing as may be required.

6.2.1.4 Gateway and Network Layer

This layer performs the basic role of connecting the nanonetwork, body area network, off-body network and the Internet together. Issues such as routing and addressing, network/transport capabilities and error detection/correction are considered in this layer.

These functions will be handled by some kinds of nanogateways, microgateways and macrogateways [11]. Due to the diversity in the various constituent networks in the IoT-ATN environment, which entails the availability of many different networking technologies and access protocols, this layer should be able to handle connectivity in a heterogeneous network.

6.2.1.5 Management and Service Layer

This layer coordinates and manages the diverse network service providers within the IoT-ATN setting. Its functions include data and application management, control, security, monitoring, storage, organisation and visualisation across various services. In this layer, different policies such as quality of service management, traffic management, device management, traffic engineering, business process modelling/execution, packet inspection, identity management, access authorisation and functions that can be applied to better manage the information generated by all the devices and network constituents are considered.

6.2.1.6 Application Layer

This layer is responsible for delivering various applications that provide user interface within the IoT-ATN environment. It defines the applications in which the IoT-ATN can be deployed, which in this case is the personalised medical care delivery.

6.2.1.7 Essential Components of IoT-ATN Solution

An IoT-ATN application system comprises primary components such as sensing, actuation, communicating, firmware/software, virtual resources and energy components.

6.2.2 Sensing Components

The sensing components gather information from the points of activities in the IoT-ATN system. This can be the information captured by the in-body nanosensors, implants, on-body sensors, off-body sensors and other wearable devices. The diversity in the sensing methods of these heterogeneous components could be a challenge to information processing and analysis.

6.2.2.1 Actuation/Moving Components

These components include nano-, micro- or macro-machines such as molecular motors, nanorobots, micro-robots and moving parts that are involved at any point of activity in the IoT-ATN system. Usually, information gathered from the sensing components is used to activate these components to act in a desired manner in order to achieve an effectively controlled ATN process.

6.2.2.2 Communication Components

The communication components are the devices whose function in the IoT-ATN system is to ensure optimal communication between the various components, systems and networks. These include the nano-, micro- and macro-transmitters, receivers, switches and routers; local area network (such as Wi-Fi, Bluetooth, ZigBee); the Internet; and virtual systems like the cloud (for big data storage). The importance of the cloud can be seen in the need to access or store massive information during the deep curation process of designing and developing nanosystems for the application.

6.2.3 Firmware and Software Components

To make information such as data, graphs, images, and audio available to the users in a simple and transparent format for the IoT-ATN process, various firmware and software are required. This necessitates the design and development of robust and accurate user interfaces that provide an optimised experience across multiple communicating device platforms.

6.2.3.1 Virtual Resources

Due to the crucial requirement for processing and storing data generated in the various networks within the IoT-ATN system, there is a need for efficient computational and storage systems. These systems can be some high-end processing mobile systems, or supercomputers with high computational and storage capabilities.

6.2.3.2 Energy Components

To be able to power the devices and networks in the IoT-ATN system, there is a need for energy sources. Unlike the conventional IoT, the IoT-ATN requires different types of energy sources to power the different systems in the network. For instance, while most electronic devices will be powered by batteries and other conventional power sources, the in-body bio-nanosystems will be powered by biological/biochemical sources that may mimic the mechanisms of the adenosine triphosphate (ATP) synthase in natural cells. The ATP synthase is an enzyme that creates the energy molecules called ATP in the cells [12]. The ATP synthase working involves the accumulation of torque by twisting a rod-shaped structure composite. The discharging of this torque by the rotation of the structure provides the energy for the synthesis of the ATP molecules.

6.3 Characteristics of IoT-ATN Applications

The fundamental characteristics of the IoT-ATN are as follows.

6.3.1 Diverse Network Devices

The devices and nodes that can be connected to the IoT-ATN systems are very diverse in composition and dimension. They could range from macro-size to nano-size in dimension, and from living to non-living in composition. In the IoT-ATN scenarios, usually, there may be so many nanosystems operating in the nanonetwork and a handful of body area sensors and other important on- and off-body devices. Hence, timely and efficient processing of the sensor data and the resultant control activity are needed.

6.3.2 Heterogeneity of Signalling

Unlike the signalling among devices in the conventional IoT, whose nature is mainly electromagnetic, signalling in the IoT-ATN systems is typically diverse. Truly, signalling in the IoT-ATN is usually the combination of all the signalling formats discussed in Chap. 2, namely, electromagnetic, biological, chemical, electrical, magnetic, optical, acoustic, and so on. With each of these signalling formats having different characteristics, the design and development of the IoT-ATN solution will be very challenging.

6.3.3 Diverse Timescale of Communication Processes

Dissimilar to the conventional electromagnetic-based IoT, whose communication processes are physical in nature, IoT-ATN communication processes are typically a combination of physical and biological (biochemical) processes. For instance, within the in-body nanonetwork, it is known that the process of molecular diffusion that mainly governs communication between nanosystems is a physical process; the interactions between the transmitted molecules and the nanoreceiver surface receptors involve biophysical processes; and the intracellular processing of received signals is basically biological in nature. These different types of nanonetwork communication processes usually operate on different timescales, which can range from nanoseconds to years. For example, the diffusion time step can occur in nanoseconds [13] with diffusion over 1 μm occurring in about 10–100 ms [14]; protein–protein interaction can occur in seconds [15]; ligand–receptor residence time can be in milliseconds [16]; and enzyme turnover time can be in microseconds [14]. On the other hand, the timescale of the electronic communication processes of the core IoT can occur at the speed of light. This diversity will make the design and development of the IoT-ATN solution very challenging.

6.3.4 Dynamism

The states of the devices and functions in the IoT-ATN system change as functions of space, time and composition. For instance, the position of nanosystems in a nanonetwork may change inadvertently or not in the course of the process. On the other hand, the position of the body area sensors may change due to variations in the patient's orientation (position change). These dynamic processes can influence the working of the entire IoT-ATN system.

6.3.5 Heterogeneity in Energy Source and Forms

Coupled with the huge data demand of the IoT, the heterogeneity in the type and characteristics of the devices in the IoT-ATN implies diverse forms and amount of energy required in the network. For instance, energy sources for the off-body and on-body systems will mostly be batteries and other conventional power sources, and the in-body nanosystems will be powered by biological/biochemical sources. Such sources may mimic the mechanisms of the ATP synthase in natural cells as mentioned earlier.

6.4 Challenges of IoT-ATN

The IoT-ATN process involves interaction among living and non-living systems in the multiple networks. In comparison to the conventional IoT, while the design, development and configuration of the various composite devices for IoT applications are well-established, the IoT-ATN and its umbrella technologies are still at the infant stage. As an offspring technology of the IoT, most of the challenges in IoT [17, 18] abound in IoT-ATN. Here, we highlight some of the unique challenges of designing and implementing the IoT-ATN. These challenges include nanonetwork interface, data fusion and analysis, nanonetwork energy management and conservation, security, privacy and standards/policy.

6.4.1 Nanonetwork Interface

A very crucial challenge that is unique to the IoT-ATN is the design and development of effective units that can be used to interface between two nanonetworks, or between a nanonetwork and a body area network/off-body network. The nanonetwork–nanonetwork interface requires what may be termed a nanogateway or microgateway, depending on the size of the gateway. The gateway/interface for the nanonetwork-body area network/off-body network will most likely be a microgateway or macrogateway depending on the size of the gateway. The architecture and working principle of these gateways, which typically resides in the gateway and network layer of the IoT-ATN protocol, depends on nature/format of the communication signals, the channel through which the signal will be propagated and the transmit/receive requirements of the communicating network access points. Unlike the gateway devices in the conventional IoT, whose nature is mainly electromagnetic, signalling in the IoT-ATN systems is typically the combination of diverse signalling. Hence, the design of protocols to manage the multiple signalling formats of the IoT-ATN implies that the gateway should be able to handle such a challenge. In such design, one is compelled to ask whether the biological nanonetworks are suitable for the transmission of the 'traditional' types of traffic such as video, images and audio. The answer is most likely no. Even when the transmission of such traditional traffic is required, achieving it with say, biochemical signalling will be challenging.

In the design of the IoT-ATN gateways, inspiration from natural biological systems and phenomena will be very helpful [19]. Some proposals for addressing the interface issue have been presented in [20, 21]. More recently, the architecture and model of a bio-cyber interface for connecting the conventional electromagnetic-based Internet to the biochemical signalling-based bio-nanonetwork is presented in [9, 22].

6.4.2 Information Fusion and Analysis

Information fusion and analysis in the IoT-ATN fundamentally focus on the combination of information from sensors, databases and other related sources in the network. This information is processed and explored in the most optimal manner possible to obtain estimates of some unique characteristics of the process. In the IoT-ATN, there are sensors of different kinds producing diverse information formats of diverse signal strength/complexity, and with different delay, bandwidth and throughput requirements. Examples of the IoT-ATN sensor information and other

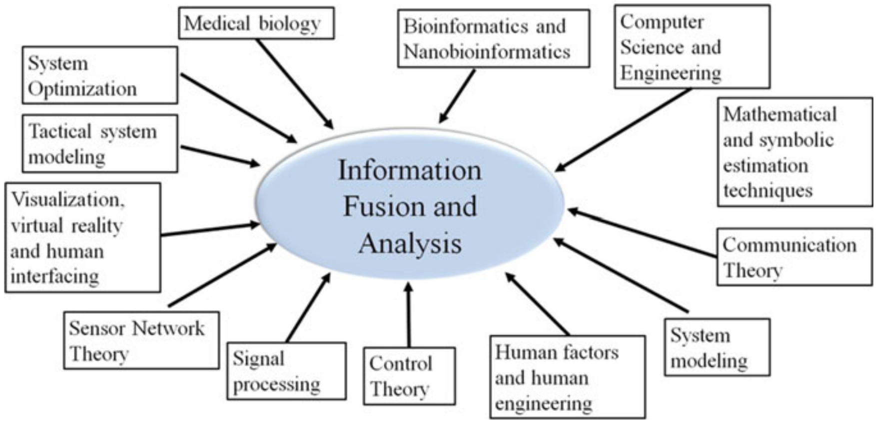

Fig. 6.2 Multidisciplinary design model of information fusion and analysis

information sources include biosignals such as electromagnetic signals, electric signals, hormonal signals, blood glucose variation, blood pressure, neuronal signals, electrical signals (from electroencephalograph, electrocardiograph, electromyography, etc. sensors), and other closely associated signals and sources such as bioluminescence, fluoresces and databases. Issues and challenges, such as whether to consider centralised, distributed [23, 24] or hybrid processing, also arise.

To deliver the promises of ATN, the information from these diverse multisources has to be fused and processed to obtain the desired results, which are challenging tasks. The process requires the design and implementation of a heterogeneous multisource information fusion and processing system based on a multidisciplinary approach, as depicted in Fig. 6.2. The sub-disciplines mentioned in Fig. 6.2 work together to refine observed information in order to make informed decisions in real time, and possibly to modify the course of the ATN process if desired.

6.4.3 Security Concern

Securing the IoT-ATN devices and networks is an important consideration for allowing multiple devices, vendors and users to participate in a single platform. For example, a set of devices may be associated with a particular service provider; therefore, the control of such devices should only be accessible to the authorised service provider. Also, the issue of unwanted malicious interference in the working of the entire system is an important and challenging concern. Securing the system requires that (i) communication between entities is genuine, (ii) only authorised sources can provide information to the network, (iii) only the desired destination systems can understand given information, and (iv) information cannot be modified by a malicious intruder. The existing methods for securing traditional wireless communication systems cannot be applied to the entire IoT-ATN system for reasons such as low computational capability and large technology variance. For instance, in conventional practice, coding, encryption and steganography are some of the methods used to secure traditional wireless communication systems. In the context of IoT-ATN, some coding schemes have been discussed [25, 26]; however, how these schemes can be practically implemented in a real IoT-ATN nanosystem is unclear, with size and complexity of the nanosystem being defining factors.

Concurrently, privacy will be a major issue to the users present in the network. Due to the integration of multiple devices into a single platform, multiple authorities may have information about who is doing what, which in turn violates the privacy of the users. Consequently, researchers need to consider such cases in order to preserve the privacy of the users while integrating multiple devices into a single platform. The fine-grained control of flows using a software-defined network may be employed to enhance the security and privacy of network traffic [27].

6.4.4 Standards

Within the scope of the IoT, several technologies are typically connected together, and different participating industries and parties define different IoT solutions. Hence, the need to define a standard for IoT to perform common backend tasks in order to guarantee levels of interoperability, manageability and portability across various platforms is important. The same need for standardisation extends to the IoT-ATN, but with the added requirement that the concerns of parties from the medical science sector be integrated. Hence, efforts have to be made to harmonise the regulatory framework for IoT and medical science, specifically, nanomedicine. The Food and Drug Administration regulations/standards and the IEEE Standards Association project, the IEEE P1906.1 [28], can provide some recommended practice that can be employed in defining the IoT-ATN standards. The FDA is a federal agency of the United States of America Department of Health and Human Services responsible for protecting public health by assuring the safety, security and efficacy of human and veterinary drugs and medical products/devices. The IEEE P1906.1 presents guidelines for developing clear, common definitions and a conceptual framework needed to accelerate, solidify and guide nanocommunication research towards practical implementation.

References

1. Chude-Okonkwo UA, Malekian R, Maharaj BT, Vasilakos AV (2017) Molecular communication and nanonetwork for targeted drug delivery: a survey. IEEE Commun Surv Tutorials 19(4):3046–3096
2. Dressler F, Fischer S (2015) Connecting in-body nano communication with body area networks: challenges and opportunities of the Internet of nano things. Nano Commun Netw 6(2):29–38

3. Atzori L, Iera A, Morabito G (2010) The Internet of things: a survey. Comput Netw 54(15):2787–2805
4. Li S, Da Xu L, Zhao S (2015) The Internet of things: a survey. Inf Syst Front 17(2):243–259
5. Miorandi D et al (2012) Internet of things: vision, applications and research challenges. Ad Hoc Netw 10:1497–1516
6. Akyildiz IF, Jornet JM (2010) The Internet of nano-things. IEEE Wirel Commun 17(6):58–63
7. Akyildiz IF, Pierobon M, Balasubramaniam S, Koucheryavy Y (2015) The Internet of bio-nano things. IEEE Commun Mag 53(3):32–40
8. Chude-Okonkwo UA, Malekian R, Maharaj BT, Chude CC (2015) Bio-inspired approach for eliminating redundant nanodevices in Internet of Bio-Nano Things. In: IEEE Globecom Workshops (GC Wkshps), 6 Dec, pp 1–6
9. Chude-Okonkwo UA, Malekian R, Maharaj BT (2016) Biologically inspired bio-cyber interface architecture and model for Internet of bio-nanothings applications. IEEE Trans Commun 64(8):3444–3455
10. Sethi P, Sarangi SR (2017) Internet of things: architectures, protocols, and applications. J Electr Comput Eng 2017:1–25
11. Balasubramaniam S, Kangasharju J (2013) Realizing the Internet of nano things: challenges, solutions, and applications. Computer 46(2):62–68
12. Yoshida M, Muneyuki E, Hisabori T (2001) ATP synthase: a marvellous rotary engine of the cell. Nat Rev Mol Cell Biol 2(9):669–677
13. Biedermann J, Ullrich A, Schöneberg J, Noé F (2015) ReaDDyMM: fast interacting particle reaction-diffusion simulations using graphical processing units. Biophys J 108(3):457–461
14. Shamir M et al (2016) Snapshot: timescales in cell biology. Cell 164(6):1302
15. Perkins JR et al (2010) Transient protein-protein interactions: structural, functional, and network properties. Structure 18(10):1233–1243
16. Sanders CR (2010) Biomolecular ligand-receptor binding studies: theory, practice, and analysis. Vanderbilt University, pp 1–42
17. Sundmaeker H, Guillemin P, Friess P, Woelfflé S (2010) Vision and challenges for realising the internet of things. Cluster Eur Res Projects Internet Things, Eur Commision 3(3):34–36
18. Chen S, Xu H, Liu D, Hu B, Wang H (2014) A vision of IoT: applications, challenges, and opportunities with China perspective. IEEE Internet Things J 1(4):349–359
19. Roberts JR, Park J, Helton K, Wisniewski N, McShane MJ (2012) Biofouling of polymer hydrogel materials and its effect on diffusion and enzyme-based luminescent glucose sensor functional characteristics. J Diabetes Sci Technol 6(6):1267–1275
20. Yonzon CR, Stuart DA, Zhang X, McFarland AD, Haynes CL, Van Duyne RP (2005) Towards advanced chemical and biological nanosensors: an overview. Talanta 67:438–448
21. Nakano T, Kobayashi S, Suda T, Okaie Y, Hiraoka Y, Haraguchi T (2014) Externally controllable molecular communication. IEEE J Sel Areas Commun 32:2417–2431
22. Kuscu M, Akan OB (2016) The Internet of molecular things based on FRET. IEEE Internet Things J 3:4–17
23. Pottie GJ, Kaiser WJ (2000) Wireless integrated network sensors. Commun ACM 43(5):51–58
24. Xu Y, Qi H (2004) Distributed computing paradigms for collaborative signal and information processing in sensor networks. J Parallel Distrib Comput 64(8):945–959
25. Shih PJ, Lee CH, Yeh PC, Chen KC (2013) Channel codes for reliability enhancement in molecular communication. IEEE J Sel Areas Commun 31(12):857–867
26. Lu Y, Higgins MD, Leeson MS (2015) Comparison of channel coding schemes for molecular communications systems. IEEE Trans Commun 63(11):3991–4001
27. Ahmad I, Namal S, Ylianttila M, Gurtov A (2015) Security in software defined networks: a survey. IEEE Commun Sur Tutorials 17(4):2317–2346
28. IEEE P1906.1—Recommended practice for nanoscale and molecular communication framework