Chapter 11
Internet of Things: Current Trends and Emerging Prospects

Amartya Sen and Sanjay Madria

Abstract The prevalence of Internet of things (IoT) paradigm has seen the rise of many useful applications in the domains of healthcare, industries, smart city, and so on. However, the paradigm itself is in its dormant stages and still has many open-ended research challenges like interoperability, security and privacy, compliance, and standardization issues which need to be addressed. In this paper, we present a high-level discussion of the overall implications of the IoT paradigm with respect to different application areas and scenarios, domains, and technicalities that needs to be focused for effective incorporation of the IoT concept. Additionally, we also discuss briefly some of the future prospects that can improve the current trends of IoT frameworks.

Keywords Internet of Things · IoT Applications and Challenges · security and risk assessment · overlay networks

11.1 Introduction

The Internet of things (IoT) paradigm and its applications to various domains like industries (Industrial Internet of things or IIoT), healthcare, and smart cities have received considerable attention in the past few years. According to IHS estimates, in 2015, there were 15.4 billion connected devices, and it is projected to rise up to 30.7 billion and 75.4 billion by 2020 and 2025, respectively [19]. In 2016 alone, IDC estimated that there were 28.3 million wearable devices sold and forecasts this value to reach 82.5 million units by 2020 [16]. Given such exponential increase in the number of interconnected devices, the global spending in IoT-related applications was estimated to be around $737 billion in 2016, which will further grow to $1.29 trillion by 2020 [17]. Additionally, the IoT paradigm will contribute about $10 to

A. Sen · S. Madria (✉)
Department of Computer Science, Missouri University of Science and Technology, Rolla, MO, USA
e-mail: asrp6@mst.edu; madrias@mst.edu

N. S. V. Rao et al. (eds.), *Proceedings of International Symposium on Sensor Networks, Systems and Security*, https://doi.org/10.1007/978-3-319-75683-7_11

$15 trillion to worldwide GDP growth. Such statistics are not an exaggeration since in 2017 it is estimated that approximately 60% of the global manufacturers will use analytics on data recorded from connected devices to outline actionable insights and develop optimized plans and processes for their workflow [40]. These are some of the staggering information which indicates that the IoT paradigm is growing at an unprecedented rate.

In the recent past, we have seen the maturity of several computing platforms like the cloud (including edge and fog computing) as a way to pool computing resources and offer services in the form of pay-as-you-use models. Further, the developments in hardware efficiency for sensor nodes [33] have also made it easier to own and maintain your wireless sensor networks (WSNs). Additionally, platforms like Sensor Cloud [21] have also made it easier to avail sensing services for users who may not own a WSN. There has also been a growth in other types of sensing devices such as wearable body sensors, RFID tags, and so forth. All these devices and their networks generate a vast amount of data everyday [44]. To make meaningful use of these data streams, we must be able to connect together these isolated islands of devices and their networks and manage them through common interfaces and platforms to perform analytics on the generated data resulting in meaningful and actionable insights applicable across different domains. This is the principal idea behind the IoT paradigm. For example, consider the IIoT services of Michelin's solutions *EFFIFUEL* service whose objective is to reduce the fuel consumptions in truck fleets [18]. They do so by capturing numerous sensing data such as fuel consumption, tire pressure, speed, and geography which are then transmitted to a cloud platform wherein they are analyzed and expert recommendations are made on how to optimize fuel efficiency.

The IoT paradigm is no doubt growing faster than our anticipation, having found roots in application domains like industries, healthcare, and smart cities [41]. Nonetheless, the paradigm and its applications itself are in dormant stages and has to traverse a long way to reach complete maturity. Numerous challenges are to be addressed along with establishment of functional and nonfunctional standards. Thus, our objective here is to discuss on a high level some of the existing trends that have taken place in the domain of IoT related to different application scenarios. Furthermore, we will discuss some of their technical aspects which need to be addressed in order to ensure effective utilization of the IoT paradigm. Finally, we will outline some of the future prospects which can improve the feasibility of IoT-based application scenarios along with introducing the concept of incorporating overlay networks for IoT frameworks which will help in facilitating a user-centric service model, capturing their desired quality of service (QoS) and security preferences.

11.2 IoT Application Scenarios

As mentioned in the previous section, the idea behind IoT and its applications is to interconnect different platforms together and make pragmatic use of the generated data. These networks typically are composed of sensory devices like

sensor nodes, RFID, and wearable body sensors. However, while implementing them for different application scenarios like healthcare or industries, we should not rely on traditional protocols of framework interconnectivity and interoperability. An effective approach requires to evolve implementation models weaving together different aspects of an IoT application scenario along with keeping the users (or consumer) of the services in the center of the service models. These kinds of models will not only require the interconnectivity between networks in the same application scenario but also across different application scenarios. In this regard, we will discuss some of the IoT frameworks belonging to different application scenario.

11.2.1 IoT in Healthcare Applications

IoT enables consistent and remote monitoring for patients in the healthcare domain [15]. Integration of sensing platforms like room sensors, wearable body sensors, and medical equipments like ECG and X-ray machines [37] to Cloud platforms realizes this scenario. Medical professionals can access the data and other analytical services [5] applied on it to take appropriate actions. IoT-based healthcare can provide tailor-made services for individual patients which can be further extended to the premises of their household. Therefore, health monitoring services need not stop once a patient leaves the confines of a hospital. This will be especially useful in activities such as medical therapy and recovery. Additionally, data can also be captured and integrated from the pharmaceutical companies to optimize operations such as logistics, supply chain management, and simulation of drug studies which will keep doctors in the loop and their understanding of patient's conditions to boost the performance of drug development.

11.2.2 IoT in Industries

IoT has widespread application in a lot of industrial sectors ranging from mining operations [42], agricultural improvements [7], to waste water management facilities [26]. Generally these IoT applications are tailor-made based on the needs and organizational policies of the industries where they are incorporated. However, on a higher granularity, they adopt the IoT domains of gathering data from sensory devices, performing analytics on the collected data, and designing intelligent machines and applications that can act upon the results of data analytics. The driving factor in this domain is to make operations cost-efficient but at the same time improve overall productivity. For example, delays and cancellation in the US passenger and cargo aviation cost the industry nearly $11 billion on a yearly basis in terms of maintenance, logistical investments, and so forth. To address this, a joint effort between Accenture and GE aviation was undertaken, called Taleris [13], which was designed using IoT concepts. Taleris is an airline fleet optimization service whose objective is to eliminate avoidable repair costs and minimize delays and disruptions in service availability due to foreseeable conditions. It does so by

collecting data from sensory components accompanied with the aircrafts to monitor the operational conditions and health of different aircraft parts. The collected data is then used to outline optimized predictive maintenance schedules. In doing so, the IoT service can also take into consideration where and when (accounting for the aircraft route) the maintenance operations should be performed in order to minimize disruptions. These kinds of applications can be further improved by integrating it with frameworks that can determine the optimized routes for aerial vehicle trajectories based on different task requests from the ground control [22].

11.2.3 IoT in Disaster Management and Response

Carrying out response and rescue operations in disaster-affected regions is a challenging task since these regions are typically characterized by areas that are devoid of information exchange. Many a times, time-critical rescue operations are to be performed (forest fires) and therefore a need for coordinated efforts exists across a span of geographical region for optimized resource allocation. This is where the concept of IoT-based applications will be beneficial. For example, consider the IoT-based disaster management framework depicted in Fig. 11.1. It consists of physical infrastructure enumerated by IoT devices such as cell phones, wireless sensors, wearable body sensors, RFIDs, gathering and relaying data like CO_2, temperature, user heart rate, and images and video feeds to a management platform like Sensor Cloud. The collected data can be analyzed and queried by regular users to avail information such as k nearest safe zones or evacuation routes. In contrast, rescue workers and first responders can use the Sensor Cloud interface to issue data

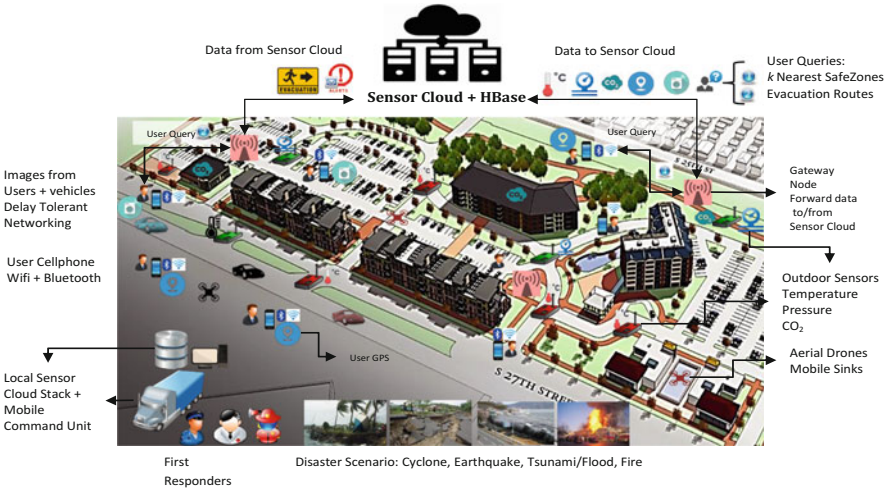

Fig. 11.1 IoT-based disaster management framework

collection tasks across a specified region of interest. The incoming sensory data along with images and video feeds can be used by rescue workers to gauge disaster hit regions they might be entering. Analytics services can also be performed to outline logistical information for the allocation of rescue resources and operations.

These aforementioned IoT application scenarios can also be brought together in order to formulate the foundations of smart cities [43]. Nonetheless, IoT applications and their frameworks should not be just about interconnecting different networks and platforms. It needs to account for the actions that can be performed based on the information obtained from data gathered via the interconnected platforms. In doing so, the users of these frameworks need to be at the center of operations such that user feedbacks and preferences can be immediately tied up to the operational functionalities of the infrastructure for optimal service facilitation.

11.3 Success Factors: Domains and Technical Implications

In the era of IoT advancement, infrastructure providers and manufacturers should not remain disconnected from their consumers. As the IoT paradigm provides a connected ecosystem of users, infrastructure, their behavioral data on which one can perform real-time analytics to suggest and outline actionable insights, there is a need to develop new operational models based on a hybrid concept of developing the products along with providing services and support associated to those products. These kinds of product-service models will essentially need to be user-centric, for example, integrating consumer usage data to product development life cycle management, or performing analytics on the sensory data generated by different devices to schedule predictive maintenance operations to prevent permanent breakdown of devices. The effective realization of the IoT paradigm through the product-service hybrid model depends on successful implementation in some few key domains. At a higher level of granularity, these domains can be summarized as:

- Sensor-driven computing
- Analytics on collected data
- Self-aware applications
- Seamless user integration

Sensor-driven computing is the core building block of IoT implementation across any application scenario. An apprehension of the environment is required to develop and perform any task related to it. This sort of desired outcome can be achieved through the embedded sensing capabilities of the interconnected sensory devices which are growing at a remarkable rate. The sensing capabilities can provide data on temperature, pressure, and CO_2 levels of the surroundings. Whereas new generation wearable body sensors can relay attributes such as heartbeat rate, blood pressure, and so forth. Furthermore, improvements to the hardware implementations and cost of sensory devices [10, 33] are enabling it with possibilities which could not have

been feasible with the traditional sensor nodes running on AA batteries and having limited processing capabilities. We also need to pay attention to efficient techniques of data collection algorithm which will save energy and operational cost in IoT environments [20] and incorporate novel techniques of data compression [9] that will improve the bandwidth consumption and be able to convey more information in a packet size as compared to the traditional scenario.

Data analytics is the key feature that helps in converting the perception provided by the sensory devices about its users and the environment into actionable insight. It is the primary component of the *service* part in the product-service hybrid model. Data analytics can generate actionable tasks like processing the sensory data from the equipment of manufacturing machinery and forecasting predictive maintenance scheduling. These kinds of analytics on sensor-driven computing have been put to practice, for example, *Caterpillar* is using industrial analytics on their dealer's sensory information originating from machines and engines, to give them feedbacks which will help in proactive engagement of any likelihood of operational failure [31]. Similarly, companies like Virtual Radiologic Corp. (vRad) is providing analytics services in the healthcare scenario by collecting and interpreting data from X-ray and MRI [37]. The role of analytics in this ecosystem is of primary importance as it cannot only suggest actionable tasks but eventually shape the public opinion about the products and devices that make up the infrastructure of an IoT framework. Although, as required in some time critical application scenarios, generating relevant actionable tasks depend upon analytics to be performed in (hard or soft) real-time. Furthermore, with the exponential rise in the number of interconnected devices, the amount of data being generated every minute can be overwhelming [35]. Therefore, traditional models of data analytics need to be revised and made more optimized to be incorporated in the IoT scenario [44].

As we traverse toward the end of the maturity spectrum for the IoT paradigm and its related applications, the future lies in the prospect of developing self-aware intelligent applications. In this regard, applications and machines in the future should be able to integrate the analytics outcome and user preferences to their product life cycle in order to perform autonomous improvements and upgrades. Applications across different platforms will also be able to interact with each other to make intelligent operational decisions further consolidating the IoT paradigm of global interconnectivity. A dormant example of such a product can be found in the Nest Thermostat which can interact with its users to comprehend and then manage their energy consumptions [23]. Products like these can be made to interact with networks such as smart electric grids in order to optimize the energy consumption of smart cities. Current practices of serving as a medium for machine-to-machine interaction can also be found in applications like Volvo's CareTrack [38] wherein it can generate reports aiding users to optimally manage their truck fleets. Looking ahead, incorporation of intelligent machines and applications will enable scenarios such as entire factories operating based on interaction between different machines with little to no human oversight thereby boosting productivity. These kinds of autonomous self-aware intelligent machines and applications will be able to launch tasks by cooperating and organizing among themselves. They will be able to self-

incorporate the feedback gained from analytical services and users to improve their interfaces and operational aspects. This in turn will help to reduce their operating costs and improve overall output. Being self-aware will also enable them to prevent accidents and failures during their operations. However, the most challenging aspect among the desired features of intelligent machines and applications will rest in their capability to operate under uncertain and adverse conditions.

Users need to be at the crux of any application scenario that we might develop. Consumer behavior and preferences help shaping and improving the operational standards of products and applications. Hence, the product-service hybrid models that will help in the effective incorporation of the IoT paradigm in different application scenarios need to be user-centric. In this regard, one must be able to take into consideration a user's preferences in terms of their quality of service and experience (QoS and QoE) [12] as well as security requirements [24, 34]. Currently, works mostly address the inclusion of QoS requirements in their IoT application scenarios to improve the overall performance. Some introductory approaches also discuss the decomposition of security requirements and address it across different layers of their IoT applications [29]. However, these incorporations need to be performed from the user's perspective. Optimization algorithms should be developed to address different aspects like operational costs, performance, security requirements, and implementations via the computed (and requested) feedbacks which must be dynamically incorporated by machines and applications in near real-time. These kinds of approaches will further consolidate the concepts of intelligent machines and applications to tailor themselves autonomously as per user requirements.

Nonetheless, addressing the success of these aforementioned domains will be challenging as some of the technical aspects of traditional computing platforms should be changed such that it can be implemented in the IoT ecosystem. We outline two such areas—networking and interoperability, cybersecurity and risk assessment in the following subsections.

11.3.1 Networking and Interoperability

A typical IoT-based application is composed of numerous devices, each having their own unique architecture, software, and hardware specifications. The interconnectivity between these devices and their networks in such a heterogeneous environment is not a trivial task [32]. Networking and interoperability is one of the primary challenges that need to be addressed in order to make strides of progress toward the maturity of IoT-based applications. Dynamic discovery of participating devices, providing resilient services, autonomous service negotiation, and facilitation are some of the key IoT features that are desired and challenged by the lack of standardized networking and interoperability techniques [6]. In a practical scenario, it is safe to assume that in the near future, the hardware and architecture of the participating devices like sensor nodes, RFIDs, and others will not change drastically. As such, the task of networking and facilitating interoperability lies in developing efficient software for these devices, designing frameworks and networking protocols that

will help bridge the gap. An instantiation of ongoing efforts in this regard can be found in AllSeen Alliance's AllJoyn framework [1] which aims to provide developers achieve interoperability between their devices in an IoT ecosystem. The framework facilitates connectivity between device-to-device and the cloud platform which helps to bypass the hassles of transport layer protocol and other heterogeneity challenges that may arise due to device brands, platforms, and operating systems. Another beneficial feature of the AllJoyn framework is in being an open source framework which currently has more than 180 contributing technology partners like LG, Microsoft, and Qualcomm. Other notable efforts lies in the proposed (yet dormant) information-centric networking (ICN) [2] protocol which is about retrieving information and content based on specific naming conventions (instead of IP addresses) which ignores data origination servers and distributed channels. In doing so, the ICN protocol supports in-network caching and replication which will benefit the plethora of resource-constrained devices that partake in a typical IoT application and will allow for the incorporation of content-based security policies which are essentially energy efficient in contrast to their traditional counter parts. This kind of protocol will also benefit data dissemination and networking tasks as it will disregard the heterogeneity of different interconnected platform and their individual traditional networking protocols.

Another effort in addressing IoT-based networking challenges can be found in software-defined networking (SDN) protocol [3, 25] which decouples the network control from packet forwarding and is directly programmable to adjust dynamically based on rate of flow and services. This sort of feature will be useful given the rate at which data is sensed and transmitted in an IoT environment. However, these solutions are in their dormant stages, and a lot of research issues still need to be addressed. We have to consider network management policies (centralized vs. decentralized) with respect to different IoT frameworks used in smart cities, healthcare, or industries. Additionally, issues such as scheduling and link selection also needs to be addressed [11] to optimize attributes like throughput and performance along with reducing the operational costs.

11.3.2 Cybersecurity and Risk Assessment

Cybersecurity and risk assessment is another challenging aspect which needs much attention in the domain of an IoT framework. The challenges essentially arise due to the interconnectivity between vast number of heterogeneous devices, all of which may have different hardware and software specifications. For example, security threats and countermeasures that are applicable to handheld devices are not the same for sensor nodes or wearable body sensors. Additionally, the strength of security requirements varies based on the nature of services provided by these devices and their networks. Therefore, it is not feasible to design universally applicable security measures and policies across an entire IoT framework. Furthermore, certain IoT framework's infrastructures are also composed of devices which may have physical impact like smart electric grid, conveyor belts, and programmable units in the

industry. Being able to exploit or cause malfunction of these devices can have much more dire consequences than traditional cybersecurity outcomes like loss or leakage of data [39].

The IoT frameworks encompass several different layers like infrastructure, services, sensing, and communicates data over wireless and wired mediums. Therefore, the security requirements also span across multiple fields like ensuring confidentiality, integrity, and availability of data. Security requirements also extend to data (user) privacy and anonymity, trust, non-repudiation, authentication, and access control [14]. One way to address all of these security requirements is to individually set up countermeasures across different layers of an IoT framework's protocol stack, for example, physical/MAC, networking, routing, and application layer. Currently, each of these layers follows a set of protocols to realize the overall framework architecture. For example, the constrained application protocol (CoAP) [4] of the application layer, used for interoperability purposes which is coherent with the representation state transfer architecture of the web. The CoAP protocol enables IoT sensing devices to interact with current Internet applications without the need of a specialized translation methodology. Securing CoAP will ensure the security requirements associated with functionalities that are realized by this protocol. Nonetheless, the protocol stack way for addressing security in IoT frameworks is not yet foolproof. There still exist several open-ended research challenges that need to be addressed. Revisiting the CoAP security instantiation which is bounded by the Datagram Transport Layer Security (DTLS) [27], this scheme has its own limitations since it requires to perform a handshake for authentication and key agreement (ECC public key cryptography) purposes with the sensing devices, much of which are resource constrained.

Additionally, security policies and protocols need not remain static throughout the lifetime of an IoT framework. In other words, service requirements may require to give more emphasis on quality of service rather than security for a given instance [24]. In such cases, tradeoffs are required between QoS and security protocols to enable the framework's or user's service demands. This becomes more challenging because to accommodate, for example, the increased QoS factors, we need to reduce the strength of the security protocols, like switch to a lightweight encryption scheme. This sort of action digresses from a framework's initial security requirements estimated by performing risk assessment. Furthermore, different components and users of an IoT framework may have different security requirements. Security requirements may also change with context, evolving threat models and use-case scenarios. This necessitates the concepts of variable and adaptive security requirements, and its implementation is something that also needs to be addressed in the IoT paradigm. Currently in this regard, initial outlines for the concept of adaptive security management have been demonstrated for E-health applications utilizing IoT paradigm [29].

However, before optimal security policies can be designed and applied, one should be able to assess the risks and threats that an IoT framework's infrastructure may be vulnerable to. As such, risk assessment is an imperative step that needs to be performed. However, the task becomes challenging considering the heterogeneity

of the involved infrastructure and the likelihood of scenarios where devices may join and leave the framework from time to time. In this regard, one must be able to account for the logical relationship between the cross-platform devices and how exploitations in one platform may affect the other platforms [30].

11.4 Future Prospects of IoT

IoT-based frameworks are the future of computing platforms that will revolutionize the way we communicate and how services will be carried out. In addition to optimizing the way things are implemented in the traditional domains like industries, healthcare, and smart cities, a lot of scope also lies in IoT's application to promising upcoming sectors like management of renewable sources of energy and its infrastructure. Furthermore, as the analytics on data generated from all the interconnected devices will be used to design more efficient and actionable insights, it can also be incorporated to weave realities and better assist users in this ecosystem of automation. To elaborate further, inclusion of the new technologies like artificial reality (AR) [8] and virtual reality (VR) [36] to IoT-based frameworks can contribute manifolds to supplant the user-centric model which is a necessity in the product-service hybrid framework for IoT applications. For example, in the domain of IoT-based healthcare framework, data from patients' wearable body sensors can be used to monitor their conditions remotely. However, this can be taken a step further and data can be integrated with AR devices to aid users perform basic first aid operations like giving CPR or using devices such as the defibrillator. In an event of emergency and lack of immediate attention from a medical professional, such actions can save a life along with ensuring that the actions are still guided without any risks. Similarly, if we consider the domain of IoT-based applications for disaster management, incoming raw sensory data along with images and video feeds can be used by rescue workers with a virtual reality (AR) platform to gauge disaster hit regions they might be entering. These kinds of incorporations will reduce the uncertainties of entering inside adverse conditions such as buildings on fire and so forth.

11.4.1 Overlay Networks Connecting IoT Devices and User Experience

With the exponential projected increase of interconnected devices, IoT frameworks will be characterized by having devices with redundant sensory ranges. To elaborate this, consider a data collection task from a region consisting of N number of devices. In a traditional approach, such a task will activate all N devices in the region. Although, if n ($n \subset N$) devices are sufficient to encompass the region of interest for

the task, this will make activating all the devices inefficient. A better approach will be to selectively activate certain number of devices such that it covers the region of interest and is able to facilitate the task. This will leave remaining devices to service other tasks in the same region. This kind of practice will also be beneficial in terms of conserving energy of these IoT devices which may be resource constrained as a result of nature of the device (wireless sensor nodes) or circumstances (lack of power in disaster hit regions to recharge or replace batteries). It will also boost the overall throughput and performance of the applications since multiple sensory-driven tasks can be carried out concurrently.

Furthermore, selection of IoT devices should not solely be guided by service parameters (region of interest or duration), but it also needs to account for metrics such as user's Quality of Service (QoS), Quality of Experience (QoE), and security preferences. This kind of outlook will also contribute to the user-centric phenomena for product-service hybrid models for IoT framework. QoS metrics can be measured in terms of network parameters like response time, throughput, packet loss, and so on. However, these kinds of QoS measure do not resonate equivocally with general users. As such, QoS measurement can be estimated by allowing users to express their Quality of Experience. QoE is more subjective in contrast to QoS measurement involving parameters like—given a time window, how does a user feel about a service (emotion), what is the end goal of the user by using this service (objective), and why does a user avail this type of service (incentive). By having users express these QoE metrics, one can measure the desired QoS metrics given the context and time window of the service. Such estimations can be done by either translating the qualitative user QoE responses to quantitative scales or using quantitative measures such as heart rate relayed from body sensors or a hybrid method that integrates both. Another piece in the puzzle for user-centric frameworks should also be able to encompass a user's security preferences as the accumulated data in IoT environments associates directly to a user's personal use and immediate surroundings. For example, consider the case of Nest thermostats or smart grid meters being able to transmit sensor information about the user's energy consumption behavior in their household. Furthermore, in the healthcare domain, majority of the sensed data is coming from wearable body sensors and so forth. If acted upon maliciously, these data can be used to monitor a user's behavior encroaching their privacy or tampering it to provide misleading information which can lead to dire consequences. Hence, service facilitation also requires users to be able to specify their desired security and privacy levels along with service parameters and QoE or QoS requirements. Overlay networks can also help in this regard because it provides the capabilities to selectively choose IoT devices that can satisfy the user requirements and also meet the framework's objectives to carry out the task efficiently.

In the formulation of overlay networks within IoTs, different sensing nodes will form an integral part of the overlays by providing data related to different sensing activities within IoT ecosystem to facilitate multiple tasks in a given time window across a geographical region. The participating IoT devices in multiple networks might be resource constrained (energy or processing power), and therefore, one

cannot incorporate all the desired QoE/QoS, security requirements and dispense the actual services (sensing). Hence, a good balance needs to be achieved between services dispensed and the security availed, adhering to the requirements of user QoE/QoS (in accordance to the user-centric model). In dense deployment of IoT networks, one can use redundant nodes to operate during the same time period to service multiple users, for example, during busy morning walks along a trail route. To generalize this concept, individual IoT nodes belonging to the same or different networks can be selected to form overlay networks on the fly to facilitate service requests [28] from different users spanning different geographical regions, thereby facilitating dedicated virtual infrastructure for users without the need to wait for a task to complete.

In the formulation of overlays in an IoT environment, we can divide service provisioning tasks into two different but correlated modules: *Performance* and *Security*. The variable security policies if addressed across multiple IoT platforms necessitate the need for a layer that will be able to translate the heterogeneous security policies. Although, applying security measures comes at the cost of network's QoS parameters (bandwidth, performance, accuracy, and precision). Users may express security requirements in terms of a lower bound and a security range [34]. The security ranges will be influenced by the nature of the IoT service (e.g., real-time vs. offline data requests) and its effect on network QoS parameters. The minimum security requirements could be in the directions of having accurate data, available with some level of encryption. However, for real-time data access, there will be a higher priority on aspects such as data stream rate as a result of which users may opt for a lightweight encryption scheme with alternate data packet authentication. If users are more concerned about their privacy, it will make them opt for heavyweight encryption schemes and authenticating every data packet. Therefore, a user's desired tradeoffs between network QoS parameters and security requirements can be specified using a security range with a minimum bound. We need to take these user requirements and map them into the available physical infrastructure and security policy encapsulated in the network. Thus, we envision that overlay networks will be formed using a two-tiered decision-making framework: (1) Tier 1, dynamically form overlays that provide optimal services to a user in terms of their QoS requirements, and (2) Tier 2, identify and output the overlays that satisfy a user's security preferences, and if not, users may want to renegotiate the prespecified security preferences.

The formulation of such overlay networks in Tier 1 can be achieved using concepts of Markov decision process, a finite state automaton having four tuples:

$$\text{MDP} = \{S, a, P_a(s_1, s_2), R_a(s_1, s_2)\} \tag{11.1}$$

where, S is a finite set of states of IoT devices belonging to the same or different networks present in the selected region of interest; a is the finite set of actions such as add a device, delete a device, put a device to sleep (active) mode, or change its functionality from one to another. Execution of certain action results in a transition of state which is denoted with a probability $P_a(s_1, s_2)$. Some factors

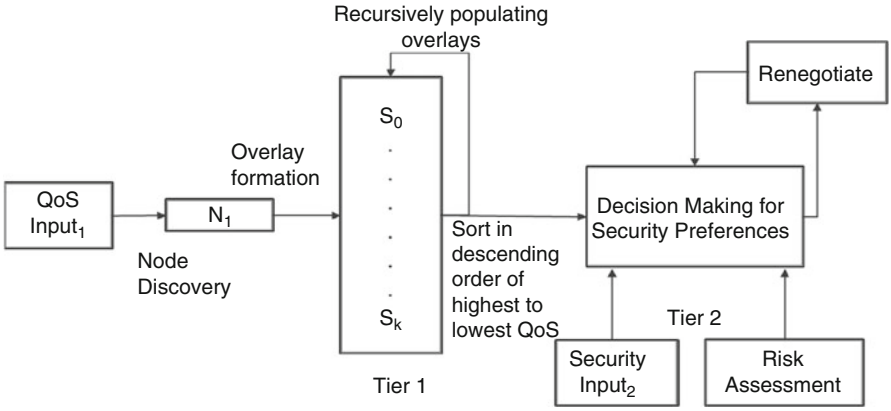

Fig. 11.2 Depicts the framework for formation of overlays for wireless network adhering to user's QoS and security requirements

in the overlay scenario that may affect P_a are remaining energy of the devices, their sensing capabilities and available processing power. The reward or expected outcome of a transition is denoted by $R_a(s_1, s_2)$. In the overlay scenario, rewards will be instantiated (in terms of QoS) to minimize the number of devices required to meet the sensing coverage, to extend the lifetime and continuity of the service, and so forth. The reward criteria for formulated overlays can have a qualitative scoring such as good, bad, and worse. This qualitative scoring will be converted to quantitative scores based on the organizational policies, and the overlays yielding maximum rewards will be shortlisted in descending order by Tier 1 of the decision-making framework (a high-level abstraction is shown in Fig. 11.2) and passed to Tier 2 for security assessment.

Tier 1 uses the QoS specification as input and performs its operation. First, the framework will start with a node discovery process in which it randomly chooses a sensor node available within the region of interest of the user application/task/query. Starting with this node (let us call it the initiator node), it will check whether the application's service region is satisfied or not. If it is unsatisfied, it will reinitiate the node discovery looking for other nodes that will help increase the coverage of the application's region of interest. In this regard, the decision to whether or not add the new nodes to the overlay of the initiator node is aided by an inference engine and Markov decision processes. The inference engine is composed of the following factors: (1) node's sensing capabilities required for the application to run, (2) remaining energy of the node being considered given the running frequency of the application, (3) node's memory and processing power required by the application, and (4) sensing coverage provided by the node being considered. It is desired to form the overlays with the most optimal number of sensor nodes. The aforementioned factors will correspond to rewards of Markov decision processes. The output of Tier

1 will be the feasible sets of overlays that can serve a user's application, sorted in decreasing order of satisfiability in terms of QoS parameters.

Tier 2 will use the output of Tier 1 along with the user's security preferences provided in the initial input. Additionally, it will use the RA (risk assessment) module [30] to compute the security policies of the formed overlays. This module will assess the feasibility of different known attacks in IoT networks and compute the net threat level to the network in terms of a percentage of confidentiality, integrity, and availability. Although we could estimate the threat level on the overlay's security parameters by estimating the impact of different feasible security attacks on a network in isolation, it would not be sufficient since attacks can be used in conjunction to execute more degenerate attacks. For example, a malware attack can subvert a node which can then legitimately participate in network activities causing attacks such a Sinkhole. Attack graphs in this context will help to depict the logical correlation between different feasible attacks. In case the user's security preferences are not met by any of the formulated overlays, then there is a need to renegotiate the user preferences, either in terms QoS parameters or security requirements or both. Along these lines, preferences on security can be higher than that for QoS requirement. In such cases, the decision-making framework can apply risk assessment before applying QoS assessment. Furthermore, this can be taken one step further by performing tradeoff analysis between performance and security and measuring the output by using utility functions to measure multiple options users can select.

11.5 Conclusion and Looking Ahead

This paper provides a summary of different applications and technical issues in the IoT domain and discusses some open research issues. There is lots of research that need to be addressed in this promising paradigm of IoT. To begin with, compliance and regulatory information needs to be established for different application scenarios. There is also a need for standardization techniques related to the fields of IoT networking, analytical services, security, and risk assessment policies. Traditional protocols for varying tasks such as access control or routing need to be modified appropriately so that they are less resource hungry and more effective. Further, the disruption that will be brought about by the adoption of IoT paradigm to legacy systems and their framework also requires much attention so as to ensure that the transition is graceful and does not result in a breakdown. This will also ensure prolonged life cycle of the IoT devices along with continuous operational guarantees. As the IoT-based applications and their framework mature, one can expect to gain dependable interconnected infrastructures that are resilient to foreseeable failures and can communicate with each other to provide smart tailor-made services to the users by utilizing the capabilities of sensing and control.

References

1. AllJoyn: Alljoyn framework. allseenalliance.org/
2. Amadeo, M., Campolo, C., Quevedo, J., Corujo, D., Molinaro, A., Iera, A., Aguiar, R.L., Vasilakos, A.V.: Information-centric networking for the internet of things: challenges and opportunities. IEEE Netw. **30**(2), 92–100 (2016)
3. Bedhief, I., Kassar, M., Aguili, T.: SDN-based architecture challenging the IoT heterogeneity. In: 2016 3rd Smart Cloud Networks Systems (SCNS), pp. 1–3 (2016)
4. Bormann, C., Castellani, A.P., Shelby, Z.: CoAP: an application protocol for billions of tiny internet nodes. IEEE Internet Comput. **16**(2), 62–67 (2012)
5. Boulton, C.: Apple's new health focus comes at propitious time. Wall Street J. (2014). https://blogs.wsj.com/cio/2014/06/10/apples-new-health-focus-comes-at-propitious-time/
6. Bröring, A., Schmid, S., Schindhelm, C.K., Khelil, A., Käbisch, S., Kramer, D., Phuoc, D.L., Mitic, J., Anicic, D., Teniente, E.: Enabling IoT ecosystems through platform interoperability. IEEE Softw. **34**(1), 54–61 (2017)
7. Bunge, J.: Big data comes to the farm, sowing mistrust: seed makers barrel into technology business. Wall Street J. (2014). https://www.wsj.com/articles/no-headline-available-1393372266
8. Buntz, B.: 10 killer applications of the IoT and augmented reality. Internet of Things Inst. News Anal. (2016). http://www.ioti.com/iot-trends-and-analysis/10-killer-applications-iot-and-augmented-reality
9. Cao, X., Madria, S., Hara, T.: A WSN testbed for Z-order encoding based multi-modal sensor data compression. In: 14th IEEE International Conference on Sensing, Communication, and Networking, SECON 2017, San Diego, CA, pp. 1–2 (2017)
10. Carbone, J.: Expect sensor prices to fall. Digikey (2013)
11. Dhondge, K., Shorey, R., Tew, J.: HOLA: heuristic and opportunistic link selection algorithm for energy efficiency in industrial internet of things (IIoT) systems. In: 2016 8th International Conference on Communication Systems and Networks (COMSNETS), pp. 1–6 (2016)
12. Dong, M., Kimata, T., Sugiura, K., Zettsu, K.: Quality-of-Experience (QoE) in emerging mobile social networks. IEICE Trans. Inf. Syst. **E97.D**(10), 2606–2612 (2014)
13. Etihad airways and taleris implement new technology to predict aircraft maintenance faults, reduce flight delays. BusinessWire (2013)
14. Granjal, J., Monteiro, E., Silva, J.S.: Security for the internet of things: a survey of existing protocols and open research issues. IEEE Commun. Surv. Tutorials **17**(3), 1294–1312 (2015)
15. Hossain, M.S., Muhammad, G.: Cloud-assisted industrial internet of things IIoT - enabled framework for health monitoring. Comput. Netw. **101**(C), 192–202 (2016)
16. Idc press release (2016). www.idc.com/getdoc.jsp?containerId=prUS41100116
17. Idc press release (2017). www.idc.com/getdoc.jsp?containerId=prUS42209117
18. Kumar, D.: Step on the pedal of cloud services. Michelin Solutions Press release (2013). CruxialCIO.com
19. Lucero, S.: Complimentary whitepaper: IoT platforms - enabling the internet of things (2016). cdn.ihs.com/www/pdf/enabling-IOT.pdf
20. Luong, N.C., Hoang, D.T., Wang, P., Niyato, D., Kim, D.I., Han, Z.: Data collection and wireless communication in internet of things (IoT) using economic analysis and pricing models: a survey. IEEE Commun. Surv. Tutorials **18**(4), 2546–2590 (2016)
21. Madria, S., Kumar, V., Dalvi, R.: Sensor cloud: a cloud of virtual sensors. IEEE Softw. **31**(2), 70–77 (2014)
22. Mekala, A.R., Madria, S., Linderman, M.: Aerial vehicle trajectory design for task aggregation. In: 16th IEEE International Conference on Mobile Data Management, MDM 2015, Pittsburgh, PA, pp. 319–322 (2015)
23. NEST: Demand response programs will reach nearly $10 billion in annual revenue by 2023. Navigant Research (2014)

24. Nieto, A., Lopez, J.: Security and QoS relationships in mobile platforms. In: 4th FTRA International Conference on Computer Science and Its Applications (CSA 2012), vol. 203, pp. 13–21 (2012)
25. Ogrodowczyk, T., Belter, B., LeClerc, M.: IoT ecosystem over programmable SDN infrastructure for smart city applications. In: 2016 5th European Workshop on Software-Defined Networks (EWSDN), pp. 49–51 (2016)
26. Press release, Accenture to help thames water prove the benefits of smart monitoring capabilities (2014). https://newsroom.accenture.com/industries/utilities/accenture-to-help-thames-water-prove-the-benefits-of-smart-monitoring-capabilities.htm
27. Rescorla, E., Modadugu, N.: DTLS: datagram transport layer security. RFC 4347 (2006)
28. Sarakis, L., Zahariadis, T., Leligou, H.C., Dohler, M.: A framework for service provisioning in virtual sensor networks. EURASIP J. Wirel. Commun. Netw. **2012**(1), 135 (2012)
29. Savola, R.M., Abie, H.: Metrics-driven security objective decomposition for an e-health application with adaptive security management. In: Proceedings of the International Workshop on Adaptive Security, ASPI '13, vol. 6, pp. 6:1–6:8 (2013)
30. Sen, A., Madria, S.: Risk assessment in a sensor cloud framework using attack graphs. IEEE Trans. Serv. Comput. **10**(6), 942–955 (2017)
31. Skipper, G.C.: Predictive maintenance and condition based monitoring (2013). ConstructionEquipment.com
32. Soursos, S., Zarko, I.P., Zwickl, P., Gojmerac, I., Bianchi, G., Carrozzo, G.: Towards the cross-domain interoperability of IoT platforms. In: 2016 European Conference on Networks and Communications (EuCNC), pp. 398–402 (2016)
33. Takahashi, D.: Spansion goes battery-less with tiny 'internet of things' chips (2014). Venturebeat.com
34. Taleb, T., Hadjadj-Aoul, Y.: QoS2: a framework for integrating quality of security with quality of service. Wiley J. Secur. Commun. Netw. **5**(12), 1462–1470 (2012)
35. Terdiman, D.: How GE got on track toward the smartest locomotives ever (2014). cnet.com
36. Vaccari, A.: How virtual reality meets the industrial IoT (2016). wiki.aalto.fi/download/attachments/109392027/How-VR-meets-IIoT.pdf
37. Virtual-Radiologic: future of radiology microsite (2011). vRad.com
38. Volvo: volvo construction equipment website. www.volvoce.com
39. Wagstaff, J.: All at sea: global shipping fleet exposed to hacking threat. The World Economic Forum report: Global Risks 2014 (2014)
40. Whitepaper: IoT and digital transformation: a tale of four industries. digitalistmag.wpengine.netdna-cdn.com/files/2016/03/IDC_IoT_white_paper_Mar2016.pdf
41. Whitmore, A., Agarwal, A., Xu, L.: The internet of things–a survey of topics and trends. Inf. Syst. Front. **17**(2), 261–274 (2015)
42. Wilson, J.: Miners tap into rich seam of internet of things. Financial Times (2014)
43. Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of things for smart cities. IEEE Internet Things J. **1**(1), 22–32 (2014)
44. Zhang, Y., Li, W., Zhou, P., Yang, J., Shi, X.: Big sensor data: a survey. In: 9th IEEE International Conference on Internet and Distributed Computing Systems IDCS, Wuhan, pp. 155–166 (2016)