Internet of Things (IoT): Growth, Challenges, and Security

24

24.1 Introduction

The Internet of things (IoT). What is it? Why is it exciting so many in the technology and innovation communities? The concept of the Internet of Things (IoT) was initially proposed by Kevin Ashton in 1998 [1], while he was working at P&G to launch a line of cosmetics for Oil of Olay. Because the father of IoT, as many call him, was bothered that this one shade of lipstick in his cosmetic line always seemed to be sold out in all his London, UK, local stores, he wanted to know where his lipstick was and what was happening to it. No one could tell him. When UK retailers experimenting with loyalty cards with a tiny "radio-enabled" chip, later called RFID, showed these to him, it gave him an idea of tracking his lipstick shade. He took the radio microchip out of the credit card and stuck it on his lipstick shade to see if a wireless network could pick up data on a card and tell him what shelf in the store the lipstick was on. By so doing, he started the forces that created the IoT. In about a decade, the simple idea and experiment have been extended to support pervasive connectivity and the integration of a variety of objects big and small creating an ecosystem of interconnected communication network whose devices or communication nodes are everyday electronic objects like mobile devices, entertainment devices in your home, fridges and temperature control devices, garage door openers, cloth and dish washers, and the list goes on and on. When network connectivity is achieved, it allows all these devices to talk to each other by sending and receiving data. This connectivity of things started long ago with the interconnection of computing devices to form the traditional computer network. Upon that a conceptual model of connectivity of all devices that can communicate and receive data forming a far wider communication network, the "Internet of Things," was born.

The conceptual model and now what is forming in reality has the potential to impact our lives in many unprecedented ways both good and bad, as most technologies are.

J.M. Kizza, *Guide to Computer Network Security*, Computer Communications and Networks, DOI 10.1007/978-3-319-55606-2_24

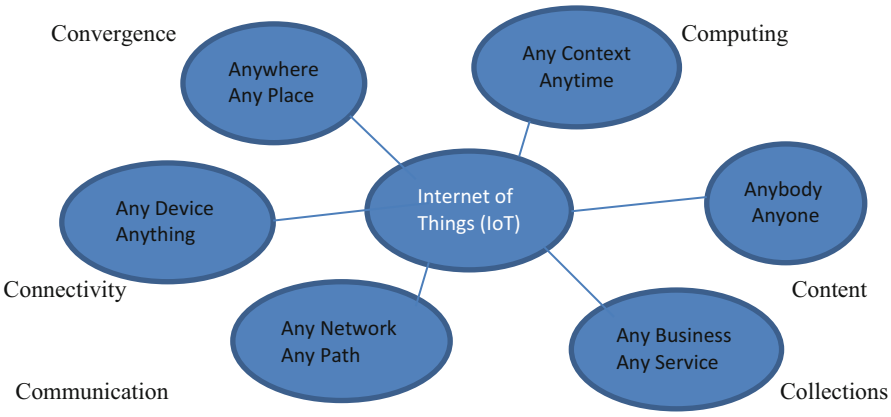

Fig. 24.1 Definition of Internet of Things (IoT) [3]

Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusica, and Marimuthu Palaniswamia [2] have defined the Internet of Things as a smart environment that is made up of an interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This smart environment is achieved by seamless ubiquitous sensing, data analytics, and information representation with cloud computing as the unifying framework. It is this ecosystem described by P. Guillemin and P. Friess in their paper "Internet of things strategic research roadmap," as part of the Cluster of European Research Projects [3] and represented in Fig. 24.1.

Jacob Morgan [4] also sees it an environmental ecosystem that "allows for virtually endless opportunities and connections to take place, many of which we can't even think of or fully understand the impact of today." Because it is going to affect our lives in every possible way, known and unknown in every sphere and dimension, it is in fact, as one scholar puts it, the new Industrial Revolution, again.

It's not hard to see how and why the IoT is such a hot topic today; it certainly opens the door to a lot of opportunities but also to many challenges. Security is a big issue that is oftentimes brought up. With billions of devices being connected together, what can people do to make sure that their information stays secure? Will someone be able to hack into your toaster and thereby get access to your entire network? The IoT also opens up companies all over the world to more security threats. Then we have the issue of privacy and data sharing. This is a hot-button topic even today, so one can only imagine how the conversation and concerns will escalate when we are talking about many billions of devices being connected. Another issue that many companies specifically are going to be faced with is around the massive amounts of data that all of these devices are going to produce. Companies need to figure out a way to store, track, analyze, and make sense of the vast amounts of data that will be generated.

24.2 Overview and Growth of Internet of Things

In their paper, "Internet of Things (IoT): A vision, architectural elements, and future directions," Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusica, and Marimuthu Palaniswamia [2] state that the phrase "Internet of Things" was first coined by Kevin Ashton in 1999 in the context of supply chain management. Since then, it has involved to its present-day meaning. But all along the way, the core essence of making a computer device, which is a node in our IoT, sense information without the aid of human intervention remains the same. In its current meaning, each node of the IoT, may it be a sensor, an actuator, or a communicating device, is interconnected to other nodes in the mess that include the existing Internet, and all are able to intercommunicate, seamlessly passing and getting information to provide services for information transfer, analytics, applications, and communications using existing Internet Protocols. Several technologies have converged to create the Internet of Things technologies. These technologies include those which have led to ubiquitous sensing enabled by wireless sensor network (WSN) technologies and ubiquitous computing; miniature, mobile, and high-powered computing and communication devices; and the existing Internet Protocols to provide services for information transfer, analytics, applications, and communications.

In their paper, "The Internet of Things: A survey," Luigi Atzori, Antonio Iera, and Giacomo Morabito [5] argue that the Internet of Things can be realized in three paradigms—Internet-oriented (middleware), things-oriented (sensors), and semantic-oriented (knowledge). But according to Jayavardhana Gubbia et al., the usefulness of IoT can be unleashed only in an application domain where the three paradigms intersect.

With the expected continued growth of the Internet, there is unanimous expectation of an enormous growth of the Internet of Things in the next 5 years and beyond. Infographics [6] estimates that by 2018, there will be 42.1 billion items connected in the IoT.

John Greenough and Jonathan Camhi both of business intelligence (BI) [7] look IoT in terms of business growth predicting that IoT is the next Industrial Revolution or the Next Internet. On the future of IoT growth, they further predict the following:

- By 2020 there are likely to be 34 billion devices connected to the Internet, from 10 billion in 2015. IoT devices will account for 24 billion, while traditional computing devices (e.g., smartphones, tablets, smartwatches, etc.) will comprise 10 billion.
- Nearly $6 trillion will be spent on IoT solutions over the next 5 years.
- Businesses will be the top adopter of IoT solutions. They see three ways the IoT can improve their bottom line by (1) lowering operating costs, (2) increasing productivity, and (3) expanding to new markets or developing new product offerings.

- Governments are focused on increasing productivity, decreasing costs, and improving their citizens' quality of life. Governments will be the second largest adopters of IoT ecosystems.
- Consumers will lag behind businesses and governments in IoT adoption. Still, they will purchase a massive number of devices and invest a significant amount of money in IoT ecosystems.

24.3 Architecture and Networking of IoT

We defined the IoT in Sect. 24.1 as an interconnection of sensing, actuating, and communication digital devices providing the ability to share information across platforms through a unified framework, developing a common operating ecosystem (COE) for enabling innovative applications. For the IoT ecosystem to function and support intended applications and accommodate the heterogeneity of devices and applications in the ecosystem, the IoT had to adopt the open standards of TCP/IP suite. However, the open standards of TCP/IP suite were initially developed for the wired global Internet several decades ago, as the networking solution. But as we have outlined above in our discussion of IoT, there are fundamental differences between the traditional wired computer networks and the heterogeneous combination of wired and wireless device ecosystem. And as Wentao Shang, Yingdi Yu, and Ralph Droms [8] observe, those differences pose significant challenges in applying TCP/IP technologies to the IoT environment, and addressing these challenges will make a far-reaching impact on the IoT network architecture. To get a good understanding of the IoT architectures and networking, we need to first understand the underlying network topology supported by the heterogeneous technologies, devices, and standards. The networking technology standard currently being used in the IoT falls into three categories: (1) *point-to-point*, for example, an end device to a gateway; (2) *star*, with a gateway connected to several end devices by one hop links; and (3) a *mesh*, with one or more gateways connecting to several end devices one or more hop links away as demonstrated in Fig. 24.2.

Based on these three topologies, we can cascade end devices and gateways to get a real model of the IoT communication network architecture as shown in Fig. 24.3.

All IoT known technologies like Wi-Fi, Bluetooth, WiMax, ZigBee, Z-Wave, RFID, near-field communication (NFC), and others support this communication architecture.

24.3.1 Architecture and Protocol Stack of IoTs

As we will see in the coming Sect. 24.3.2, a typical TCP/IP IPv6 has a maximum transmission unit (MTU) size of 1500 bytes or higher and a near-infinite address space covering up to 2^{128} unique addresses, while IoT constrained low-energy links have very small MTUs averaging around 127 bytes. Even with the two IPv6 design specifications that include (a) IPv6 of 40-byte fixed length header with optional

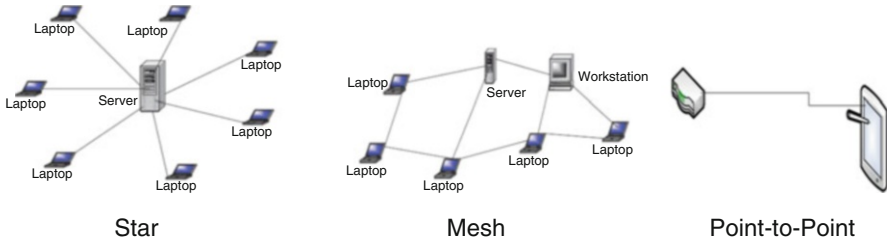

Fig. 24.2 Current IoT topologies

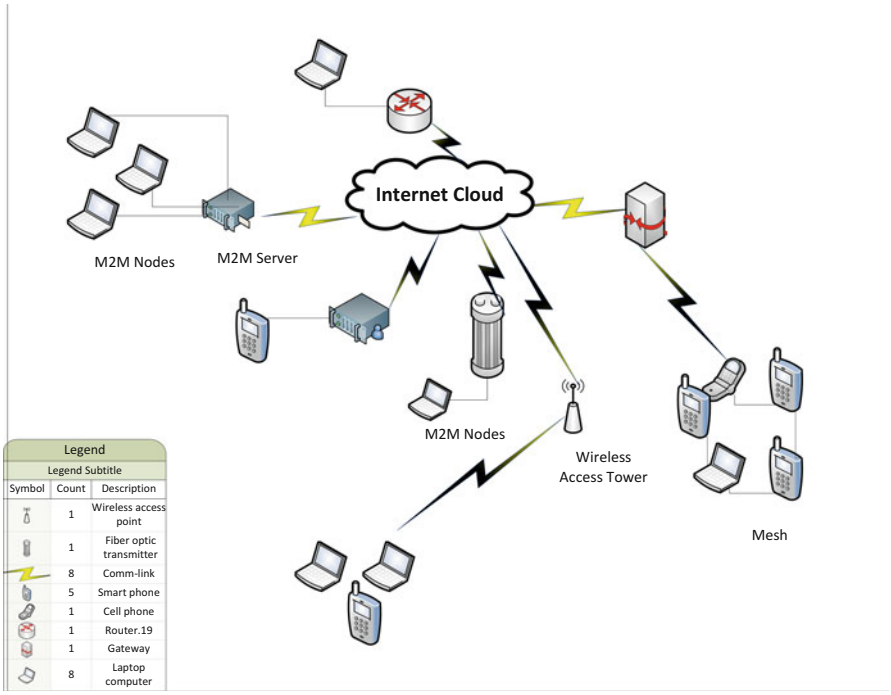

Fig. 24.3 IoT communication network architecture

extension headers, which causes big protocol overheads for small packets, and (b) IPv6 specification requiring all IPv6-capable networks to support a minimum MTU size of 1280 bytes, typical IPv6 packets cannot be carried over the constrained IoT links. So a new 6LoWPAN protocol was defined to enable IPv6 packets to be carried on top of low-powered and lossy personal area networks (LLNs). A draft architecture for a gateway or middleware that provides interoperability between 6LoWPAN and external IPv6 networks has been defined. Other protocols have been defined to support the smooth transmission between IPv6 and low-powered IoT devices. These include [9]:

TCP/IP Protocol suite		IoT Protocol suite	
Application layer	HTTP/FTP/SMTP, etc	Application layer	CoAP
Transport layer	TCP/UDP	Transport layer	UDP
Network layer	IPv4/IPv6, RP, ICMP	Network layer	IPv6/6LoWPAN
Data Link layer	IEEE 802.3 Ethernet/802.11, Wireless LAN	Data Link layer	IEEE 802.15.4e
Physical layer	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI, and others	Physical layer	IEEE 802.15.4

Fig. 24.4 Comparative view of TCP/IP and IOT (IP Smart Objects) protocol suites

Constrained Application Protocol (CoAP)—this was developed by the IETF Constrained RESTful Environments (CoRE) workgroup. The protocol includes several HTTP functionalities although it has modified to work with low processing power and energy consumption constraints of IoT devices. Because CoAP is similar to HTTP, it also uses a universal resource identifier (URI) to identify resources and allow the resource to be affected using similar methods such as GET, PUT, POST, and DELETE.

Figure 24.4 gives a comparative view of TCP/IP and IOT (IP Smart Objects) protocol suites.

Another way of looking at the IoT protocols is via IoT device functionality. IoT devices must communicate with each other. This is referred to as D2D. An example for this is Web services and business applications. Data on data then must be collected and sent to the server infrastructure. This is referred to as D2S. An example for this is in all devices where there is a need for control plane. Finally the server infrastructure has to share device data, possibly providing it back to devices, to analyze programs, or to people. This is S2S. This includes all devices and intelligent systems. The protocols to do these services are [10]:

- MQTT: a protocol for collecting device data and communicating it to servers (D2S)
- XMPP: a protocol best for connecting devices to people, a special case of the D2S pattern, since people are connected to the servers
- DDS: a fast bus for integrating intelligent machines (D2D)
- AMQP: a queuing system designed to connect servers to each other (S2S)

Other IoT protocols include [11]:

- *Infrastructure* (e.g., 6LowPAN, IPv4/IPv6, RPL)
- *Identification* (e.g., EPC, uCode, IPv6, URIs)
- *Comms/transport* (e.g., Wi-Fi, Bluetooth, LPWAN)
- *Discovery* (e.g., Physical Web, mDNS, DNS-SD)
- *Data protocols* (e.g., MQTT, CoAP, AMQP, Websocket, Node)
- *Device management* (e.g., TR-069, OMA-DM)
- *Semantic* (e.g., JSON-LD, Web Thing Model)
- *Multilayer frameworks* (e.g., Alljoyn, IoTivity, Weave, HomeKit)

24.3.2 Challenges of Using TCP/IP Architecture over the IoT

As we just stated above, the IoT ecosystem of heterogeneous devices, wired, wireless, and restricted, using the traditional TCP/IP (though IPv6) meant for wired devices, presents a growing number of challenges in IoT networking that are likely to grow as the IoT ecosystem grows. Some of the issues causing these challenges are easy to see. Others are not. Most of the challenges are brought about by the IoT inherent heterogeneous low-battery-powered wireless devices, the multi-link subnet model, and the mesh network nature of the ecosystem that requires new scalable routing mechanisms. These challenges are thoroughly discussed by Wentao Shang, Yingdi Yu, and Ralph Droms in their paper "Challenges in IoT Networking via TCP/IP Architecture" as follows [8]:

1. *Maximum transmission unit (MTU) size*—While a typical TCP/IP IPv6 MTU has a minimum size of 1500 bytes or higher, the IoT constrained low-energy links have very small MTUs averaging around 127 bytes. Along with size, the IPv6 specification, of two design decisions that utilize either (a) IPv6 of 40-byte fixed length header with optional extension headers, which causes big protocol overheads for small packets, or (b) IPv6 specification requiring all IPv6-capable networks to support a minimum MTU size of 1280 bytes, is unrealistic for the IoT constrained links.
2. *Multi-link subnet model*—The current subnet model of both IPv4 and IPv6 considers two types of Layer-2 networks: multi-access link, where multiple nodes share the same access medium, and point-to-point link, where there are exactly two nodes on the same link. Both of them assume that the nodes in the same subnet can reach each other within one hop. However, the current IoT mesh network contains a collection of Layer-2 links joined together without any Layer-3 device, like routers, in between. This essentially creates a multi-link subnet model that is not anticipated by the original IP addressing architecture.
3. *Multicast efficiency*—A lot of IP-based protocols make heavy use of IP multicast (one-to-many or many-to-many where information is addressed to a group of destination computers simultaneously; see Sec. 5.3.4) to achieve one of the two functionalities: notifying all the members in a group and making a query without knowing exactly whom to ask. However, supporting multicast packet delivery is a big challenge for constrained IoT mesh networks. First, most wireless MAC

protocols disable link-layer ACK for multicast; consequently lost packets are not recovered at link layer. Second, multicast recipients may experience different data transmission rate due to the coexistence of multiple MAC protocols and/or the link-layer rate adaptation; therefore the sender has to transmit at the lowest common link speed among all receivers. Third, IoT nodes may switch to sleeping mode from time to time to conserve energy and thus may miss some multicast packets. Lastly, when nodes are connected through a mesh network, a multicast packet needs to be forwarded over multiple hops along many paths, potentially waking up many sleeping nodes and overloading the already-scarce network resource.

4. *Mesh network routing*—The topologies of typical IoT networks fall into three categories, as seen in Fig. 24.1: star topology, mesh (peer-to-peer), and point-to-point. The routing configuration is straightforward on a star and point-to-point networks where the hub node in a star topology and one of the two nodes in a point-to-point topology can act as the default gateway for the peripheral nodes. However, this limits the signal coverage of a single hub node in these two deployment topologies, making them unsuitable for applications that need wider coverage. The mesh topology, on the other hand, enables larger coverages by having the nodes relay the packets for each other. All mesh nodes cooperate in the distribution of data in the network. Mesh network routing can be supported at either the link layer or the network layer. The link-layer approach, called *mesh-under* in the IETF terminology [8], relies on Layer-2 forwarders to join multiple links into a single "one-IP-hop" subnet. The network-layer approach, called *route-over*, instead relies on IP routers to forward packets across multiple hops. IoT suffers from a *transport layer problem*. The Internet's TCP/IP architecture transport layer provides *congestion control and reliable delivery*, both of which are implemented by TCP, the dominant transport layer protocol on the Internet. TCP efficiently deliver a large bulk of data over a long-lived point-to-point connection without stringent latency requirement. It models the communication as a byte stream between sender and receiver and enforces reliable in-order delivery of every single byte in the stream. However, IoT applications usually face a variety of communication patterns which TCP cannot support efficiently. First, due to the energy constraints, devices may frequently go into sleep mode; thus it is infeasible to maintain a long-lived connection in IoT applications. Second, a lot of IoT communication involves only a small amount of data, making the overhead of establishing a connection unacceptable. Third, some applications may have low-latency requirement, which may not tolerate the delay caused by TCP handshaking.
5. *Resource discovery*—The resource-oriented communication model usually requires a resource discovery mechanism, whereby the applications can request or invoke operations on the resources. The solution for resource discovery in traditional IP networks is DNS-based Service Discovery (DNS-SD) [8]. However, this solution has several limitations in supporting IoT applications. First of all, DNS-SD aims to support service discovery, where the service usually refers to a running program. In contrast, the resources in the context of IoT cover a

broader scope: besides services, it may also refer to IoT devices, sensor data, etc. Therefore, the IoT resource discovery requires a more general approach to identify heterogeneous resources. For example, instead of using DNS records, CoAP adopts a URI-based naming scheme to identify the resources (like in HTTP). Based on that, the IETF core WG has developed CoRE-RD [26], a CoAP-based resource discovery mechanism that relies on less constrained resource directory (RD) servers to store the metainfo about the resources hosted on other devices. Secondly, traditional service discovery often relies on multicast when dedicated services such as DNS and CoRE-RD are not available in the local environment. For example, DNS-SD uses Multicast DNS (mDNS) [8] as the carrier of communications for service discovery and names resolution within the local network. However, link-local multicast has efficiency issues in IoT environments.

6. *Caching*—The TCP/IP communication model requires that both the client (resource requester) and the server (resource holder) are online at the same time. However, in IoT scenarios, the constrained devices may frequently go into sleeping mode for energy saving. Moreover, the dynamic and/or intermittent network environment usually makes it difficult to maintain stable connections between communicating parties. Consequently, the IoT applications often rely on caching and proxying to achieve efficient data dissemination. The selected proxy node can request the resources on behalf of the sleeping nodes and store the response data temporarily until the requesting nodes wake up. The cached contents can also be used to serve similar requests from other nodes who share the same proxy, which saves network bandwidth and reduces response latency. The resource origin server may also appoint some proxy nodes to handle the requests on its behalf (called reverse proxy) so that it can reduce the client traffic and may go offline when it needs to. While it is helpful, the application-level caching implemented by CoAP and HTTP has several limitations in the IoT environment. First, the clients need to explicitly choose a forward- or reverse-proxy node in order to utilize the content caching capability. Second, in dynamic network environments where the connectivity is intermittent, the preselected proxy point may become totally unreachable. When the network topology changes, the clients need to reconfigure or rediscover the proxies or otherwise stop using caches and proxies at all. Third, the caches and proxies break the end-to-end connections assumed by the current security protocols, making it even harder to protect the application data.

24.4 IoT Governance, Privacy, and Security Challenges

As we have pointed out throughout this chapter, an inherent characteristic of the IoT is its heterogeneity resulting from a plethora of things with different data communication capabilities like protocols and hardware, data rates, reliability, and others; computational, storage, and energy capabilities; diversity in the types and formats

of data like audio, video, text, numeric, and streams; and IoT standards including device standards, standards to represent data, IEEE projects on IoT standards, ITU and ISO IoT standards, and others [12]. This diversity in devices, service, and protocols presents challenges unseen and unprecedented in the modern communication.

24.4.1 Governance and Privacy Concerns

As the IoT grows, it presents us with several challenges including global governance, individual privacy, ethics, and of course security. These are the most critical issues in the growth of IoT. As it grows, the IoT is expected to involve multiple stakeholders around the globe. It is important to understand that the meanings of and what defines these issues are differently understood and defined around the globe. So we will deal with the most widely accepted definitions and meanings here. Globally, governance is mostly understood to refer to the rules, processes, and behavior that affect the way in which powers are exercised, particularly as regards openness, participation, accountability, effectiveness, and coherence [13]. These five *principles of good governance* have been already applied to the Internet for specific aspects, and there are already organizations like IETF, ICANN, RIRs, ISOC, IEEE, IGF, and W3C, which are each responsible and dealing with every specific area [13]. But currently this is not the case with the IoT. What this is pointing to is that the governance of the current IoT possesses an array of problems for all those connected to the Internet, the most serious of which are security threats and attacks originating from and targeting both Internet-connected endpoints and data privacy risks posed by those same devices. Consider an IoT with 70 billion wireless-like standalone and embedded sensors and wired devices predicted in the next 3–5 years, all capturing, storing, and communicating data. A number of questions arise. For example, who owns that data? If those devices communicate with your mobile device in the public commons, who owns that data into and on your smart device? Where is the data exchanged with your device going to go? What is it going to be used for? From that point, if the data from or into your smart device is automatically combined with data from a smart passing car, what happens? Do others come to know about you? Do others come to spoof into your devices later? For those wearing medical devices that monitor their vital signs, what about their medical data? This raised a million security and privacy issues with no immediate answers. All these are happening because of lack of a central or at least coordinated distributed authority to harmonize governance of the IoT.

However, everything about the governance of IoT is not bad; there are promising efforts and initiatives in different places like North America and Europe that are developing policies and protocols that will eventually archive these governance goals.

24.4.2 Security Challenges

Security is critical to IoT applications due to their close interaction with the physical world. In Internet communication, based on TCP/IP, IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information. As a most widely used secure protocol in IP, TLS and its datagram variant DTLS are the main security protocols offering end-to-end secure communications between a server and client. TLS, with its two main constituent protocols, the handshake protocol, responsible for key exchange and authentication, and the record protocol, responsible for a secure channel for handling the delivery of data, makes the security of all IP-based communications a channel-based security. The secured-channel solutions, however, do not fit into the IoT environments for several reasons:

1. The first issue with *channel-based security* is the overhead of establishing a secure channel. Both TLS and DTLS require two or more rounds of security handshake to authenticate a channel and negotiate the security parameters, before the first application data is sent out. The second issue is that both ends of a channel have to maintain the states of the channel until it is closed. This may impose a high pressure on memory usage when a device needs to communicate with many peers simultaneously in a densely meshed network. Third, channel-based security does not guarantee the security of request-response once the application data get out of the channel. This is most troublesome when the *middleboxes*, like caches and proxies (see more details on this in Sect. 24.4.6), are deployed to cache the application data. The resource owners need to trust the middleboxes to enforce the access control policies correctly, while the resource requestors need to trust the middleboxes to provide authentic data without tampering. The limitations above highlight the need for a different security model for IoT applications.
2. *Insufficient authentication/authorization*—If recent attacks on the Internet, using smart house monitoring camera, resulting in distributed denial of service (DDS), are any evidence, the IoT with its growing mesh of heterogeneous devices, whose users and devices rely on weak and simple passwords and authorizations, is a growing security quagmire.
3. *Lack of transport encryption*—Most devices fail to encrypt data that are being transferred, even when the devices are using the Internet.
4. *Insecure Web/mobile interface*—Most of the billions of IoT-based devices connect on the Internet using bridging communication protocols and device management schemes that do not do an effective job. See more details in Sect. 24.3.2.

24.4.3 Autonomy

High heterogeneity and complexity and lack of dynamic and scalable management schemes in the IoT due to its plethora of sometimes constrained devices, with

different data communication capabilities, create a challenge in the manual maintenance of a large number of devices, become inefficient, and demand the presence of intelligent and dynamic management schemes. According to Qazi Mamoon Ashraf and Mohamed Hadi Habaebi [14], strong autonomy in IoT can be realized by implementing self-managing systems. Self-management is the property of a system to achieve management and maintenance of its resources intrinsically and internally. It is achieved through levels of decision-making including access management, device management, as well as service management. This thus should lead to all devices in the IoT being aware of their owners' preferences and autonomously make decisions on behalf of their owners and at the same time cooperate with other devices on including securing network communication.

24.4.4 Computational Constraints

One of the characteristics of IoT is its heterogeneity and complexity as it connects to billions of sometimes constrained devices running different communication protocols and management schemes. Low-level devices on the fringes can be of limited power sometimes of less than 10 KBs of RAM, which are sometimes orders of magnitude lower than an ordinary desktop computer with GIGs of RAM. This presents data transfer, computation, and communication challenges. So in cases where high-demand computations cannot be handled by the low-power devices, a delegation of operations may be required.

24.4.5 Discovery

With the rapid growth of devices connected to the IoT, expected to hit 70 billion in the next few years, challenge for search and discovery for available services is increasingly becoming an impediment to the growth of IoT and will diminish future expected benefits of the IOT. Moreover, discovery methods currently being used in the Internet are not flexible to accommodate a growing regime of new services, and they are not capable of searching the heterogeneous devices running different discovery protocols. Therefore, we need new discovery technologies that are more expressive and able to evolve over time.

Discovery in the IoT is the process that enables application to access the IoT data without the need to know the actual source of data, sensor description, or location. According to Arkady Zaslavsky and Prem Prakash Jayaraman, the discovery process can be defined as two successive loops [12]:

- *Foraging loop*—Data sources are identified and assessed, where the relevant data is extracted and formatted into consumable form.
- *Sense-making loop*—The extracted data is analyzed and exploited to provide answers around a specific problem.

The challenge is then to develop a scalable framework (or architecture) along with protocols to provide complete capabilities, which work for all those who will use the IoT.

24.4.6 Trust Relationships

We have already seen and discussed the connectivity and heterogeneity of the IoT. We know that IoT connects to billions of devices with high connectivity complexities and challenges. IoT end devices play a variety of roles and perform many functions for the device owner. Some devices are wired; others are wireless. Some are low powered; others have access to full power. To enable communications with all these devices, there is a need for some degree of intelligence in these devices. The growth of embedded intelligence behavior in the end devices, as an extension of the device owner relationship, will increase and indeed become ubiquitous as the IoT plethora of things with different data communication capabilities grows. As the strong relationships and embedded intelligence between end devices and their owner grow, a citizen (user) relationship is created and introduced into the IoT. The "things" in an IoT are indeed the end devices. There are the new entities (new ontologies). Now these new entities are endowed with identity, connectivity, intelligence, and agency with and through which relationships.

These *human-IoT* relationships create a relationship-trust mesh in the IOT which result into a multitude of questions of a social, ethical, and legal nature. Questions are as follows [15]:

- What threats are caused by delegating fundamental aspects of humanness?
- How can we preserve the human capability to freely act and make choices in the IoT?

A lot more issues are and will continue to be raised as the IoT grows.

Exercises

From self-driving cars to factory robots, engineers are imagining new ways of connecting our world through IoT-enabled machines that integrate production processes.

1. In a short three-page paper, discuss how this is likely to happen.
2. Also using the same scenario above, cars, in say a four-way intersections, will be able to talk to each other and negotiate who goes first without involving the drive. What are the likely dangers of this?
3. With IoT, the toaster in your house will be able to wake you up to tell you that your sliced bread is just about ready. In man-machine interdependence so created, discuss our role, as humans.

4. Jack Williamson in *With Folded Hand* portrays a world ruled by robots, which seem benign but must follow and exist to discharge the Asimovian Prime Directive. The Prime Directive is "to serve and obey, and guard men from harm." In the story, robots replicate themselves and do all the jobs the man wants them to do until he realizes the mistake he make to create the robots in the first place. They just made him useless. Is the IoT likely to produce this utopia for humanity?
5. In this chapter, I call the IoT a security quagmire. Do you agree?

Advanced Exercises

1. What's the biggest risk associated with the IoT on society?
2. What factors would most influence and accelerate the benefits of the IoT?
3. Will IoT, including devices that make it, be secure? Perhaps this is the most difficult question to answer. Do you know why?
4. In any communication regime, privacy issues play a vital role. The IoT, as the future backbone of ubiquitous communication, how will privacy be assured? Or can it?
5. With the ubiquitous communication brought about by IoT, interoperability is critical. Can IoT architecture guarantee interoperability?

References

1. Maney K. Meet Kevin Ashton, father of the internet of things. http://www.newsweek.com/2015/03/06/meet-kevin-ashton-father-internet-things-308763.html
2. Gubbia J, Buyyab R, Marusica S, Palaniswamia M. Internet of Things (IoT): a vision, architectural elements, and future directions. Elsevier. http://www.sciencedirect.com/science/article/pii/S0167739X13000241
3. Guillemin P, Friess P. Internet of things strategic research roadmap. The Cluster of European Research Projects, Tech. Rep., September 2009. http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf
4. Morgan J. A simple explanation of 'the internet of things'. http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#5939c9768284
5. Atzori L, Iera A, Morabito G. The Internet of things: a survey. Computer Networks, Elsevier. http://ac.els-cdn.com/S1389128610001568/1-s2.0-S1389128610001568-main.pdf?_tid=1094eeaa-85ae-11e6-a405-00000aab0f01&acdnat=1475089513_ff39eabceaa7caece0fbe703937e25c1
6. Infographic: The growth of the internet of things. https://www.ncta.com/platform/industry-news/infographic-the-growth-of-the-internet-of-things/
7. Greenough J, Camhi J. Business intelligence. Here are IoT trends that will change the way businesses, governments, and consumers interact with the world, Aug. 29, 2016. http://www.businessinsider.com/top-internet-of-things-trends-2016-1?IR=T
8. Shang W, Yu Y, Droms R. Challenges in IoT networking via TCP/IP architecture. NDN Technical Report NDN-0038, 2016. http://named-data.net/techreports.html
9. Sutaria R, Govindachari R. Understanding the internet of things. http://electronicdesign.com/iot/understanding-internet-things#IoT
10. Schneider S. Understanding the protocols behind the internet of things. http://electronicdesign.com/iot/understanding-protocols-behind-internet-things

11. IoT Standards and Protocols.: http://www.postscapes.com/internet-of-things-protocols/
12. Zaslavsky A, Jayaraman PP (2015) The internet of things: discovery in the internet of things. Ubiquity 2015(October): 1–10
13. IERC. Internet of things IoT governance, privacy and security issues. European research cluster on the internet of things January, 2015. http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf
14. Ashiraf QM, Habaebi MH. Introducing autonomy in internet of things. http://www.wseas.us/e-library/conferences/2015/Malaysia/COMP/COMP-27.pdf
15. Kounelis I, Baldini G, Neisse R, Steri G, Tallacchini M, Pereira ÂG. Building trust in the human – Internet of things relationship. IEEEXplore. IEEE Technology and Society Magazine. Winter, 2014. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6969184