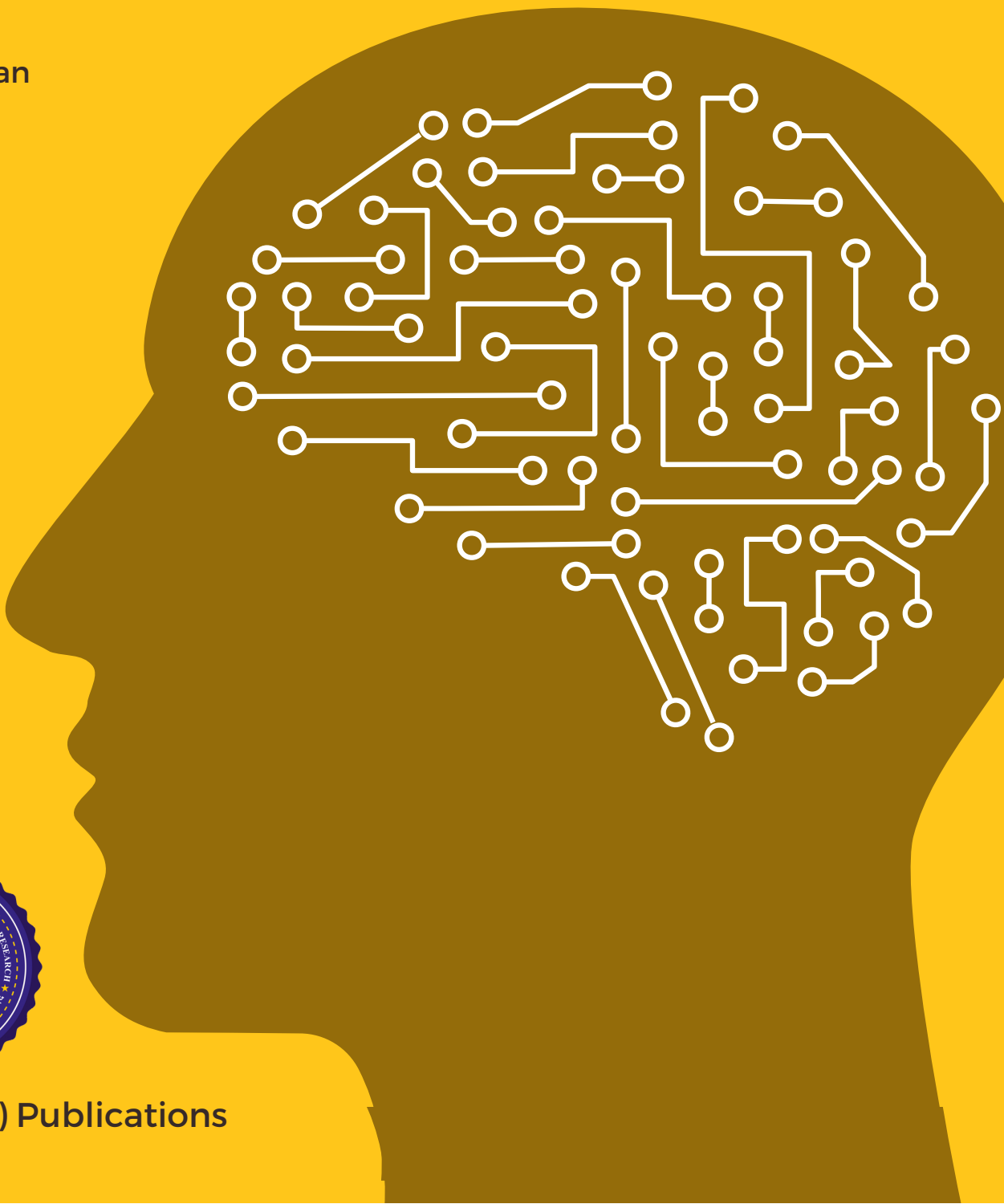
April 2023

IOT BASED SMART SENSING & DETECTION SYSTEMS

EDITED BY
Dr. C. Kalaiarasan



CIIR (R&D) Publications

IoT Based Smart Sensing & Detection Systems

EDITED BY

Dr. C. Kalaiarasan

CIIR (R&D) Publications
Noida, India.

CIIR (R&D) Publications

IoT Based Smart Sensing & Detection Systems

First published April 2023 by CIIR (R&D) Publications, Noida, India.

April 30, 2023

ISBN 978-81-962235-1-9

Edited and Compiled by
Dr.C. Kalaiarasan

Publisher Address
Council for Industrial Innovation and Research
B-17, Sector-6, Noida,
Uttar Pradesh, India.
201301
Email: info@ciir.in
www.ciir.in

Contents

Preface

Massive improvements in telecommunications networks and the birth of the idea of the Internet of Things (IoT) are the results of incredible changes in the everyday use of electronic services and applications. The Internet of Things (IoT) is an emerging communications paradigm in which devices act as objects or "things" that can connect to one another, perceive their surroundings, and exchange data online.

Enhancing the comfort and effectiveness of human life is one of the objectives of smart settings. A technique for creating smart surroundings has recently emerged from the Internet of Things (IoT) paradigm. In any actual smart environment based on the IoT concept, security and privacy are seen as essential concerns. Applications for smart environments are threatened by security because of security flaws in IoT-based systems. Therefore, IoT-specific intrusion detection systems (IDSs) are essential for preventing security attacks against IoT that take use of some of these security flaws. It's possible that conventional IDSs are not an option for IoT environments due to the constrained CPU and storage capabilities of IoT devices and the particular protocols used. In-depth analysis of the most recent IDSs created for the IoT model is presented in this article, with an emphasis on the corresponding techniques, characteristics, and procedures. In-depth information about the IoT architecture, newly discovered security flaws, and their connections to the various layers of the IoT architecture are also provided in this article. This paper shows that, despite earlier research on the design and implementation of IDSs for the IoT paradigm, creating effective, dependable, and durable IDSs for IoT-based smart settings is still an important challenge. At the conclusion of this book, important factors for the future growth of these IDSs are presented.

IoT success depends in part on sensors, but they are not your typical sensors that merely translate physical factors into electrical impulses. To play a technically and financially feasible role in the IoT ecosystem, they had to develop into something more advanced. This book examines the requirements for the IoT's big sensor array and what has to be done to meet those requirements. The book informs how manufacturers have responded with better fabrication, greater integration, and integrated intelligence, which has led to the widely adopted idea of smart sensors. It will become clear that sensor intelligence produces many additional advantages relating to predictive maintenance, more adaptable manufacturing, and increased productivity in addition to facilitating IoT connectivity. Physical variables are converted into electrical signals or changes in electrical characteristics by sensors, which have historically been functionally simple devices. While this capability is a necessary foundation, sensors must also possess the following qualities to serve as IoT components: Low cost allows for its affordable deployment in big quantities; Physically small, to discretely "disappear" in any setting due to the inability of a wired connection, wireless; self-validation and self-identification extremely low power, allowing it to function with energy harvesting or last for years without a battery change; robust, requiring less or no maintenance; able to diagnose and treat oneself; self-calibrating or able to take wireless link-based calibration commands reducing the demand on gateways, PLCs, and cloud resources through data pre-processing.

Dr. C. Kalaiarasan
Editor

CHAPTER - 1

INTRODUCTION TO IoT INDUSTRY PROTECTION SYSTEM CONTROLLER

Dr. Mahalakshmi
Professor & Head, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka.
Email Id: - Presidency University, Bengaluru, Karnataka.

The Internet has spread to practically every corner of the globe today and is having an inconceivable impact on how people live their lives. We are now approaching a period of connectedness that is much more prevalent, where a very vast number of various appliances will be web-connected. One year after the release of the last edition of Cluster book 2012, it is evident that the Internet of Things (IoT) has attracted a wide range of participants and achieved wider exposure. Smart Cities (and regions), Smart Cars & mobility, Smart homes and assisted living, Smart Industries, Public Safety, Energy & protection of the environment, Agriculture, and Tourism as part of a future IoT Ecosystem are some of the possible Internet of Things application areas [1].

The interplay between the digital and physical worlds is all that the term "Internet of Things" refers to. Numerous sensors and actuators are used to communicate between the physical and digital worlds. Another is the Internet of Things, which is a model in which networking and computer functions are incorporated into any type of imaginable device. We make advantage of these features to check the object's status and, if necessary, update it. The term "Internet of Things" describes a new type of environment where nearly all of the appliances and products that we use were linked to a network. We may work with them cooperatively to complete challenging tasks that call for a high level of intellect IoT devices have this intelligence and connectivity.

IoT devices have incorporated sensors, actuators, CPUs, and transceivers for this cognition and connectivity. IoT is an amalgamation of several technologies rather than a single technology that collaborates in tandem. Devices that aid in interacting with the physical world include sensors and actuators. To draw valuable conclusions from the data the sensors have acquired, it must be intelligently stored and processed. Keep in mind that we define the term "sensor" generally; a mobile phone or a microwave might qualify as a sensor if it transmits information about its present state internal state plus surroundings. A device called an actuator alters the environment, as the temperature controller in an air conditioner.

Data processing and archiving might be carried out on a distant server or at the network's edge. If any data preparation is feasible, it is normally carried out at the sensor, or the processed data is then often transferred to a distant server from some other nearby device. The resources that are accessible, which are frequently severely confined owing to limits of size, energy, power, or computational capability, also limit the processing and storage capabilities of an IoT item. Therefore, obtaining the appropriate data with the requisite level of precision is the key research difficulty [2]. The obstacles of data collecting and handling are joined by difficulties in communication. Because they are often deployed, IoT devices communicate mostly wirelessly.

ISBN 978-81-962235-1-9 April 2023

The wireless channels are unstable and frequently exhibit significant rates of distortion. Communication technologies are essential to the study since under this situation, successfully transferring data without requiring too many replay attacks is a significant difficulty. Through actuators, we may directly alter the actual environment, or we can do an action remotely. We could communicate certain information to other intelligent objects, for instance.

The process of bringing about a change in the physical world frequently depends on its current state. Context awareness is what we refer to as. Every decision is made while taking the situation into account because every application behaves differently. Messages from the workplace may not be welcome interruptions when someone is on vacation, for instance. The fundamental architecture of an IoT framework is composed of sensors, actuators, computation servers, and the communication network. But there are a lot of software-related factors to take into account. To link and handle all of these diverse components, we first need middleware. To link a wide range of devices, we need to standardize several things through the Internet of Things.

Health care, fitness, education, entertainment, social interaction, energy conservation, environmental monitoring, home automation, and transportation systems are just a few of the industries where the Internet of Things finds use. IoT devices may connect with other IoT devices, cloud-based apps, and services thanks to networking technology. To start interacting between devices on the internet, established protocols are used. It is safe and dependable to use heterogeneous devices. Standard protocols outline the guidelines and formats that devices must follow to create, maintain, and transport data via networks. A "stack" of technologies is how networks are constructed. Bluetooth LE is at the bottom of the stack of technologies. While others, like IPv6 technologies, are higher up the stack and are in charge of logical device addressing and network traffic routing [3]. Applications that are executing on top of such layers leverage technology at the top of the stack, such as messaging systems.

This article discusses commonly used IoT networking technologies and standards. Additionally, it offers recommendations for selecting one network protocol over another. Next, it talks about important issues and difficulties with networking range, bandwidth, power consumption, sporadic connection, interoperability, and security all about IoT. The Open Systems Interconnection (OSI) model is a stack of seven protocol layers that is an ISO-standard abstract model [4]. They are, in order, application, presentation, session, transportation, physical, data connection, and network. The foundation of the internet is TCP/IP, or the Internet Protocol Suite, which offers an abridged concrete implementation of these levels in the OSI model.

One of the next technological advancements in internet-based computing is the internet of things (IoT) paradigm, which is already making a positive difference in a wide range of application sectors like smart cities, sustainable lifestyle, healthcare, production, and other things. Analyzing data from various IoT data sources, such as sensors, actuators, smart devices, and other items linked to the internet, is referred to as IoT analytics. The gathering and analysis of data flow from IoT devices are now recognized as a critical component of the IoT's disruptive power and as a requirement for achieving the projected market potential of the IoT. Less than 1% of IoT data is now utilized, which is a severe setback to maximizing IoT's economic value.

ISBN 978-81-962235-1-9 April 2023

Bibliography:

[1] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," *Internet of Things (Netherlands)*, vol. 10. 2020. doi: 10.1016/j.iot.2019.100081.

[2] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*. 2019. doi: 10.1109/ACCESS.2019.2924045.

[3] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

[4] F. Hussain *et al.*, "A framework for malicious traffic detection in iot healthcare environment," *Sensors*, vol. 21, no. 9, 2021, doi: 10.3390/s21093025.

ISBN 978-81-962235-1-9 April 2023

CHAPTER - 2

NETWORK ACCESS AND PHYSICAL LAYER IOT NETWORK TECHNOLOGIES

Dr. Mahalakshmi
Professor and Head, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: - mahalakshmi@presidencyuniversity.in

Cellular, Wi-Fi and Ethernet are examples of IoT network technologies to be aware of towards the bottom of the protocol stack, along with more specialized options like LPWAN, Bluetooth Low Energy (BLE), ZigBee, NFC, and RFID. According to Gartner, NB-IoT is becoming the industry standard for LPWAN networks [1].

The following are network technologies with brief descriptions of each:

LPWAN

A group of technologies called (Low Power Wide Area Networks) is made for low-power, long-distance wireless communication. They are perfect for widespread IoT device deployments that need little power, including wireless sensors. LPWAN technologies include Said something, Haystack, and Long-range Physical Layer Protocol NB-IoT and LTE-M (Narrow-Band IoT).

Cellular

Low-power, low-cost IoT communication methods using current cellular networks are addressed by the LPWAN NB-IoT and LTE-M protocols. The newest of these standards, NB-IoT, is focused on long-range communications between significant numbers of devices, mostly indoor ones. NB-IoT and LTE-M were created. However, cellular technologies now in use are widely utilized for long-distance wireless communication, particularly for IoT. In addition to 2G (GSM), which is now being phased out in older devices, and CDMA, which is also being retired or phased out, 3G is also being phased out quickly, with numerous network operators retiring all 3G handsets. Up until the time that 5G is completely deployed and available, 4G will continue to be in use [2].

Bluetooth

The well-known Bluetooth 2.4 GHz wireless communication technology has a low-power variant called BLE. It is made for short-range communication (no more than 100 meters), usually in a star arrangement, with a single main device that controls several auxiliary devices. Both levels 1 (PHY) and 2 (MAC) of the OSI model are supported by Bluetooth. Devices that send brief bursts of small amounts of data are best suited for BLE. When they aren't sending data, devices are made to sleep and conserve power. BLE is frequently used by personal IoT devices, such as monitors for fitness and health.

ZigBee

On the 2.4GHz wireless communication frequency, ZigBee runs. Its range is up to 100 meters longer than BLE's. Additionally, compared to BLE, it offers a little lower maximum data rate (250 kbps as opposed to 270 kbps). The ZigBee mesh network protocol. Not all gadgets can sleep in between bursts, unlike BLE. Their position inside the mesh and whether they must

ISBN 978-81-962235-1-9 April 2023

serve as controllers or routers within the mesh will both have a significant impact. ZigBee was created for use in the home and building automation. The Z-Wave technology, which is likewise based on IEEE 802.15.4, is a near relative of ZigBee. Z-Wave is a home automation system. It was previously a private technology, but a public domain specification was only just made available [3].

NFC

Holding an NFC card or tag next to a reader is one example of using the near-field communications (NFC) protocol, which has a very short range (up to 4 cm). NFC is beneficial for check-in systems and payment methods, in addition to monitoring assets using smart labels.

RFID

The reader has read. While aided passive tags become active when an RFID reader is available, active tags constantly broadcast their ID. Dash7 is an active RFID-based communication protocol that is intended for usage in applications for industrial IoT that enable safe long-distance communication. Similar to NFC, tracking inventory goods in industrial and retail IoT applications is a popular use case for RFID.

While aided passive tags become active when an RFID reader is available, active tags constantly broadcast their ID. Dash7 is an active RFID-based communication protocol that is intended for usage in applications for industrial IoT that enable safe long-distance communication. Similar to NFC, tracking inventory goods in industrial and retail IoT applications is a popular use case for RFID.

Wifi

Internet is a type of wireless networking that adheres to IEEE 802.11a/b/g/n standards. Since 802.11n has the maximum data speed but also uses a lot of power, IoT devices could only use ZigBee protocol or g to save electricity reasons. Although many prototypes and current-generation IoT devices use wireless, it is expected that lower-power alternatives may eventually replace wireless internet as longer-range and less-powerful options become more accessible [4].

Ethernet

Ethernet utilizes the IEEE 802.3 standard for wired communication inside local area networks. Not all Internet of Things (IoT) devices have to be mobile. For instance, sensors embedded inside a structure automation systems can make use of Ethernet-like wired networking technology. An alternative hard-wired method called power line communication (PLC) substitutes pre-existing electrical wiring for dedicated network lines.

Bibliography

[1] U. Pesch and G. Ishmaev, “Fictions and frictions: Promises, transaction costs and the innovation of network technologies,” *Soc. Stud. Sci.*, 2019, doi: 10.1177/0306312719838339.

[2] O. V. Syuntyurenko and R. S. Gilyarevskii, “Trends and Risks of Network Technologies,” *Sci. Tech. Inf. Process.*, 2021, doi: 10.3103/S0147688221020088.

[3] Q. Ouyang, J. Zheng, and S. Wang, “Investigation of the construction of intelligent logistics system from traditional logistics model based on wireless network technology,” *Eurasip J. Wirel. Commun. Netw.*, 2019, doi: 10.1186/s13638-018-1334-8.

[4] Y. Meng, M. A. Naeem, A. O. Almagrabi, R. Ali, and H. S. Kim, "Advancing the state of the fog computing to enable 5g network technologies," *Sensors (Switzerland)*. 2020. doi: 10.3390/s20061754.

ISBN 978-81-962235-1-9 April 2023

CHAPTER - 3

IOT NETWORKING CONSIDERATIONS AND CHALLENGES

Dr. Sukruth
Assistant Professor, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: - sukruthgowda@presidencyuniversity.in

Keep the following limitations in mind when you decide which networking technology to use for your IoT application:

- Range
- Bandwidth
- Power usage
- Intermittent connectivity
- Interoperability
- Security

Range:

The lengths that IoT devices connected to a network generally send data over may be used to characterize networks:

PAN (Personal Area Network)

PAN is short-range, and distances are measured in meters, such as in the case of a wearable fitness tracker that connects to a mobile phone app [1].

LAN (Local Area Network)

LAN refers to short- to medium-range networks, where the distances between nodes can be as much as hundreds of meters. Examples include home automation systems or sensors positioned inside a factory production line that interact through Wi-Fi with a gateway device installed inside the same structure.

MAN (Metropolitan Area Network)

Long-range (city-wide) MAN uses a mesh network architecture to connect smart parking sensors that are located all over a city and can communicate across distances of up to a few kilometers.

Wide Area Networks (WANs)

Long-range networks, or WANs, may communicate over distances that can be measured in kilometers. An example of this would be agricultural sensors deployed throughout a sizable farm or ranch to track localized climatic conditions known as microclimates [2].

Data from IoT devices should be retrieved by your network and transmitted to the correct location. It is necessary to choose a protocol stack that works with the range. For a WAN application, for instance, that has to function over a range of many miles, avoid using BLE. Data transmission across the necessary distance is difficult; think about edge computing. Instead of using data from a faraway data centre or anywhere else, edge computing examines data that is straight from the devices.

ISBN 978-81-962235-1-9 April 2023

Bandwidth:

The quantity of data that may be delivered in a given length of time is known as bandwidth. It restricts the amount of data that may be gathered from IoT and sent upstream. Several factors impact bandwidth, including the amount of data that each device collects and sends the quantity of equipment used whether data is being transmitted continuously or in sporadic bursts, and whether there are any observable peak periods. The networking protocol's packet size should correspond to the amount of data that is frequently sent. Sending packets padded with useless data is inefficient. In contrast, there are costs associated with dividing bigger data amounts among too many little packets [3].

In other words, upload rates might be slower than download rates since data transmission speeds are not always symmetrical. Data transmission must thus be taken into consideration if there is two-way contact between the devices. Cellular and wireless networks are considered if wireless technology is the best option for high-volume applications given its customarily low bandwidth. Examine if sending full raw data is necessary. Reduce the amount of data that is collected by the sample less frequently as one solution. As a result, you'll record fewer variables and could filter the device's data to eliminate irrelevant information. The amount of data communicated is decreased if the data is aggregated before being transmitted. However, the granularity and flexibility of the upstream analysis are impacted by this procedure. Bursting and aggregation are not necessarily appropriate for time-sensitive.

Power usage:

Power is used when a gadget transmits data. More electricity is needed to transmit data over long distances than it does over short distances. A device's power source, such as a battery, solar cell, or capacitor, as well as its whole lifespan, must be taken into account. Lengthy and durable lifecycles will increase dependability and save operational costs. Longer power supply lifecycles can be achieved with the aid of actions. For instance, you may put the gadget in sleep mode while it is inactive to increase battery life. Another recommended practice is to simulate the device's energy consumption under various loads and network circumstances to make sure that its power supply and storage capacity correspond to the power needed to transport the data [4].

Interoperability:

Devices are interoperable; they can operate with other devices, machinery, systems, and technology. Interoperability can be difficult with the IoT since there are so many different types of connected devices. Traditionally, implementing standard protocols has safeguarded the Internet's interoperability. Industry participants have established standards that prevent the use of several unique designs and approaches. Interoperability problems may be avoided with appropriate standards and people who agree with them.

However, standardization procedures sometimes find it difficult to keep up with innovation and development in the IoT. They are created and published following standards that are currently being revised for forthcoming revisions taking into account the technological ecology.

Bibliography

[1] Y.-H. Jeon, “Impact of Big Data: Networking Considerations and Case Study,” *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, 2012.

[2] D. E. Sandberg, N. Callens, and A. B. Wisniewski, “Disorders of sex development (DSD): Networking and standardization considerations,” *Hormone and Metabolic Research*. 2015. doi: 10.1055/s-0035-1548936.

[3] H. E. Schier and W. R. Linsenmeyer, “Nutrition-Related Messages Shared Among the Online Transgender Community: A Netnography of YouTube Vloggers,” *Transgender Heal.*, 2019, doi: 10.1089/trgh.2019.0048.

[4] J. Roschelle, P. Vahey, D. Tatar, J. Kaput, and S. Hegedus, “Five Key Considerations for Networking in a Handheld-Based Mathematics Classroom,” *Int. Gr. Psychol. Math. Educ.*, 2003.

ISBN 978-81-962235-1-9 April 2023

CHAPTER - 4

IOT SECURITY

Mr. Vetrimani
Assistant Professor, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: - vetrimani.elangovan@presidencyuniversity.in

Priority one is security. It is essential to use networking solutions that provide end-to-end security, including open port protection, authentication, and encryption. A security model included in IEEE offers security features such as access control. Thermal techniques on this standard, like ZigBee, implement management, message integrity, message secrecy, and replay protection [1].

To build a secure and reliable IoT network, take into account the following factors:

Authentication

Adopt secure protocols that provide a device, gateway, user, service, and application authentication. Think about utilizing the X.509 standard to authenticate devices.

Encryption

Use Wireless Public Enabling learners for wireless network encryption if you're using a Wi-Fi connection. A Private which was before the Key strategy is another option. To guarantee data security and privacy when communicating across apps, be sure you implement Transport layer security or Datagram Transit Security, a kind of TLS modified for shaky connections made over UDP. TLS protects the integrity of application data by encrypting it.

Port

Only the ports necessary for interaction with the gateway or upstream services or applications are left available to external connections thanks to port protection. All other ports ought to be closed or firewalled off. Devise when using UPnP (Universal Plug and Play) vulnerabilities, ports may be exposed. Consequently, the router should have UPnP turned off. A seven-layer IoT architectural reference model was released by the architectural committee, which was chaired by Cisco, IBM, Rockwell Automation, and others. Although there are many other IoT reference models, the one proposed by the IoT World Forum gives a clear, streamlined viewpoint on the Internet of Things and covers edge computing, data storage, and access. It offers a clear method to understand IoT from a technological standpoint. Security covers the entire model and is divided into distinct functions for each of the seven levels. The IoT Reference Model described in the figure below was released [2]. Each of the IoT Reference Model's seven levels is examined in further detail in the sections that follow.

Layer 1: Physical Devices and Controllers Layer

The hardware objects and controllers layer is the top layer of the IoT Reference Model. The many endpoint devices and sensors that transmit and receive information reside in this layer, which is home to the "things" of the Internet of Things. These "objects'" sizes might range from practically minuscule sensors to enormous manufacturing equipment. Their main job is to produce data and have network access to be queried and/or managed.

ISBN 978-81-962235-1-9

Layer 2: Connectivity Layer

The IoT Reference Model's second layer focuses on connection. The timely and accurate conveyance of data is this IoT layer's most crucial role. Transmitters between Higher layers devices as well as the network are expressly included in between network and Control layer (the edge computing layer) processes. As you may have noticed, the connection layer includes all networking components of the Internet of Things (IoT) and doesn't discriminate between the backhaul, gateway, or last-mile networks the connection layer's functions are described in depth [3].

Layer 3: Edge Computing Layer

Layer 3's function in computing at the edge. In the section "Fog Computing" further in this chapter, edge computing also known as the "fog" layer is covered. Data reduction and turning network data flow into data that is more manageable are the main goals at this layer ready for processing and storage by higher levels. This reference model's fundamental tenet is that information should start as soon as feasible, and as near to the network's edge as is practical. The functions handled by Layer three of the Internet Reference Model are highlighted.

Data review to see whether information can be filtered or aggregated before being passed to a higher tier is another crucial job carried out at Level. Additionally, this enables data to be reformatted or decoded, simplifying further processing by other systems. Thus, Analyzing the data to determine whether established criteria are crossed and whether any action or warnings are required is a vital role. Future Internet technologies like cloud computing and big data analytics are on the increase, making it possible to build and employ advanced IoT analytics applications beyond those for simple sensor processing. To develop and implement cutting-edge applications that analyze IoT streams, IoT technologies are integrating with cloud computing and Big - data analytics technologies. IoT analytics applications may take use of the capacity and performance of cloud computing infrastructures by integrating IoT data streams into such systems. IoT analytics applications are frequently combined with edge computing infrastructures, which deregulate IoT data stream processing at the very edge of the network. Just some IoT data from the edge devices to the cloud across the network. As a result, IoT analytics applications are frequently deployed within the edge and cloud services infrastructures. IoT analytics and advanced analytics are closely related, in addition to their shared relationship with cloud computing infrastructures. Since they contain some of the Big - data Vs, IoT data are indeed Big Data in essence. [4].

Bibliography

[1] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," *Internet of Things (Netherlands)*, 2021, doi: 10.1016/j.iot.2019.100129.

[2] T. M. Popescu, A. M. Popescu, and G. Prostean, "Leaders' perspectives on iot security risk management strategies in surveyed organizations relative to iotsrm2," *Appl. Sci.*, 2021, doi: 10.3390/app11199206.

[3] S. K. Choi, C. H. Yang, and J. Kwak, "System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats," *KSII Trans. Internet Inf. Syst.*, 2018, doi: 10.3837/tiis.2018.02.022.

[4] R. Ahmad and I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review[Formula presented]," *Internet of Things (Netherlands)*. 2021. doi: 10.1016/j.iot.2021.100365.

CHAPTER - 5
M2M COMMUNICATION

Ms. Napalakshmi
Assistant Professor, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: - napalakshmi@presidencyuniversity.in

The term "machine-to-machine communication," or M2M, refers to the exchange of data between two machines without the use of a human interface or other human involvement. This comprises wireless communications, powerline connections (PLC), and serial connections to the Internet of Things in the industry (IoT). By moving to wireless, M2M communication has become considerably simpler, and more applications may now be connected. In general, cellular connectivity for embedded devices is frequently meant when someone mentions M2M communication. In this instance, M2M communication examples include vending machines transmitting inventory data or ATMs receiving authorization to disburse cash [1].

In general, cellular connectivity for embedded devices is frequently meant when someone mentions M2M communication. In this instance, M2M communication examples include vending machines that transmit inventory data or ATMs that receive permitting to distribute money. M2M has a new name: the Internet of Things as corporations have come to understand its potential. IoT and M2M both promise to significantly alter how society functions. Similar to IoT, M2M enables almost any sensor to connect, opening the door to systems checking themselves and autonomously reacting to environmental changes with a significantly decreased requirement for human participation.

M2M and IoT are nearly interchangeable, with IoT (the more recent word) often referring to wireless technology. M2M has traditionally concentrated on "industrial telematics," which is a fancy term for data transmission for some kind of economic gain. But many of the initial M2M applications, such as smart meters, are still relevant today. Since its introduction in the 1990s, cellular has dominated wireless M2M mid-2000s with 2G mobile networks. Due to this, the cellular industry has attempted to position M2M as something that is intrinsically cellular by providing M2M data plans. However, cellular M2M shouldn't be viewed as a cellular-only niche because it is only one segment of the business.

The Internet of Things is made feasible through machine-to-machine connectivity, as was previously mentioned. Forbes reports that M2M technologies are now among the linked device kinds with the quickest market growth rates, partly due to their ability to connect a single network with millions of devices. Any form of the machine from hospital devices to automobiles to structures is included in the variety of linked devices. Any device that contains sensor or control technologies can be linked to a wireless network [2].

Although it appears complicated, the fundamental principle is pretty straightforward. M2M networks essentially require broad or Fiber channel networks with the exception that they are only utilized to support machine, sensor, and control communication these devices transmit the data they gather to other network nodes. These devices transmit the data they gather to other network nodes. This procedure enables a person (or intelligent control unit) to evaluate what is occurring throughout the whole system and issue important guidelines for member devices.

ISBN 978-81-962235-1-9 April 2023

M2M applications

Manufacturing

Every industrial environment, whether it be for the production of food or other goods, depends on technology to guarantee that costs are controlled and operations are carried out effectively. Automating production procedures in such hectic environment processes should be improved even more by the environment.

This can entail fully automated maintenance of equipment and safety processes in the industrial sector. M2M solutions, for instance, enable company owners to receive alerts on their cell phones when a crucial piece of equipment requires maintenance so they can take care of problems as soon as they appear. Intelligent sensor networks that are connected to the web could potentially be able to autonomously order replacement parts [3].

Home Appliances

Through platforms like Nest, IoT already has an impact on the connection of household appliances. M2M is anticipated to advance home-based IoT, nevertheless. To help secure a higher standard of living for consumers, companies like Samsung and LG have already started to gradually introduce smart home products to occupants. For instance, a smart refrigerator might automatically purchase goods from Amazon once its stock is low, and an M2M-capable washing machine may inform the owners of smart devices once it has finished washing or drying. Several more instances of automation may enhance inhabitants' quality of life, such as systems that let family members use mobile devices to remotely regulate HVAC systems. If a homeowner chooses to leave work earlier than planned.

Healthcare Device Management

Healthcare is one of the industries where M2M technology has the most potential. Hospitals may automate procedures with M2M technologies to guarantee the best possible care using tools that respond more quickly than a personal healthcare worker in an emergency. Emergency circumstances enable this. For instance, an M2M-connected life-supporting device might automatically deliver oxygen and extra treatment when a patient's vital signs fall below normal until a medical expert gets on the scene. M2M also makes it possible to monitor patients at home rather than in clinics or hospitals. For instance, sensors that monitor a fragile or old person's regular movements can spot when he or she has fallen and notify a healthcare professional of the incident.

Smart Utility Management

Automation will swiftly replace the old standard in the new era of energy efficiency. M2M steps in to assist energy firms in automatically collecting data on energy use as they search for innovative methods to streamline the metering process that can bill consumers correctly. Meters can detect how so much energy a home or business consumes and instantly notify the energy provider, eliminating the need to send out a worker to read the meters or ask the client for a reading [4]. As utility transition to more variable pricing models, which charge customers more for energy use during peak hours, this becomes even more crucial. Every object or gadget will soon have to be capable to connect to the cloud, according to a few influential analysts.

Bibliography

[1] A. Esfahani *et al.*, “A Lightweight Authentication Mechanism for M2M

Communications in Industrial IoT Environment," *IEEE Internet Things J.*, 2019, doi: 10.1109/JIOT.2017.2737630.

[2] F. Ghavimi and H. H. Chen, "M2M communications in 3GPP LTE/LTE-A networks: Architectures, service requirements, challenges, and applications," *IEEE Commun. Surv. Tutorials*, 2015, doi: 10.1109/COMST.2014.2361626.

[3] J. Huang, C. C. Xing, S. Y. Shin, F. Hou, and C. H. Hsu, "Optimizing M2M Communications and Quality of Services in the IoT for Sustainable Smart Cities," *IEEE Trans. Sustain. Comput.*, 2018, doi: 10.1109/TSUSC.2017.2702589.

[4] Y. Mehmood, C. Görg, M. Muehleisen, and A. Timm-Giel, "Mobile M2M communication architectures, upcoming challenges, applications, and future directions," *Eurasip Journal on Wireless Communications and Networking*. 2015. doi: 10.1186/s13638-015-0479-y.

ISBN 978-81-962235-1-9

CHAPTER - 6

IoT FUNCTION

Dr. Galiveeti Poornima
Assistant Professor, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: - galiveetipoornima@presidencyuniversity.in

The IoT network has to be built to accommodate its particular needs and limitations. An overview of the whole proposed network, from sensors to the applications layer, is given in this section. IoT networks are designed around the idea of "things," or intelligent devices, carrying out tasks and creating new linked services. Because they conduct activities using a mix of specified objectives and contextual knowledge, these objects can be considered "smart." However, in most cases, the "thing" interacts with an external device to submit reports that the smart object collects, to exchange with other artifacts, or to interact with a management portal. These actions can be self-contained, meaning the smart object does not depend on external systems for them [1].

In this situation, processing data gathered from the smart object and directing the smart object's activity may both be done via the management platform. From an architectural perspective, various elements must an n IoT network requires cooperation to function: Layer of "Things" At this layer, the physical devices must be able to supply the necessary information while yet fitting within the confines of the area in which they have been placed. Network layer for communications: When intelligent things are not self-sufficient, they must interact with an outside system. This communication frequently makes use of wireless technologies [2]. Four sublayers make up this layer: Sublayer for access networks the access network makes up the final mile of the IoT network.

Typically, this consists of wireless technologies like access network's linked sensors could also be wired. Gateways and the network sublayer for backhaul: Multiple smart objects are arranged in a shared communication system specified vicinity of a shared entrance. The smart items and the gateway have direct communication. The function of the gateway is to transmit the gathered data via a longer-distance channel referred to as the backhaul to a headend central train station where the data is processed. This object is referred to as a gateway since the information exchange facilitates function. This gateway serves as a router on IP networks by forwarding packets from one IP network to another.

To enable the range of devices to join and media to use, network and transit layer protocols like IP and UDP must be developed for communication to be successful. Sure improvements must be in place for the headend apps to be able to communicate with the sensors through the network management sublayer. Application and analytics layer: At the top layer, an application must process the data gathered to not only operate the smart objects when necessary but also to make wise decisions based on the data gathered and, in turn, give instructions to the "things" or other devices systems to modify their actions or characteristics to adapt to the evaluated environment. The sections that follow look at these components and provide guidance for designing your IoT communication network.

The majority of IoT networks begin with the device that has to be linked or the "thing." From an architectural perspective, the various IoT protocols and architecture are driven by the

ISBN 978-81-962235-1-9 April 2023

various smart object kinds, forms, and requirements. Smart objects may be classified in a variety of ways. One category for architecture may be:

Battery-powered or power-connected:

This categorization depends on whether the device has a built-in energy source or is constantly powered by an outside source. Items powered by batteries can be transported more readily than things powered by lines. However, batteries restrict the amount of energy and lifetime that consumption by the item is permitted, driving up transmission distance and frequency [3].

Mobile or static:

Whether a "thing" should move or always remain in one place determines whether it should be classified as mobile or static. When a sensor is transferred from one thing to another, it is said to be mobile for instance, a viscosity sensor is transferred from batch to batch because it is attached to a moving object (like a position sensor on moving commodities in a warehouse or factory floor), or because it is a stationary object (like a chemical plant). Additionally, the movement's frequency might change, ranging from infrequent to constant. The potential power source is frequently determined by the mobility range (from a few inches to miles distant).

Low or high reporting frequency:

Based on how frequently the item should report monitored metrics, this categorization was created. Once each month, a rust sensor could report readings. Several hundred times per second, a motion sensor may report acceleration. Higher frequencies result in more energy consumption, which might put restrictions on the transmission range and the available power source (and hence the mobility of the device).

Simple or rich data:

Based on the volume of data transferred throughout each reporting cycle, this categorization was developed. While an engine sensor may provide hundreds of data points, a moisture sensor in a field may just provide basic daily index value characteristics, including temperature, pressure, carbon index, gas velocity, and many others. Higher power usage is often a result of richer data. To determine the object data throughput, the preceding categorization is frequently paired with this one. It can be helpful to remember that throughput is a composite statistic. Simple data may be sent by a medium-throughput item at a very high frequency; in this instance, the flow structure appears [4].

Report Range:

Based on the distance from the gateway, this categorization is made. For instance, your phone and fitness band must be no more than a few meters apart for them to interact. It is assumed that your phone you must be able to see the phone screen to review the reported data there. When the phone is far away, you normally do not use it, thus there is no need to send data from the band to the phone. Contrarily, a moisture sensor in a road's asphalt may need to interact with its reader from a distance of several hundred meters to a few kilometers.

Object density per cell:

This categorization is based on the amount of connected smart things in a specific region that has a comparable demand for communication. One sensor may be used at strategic points every

ISBN 978-81-962235-1-9

few miles along an oil pipeline. Contrarily, observatories like the Turing Behemoth telescope at the Whipple Telescope place hundreds or even thousands of mirrors across a restricted space, each equipped with several gyros, gravitation, and vibration sensors.

Bibliography

[1] L. Nkenyereye, J. Hwang, Q. V. Pham, and J. Song, "Virtual IoT Service Slice Functions for Multiaccess Edge Computing Platform," *IEEE Internet Things J.*, 2021, doi: 10.1109/JIOT.2021.3051652.

[2] W. Ren, Y. Sun, H. Luo, and M. S. Obaidat, "A new scheme for iot service function chains orchestration in SDN-IoT network systems," *IEEE Syst. J.*, 2019, doi: 10.1109/JSYST.2019.2921786.

[3] I. Alam *et al.*, "A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV," *ACM Computing Surveys*. 2020. doi: 10.1145/3379444.

[4] X. Fu, F. R. Yu, J. Wang, Q. Qi, and J. Liao, "Dynamic Service Function Chain Embedding for NFV-Enabled IoT: A Deep Reinforcement Learning Approach," *IEEE Trans. Wirel. Commun.*, 2020, doi: 10.1109/TWC.2019.2946797.

ISBN 978-81-962235-1-9 April 2023

CHAPTER - 7

INTRODUCTION TO IOT-BASED OBSTACLE SENSING USING ARDUINO

Dr. Saira Banu Atham
Assistant Professor, Department of Computer Science and Engineering,
Presidency University, Bangalore, Karnataka, India.
Email Id: - sairabanuatham@presidencyuniversity.in

Every precedent and preconceived concept of network design are destroyed with the advent of the Internet of Things (IoT). To date, engineers knowledgeable in routing theory and protocol design have created networks. However, the Internet of Things architecture will rely far more on natural teachings than conventional (and, in my opinion, ossified) networking strategies. This chapter will look at the reasons why the Internet of Things architecture must be fundamentally different from the old Internet, examine the technological and financial underpinnings of this new design, and then start outlining a solution [1].

Long before the idea of interacting with billions of really basic objects like sensors and utilities was even considered, the original Internet's architecture was developed. There are enormous issues brought on by the impending emergence of these far simpler gadgets the number of devices, the unprecedented need for low-cost connection, and the challenge of managing dispersed and heterogeneous equipment for the existing networking paradigm. Even if these difficulties are now apparent, as the pace of this transition quickens, they will become a bigger, more pressing issue. In this book, a new paradigm for the Internet of Things is described, but first, the issue.

The field of technology known as robotics is concerned with the creation, maintenance, use, and deployment of robots. Robots are machines that can perform a complicated series of tasks automatically, particularly ones that can be programmed by computers. Robots that can identify impediments in their path and create their obstacle-free path are said to be capable of obstacle avoidance. The two processes covered by the thesis are creating an obstacle-avoiding robot and providing an introduction to engineering to first-year engineering students. When dealing with concepts like Infrared (IR), IR sensors, electromagnetic spectrum, and embedded computer when building the robot, the thesis will assist them in learning about physics.

When interacting with concepts like Infrared (IR), IR sensors, emission spectra, and embedded computer when building the robot, the thesis will assist them in learning about physics. The Council of Education (BOE-Bot) is the project's operational foundation. A basic understanding of robotics, programming, or electronics is not necessary for the BOE-Bot family of programmable robots. The goal of the project is to create a robot that can navigate around obstacles while still moving following the given code to find a vacant place. This type of barrier is highly helpful in fields where automated monitoring is required, for instance, in locations where human presence may be dangerous [2].

Depending on the situation, these robots can also be created by including other sensors, such as light or line sensors. However, adding a camera will make the robot smarter, which might benefit humans if required. For instance, it might not always be able to travel to all locations, but we can send this robot instead, which will be present and take its route while sending various pieces of information. The project offers guidance to students who are new to the Arduino community and aids in their understanding of embedded systems, IR sensors, microcontrollers, and how to build a robot utilizing these technologies. Students will

ISBN 978-81-962235-1-9 April 2023

understand more about fundamental servo, programming, and mathematical concepts as a result of the thesis.

Students will learn more about fundamental servo, programmed, and mathematical knowledge and abilities necessary to calculate software values as a result of the thesis. The BOE-Bot will be taught how to do simple moves by new pupils. Students will learn to create subroutines to conduct fundamental maneuvers, as well as progressive deceleration and acceleration of the robot to get it out of manipulations. The thesis seeks to assess the lessons that students may take away from designing, building, and programming an autonomous robot in the areas of engineering, systems engineering, and software development. The thesis informs incoming students or beginners about IR, IR sensors, and the PBASIC indicating better performance in addition to providing in-depth knowledge on Arduino and the usage of the Android Platform for Android application design [3]. The offered instructions are quite straightforward to follow and comprehend, making it very simple for new students to lay the groundwork for their robotics education. This undertaking is quite useful to first-year students with a strong passion for robotics, especially Arduino robotics. Students will get knowledge of servos and how to control them.

Arduino

Popular programmable boards like Arduino are used to make projects. It includes a straightforward hardware platform and a cost-free source code editor with a "one-click build or uploads" function. Therefore, it is made such that one may operate it without having to be a skilled coder (Kushner 1987). The open-source electrical prototyping platform provided by Arduino is user-friendly and adaptable in terms of both hardware and software. Arduino can detect its surroundings by gathering data from various sensors. It can manage its surroundings by turning on and off lights, motors, and other actuators. The Arduino development environment is based on processing, and the Arduino programming language is based on a wire [4].

History

The Interaction Design Institute Ivrea (IDII) students that created Arduino published it in 2005 as a simple utility for Windows and Mac OSX. Since that time, Arduino has been able to spark a global DIY movement in the electronics sector. The free software and the hardware of microcontrollers have been created in such a way that they can readily interact with different sensors, registering user inputs and controlling the actions and reactions of extraneous parts like speakers, motors, and LEDs responding to the user inputs. Since Arduino is so easily programmable, even individuals with minimal programming experience may utilize it. Due to this feature, designers and artists frequently choose Arduino for building interactive settings and installations.

Development

It is important to provide a quick overview of the evolution of microcontrollers before addressing the development of Arduino. Following the invention of solid-state computers (such as the IBM 1401), which employed transistors rather than vacuum tubes, the computing industry underwent a major shift in the 1960s. The computer hardware was made more compact by the use of transistors to execute its operations and a magnetic core memory for its storage (instead of vacuum tubes). In addition, the development of integrated circuits by Jack Kelby in 1959 allowed for the further downsizing of the computer component by fusing circuits and transistors onto small silicon chips. The high-level computer coding languages, are written in symbolic languages.

ISBN 978-81-962235-1-9 April 2023

Bibliography

[1] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," *Internet of Things (Netherlands)*. 2020. doi: 10.1016/j.iot.2019.100081.

[2] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*. 2019. doi: 10.1109/ACCESS.2019.2924045.

[3] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

[4] F. Hussain *et al.*, "A framework for malicious traffic detection in iot healthcare environment," *Sensors*, 2021, doi: 10.3390/s21093025.

ISBN 978-81-962235-1-9

CHAPTER - 8

INTERNET OF THING (IoT) EVOLUTION

Dr. C. Kalaiarasan
Professor & Associate Dean, Department of Computer Science and Engineering,
Presidency University, Bangalore, Karnataka, India.
Email Id: -kalaiarasan@presidencyuniversity.in

Considering the growth of microcontrollers, it is clear that more recent iterations of the technology have been created to meet the demands of hobbyists and non-technical users who happen to have little technical expertise. Alternatively said, Microcontrollers are being used for less sophisticated applications in the corporate, scientific, and commercial sectors. Before the creation of Arduino, one of the most popular tools for electrical hobbyists was the PIC microcontroller board, which General Instruments first offered in 1985. The PIC microcontroller board was chosen because of its quick operation and simple programming capabilities, including PBASIC. The fact that it could store software on a flash memory was another factor [1].

Another factor was its ability to store instructions on a flash memory chip, which allowed the board's instructions to be reprogrammed or wiped at whim with an endless number of options. Additionally, it supported output gadgets like LEDs and input sensors as well as motors. Other well-liked hobbyist boards are BASIC Stamp and wire, which are microcontroller boards made for exploring tactile media and creating electrical art. The benefits of quick prototyping and easy programming are shared by the two boards. The Italian Arduino team, which included Barragan Massimo, David Cuatrillo, Marino, Dave Mallis, and Nicholas Zambesi, was founded in 2005.

In its first two years of operation, Arduino saw remarkable success, selling more than 50,000 boards. By 2009, there were more than 13 different versions of Arduino, each with a unique use. As an illustration, Arduino Mini was a miniature designed for small interactive goals, the Bluetooth-capable Arduino BT, and the Arduino Fabric reinforced for wearable technology applications. The Arduino is a well-known prototyping platform today and a great illustration of how software and hardware may work together.

Hardware innovations initially developed for commercial, military, or scientific uses have been repurposed to meet the demands of those working on new media, art, and design initiatives. Arduino shields, Arduino USB, Arduino single-sided serial, Arduino serial, Arduino Mega, Lilly pads Arduino, Arduino Individualized, Arduino BT, Mini USB adapter, and Arduino Mini are only a few of the current and previous Arduino boards. The following silverware times have been produced throughout the development of Arduino: in 2005, a project was launched to create a tool that would control student-built interactive design projects and was less expensive than other prototype systems that were available at the time. The project was started by David Cuatrillo and Massimo Bans, who gave it the name Arduino of Ivrea [2].

Then, in a little plant in Ivrea, Northwestern Italy, they started making boards. They introduced Arduino Mini in September 2006, and then Arduino in October 2008. The Atmel Come in very handy 168 and AT mega 328 served as the foundation for the creation of Dongle. After that, the Atmel Arduino mega 1280-based Arduino Mega was introduced in March 2009. In May 2011, there were more than 300,000 Arduinos in use worldwide. Later, in July 2012, Arduino Leonardo was made available. It is based on the Atmel SAM3X8E, which includes an ARM Cortex-M3 CPU. Based on the Atmel ATMega32u4 processor, the Arduino Micro was first available in November 2012.

ISBN 978-81-962235-1-9 April 2023

The project will make use of an Arduino Uno to compare it to earlier iterations. Based on the 14-bit ATmega328 microprocessor, the Arduino Uno is a microcontroller board pins for digital I/O. Six of these pins can be used as PWM outputs, one as a crystal oscillator operating at 16 MHZ, six as analog inputs, one as a USB port, one as an ICSP header, and one as a power connector and reset button. The board has everything needed to support the microcontroller, including USB ports for connecting to computers and powering it with an AC-to-DC battery or converter. Due to its features, including an ATmega8U2 that is set up as an Arduino Uno stands out from earlier boards [3].

Due to its features, such as an ATmega8U2 that is set up as a USB-to-serial converter, the Arduino Uno stands out from earlier boards. Using an external power supply or the USB connection, Arduino Uno may be powered the choice of power pins on the Arduino board is: VIN, which is the input voltage when utilizing an external power source, as opposed to the 5 volts from a regulated power supply or USB connection. The source is automated. This pin can be used to access voltage while it is being supplied by the power jack or to feed voltage through. The microprocessor and other components found on the board are powered by a controlled 5V power source.

Any other regulated 5V source or USB can provide it. The onboard regulator produces a 3.3V supply, or it can receive one from VIN through the onboard regulator. The 50 mA maximum current drain. The GND surface ATmega328 pins contain 32 KB of memory, including 0.5 KB for the boot loader. It features 2 KB of SRAM and an additional 1 KB of EEPROM that is accessible via the EEPROM library and may be written to or read. The Uno PCB's maximum width and length are 5.3 and 6.8 cm, respectively. Beyond these measurements are the USB connection and power jack. The board may be mounted to a case or suction cup using the four screw holes.

Compared to traditional networking, the IoT design demands a much more organic approach since it represents the very edge of communications. The devices that need to be linked have a large range and breadth, and the connection to the edges of the network on which these devices will be arranged will be "low fidelity," meaning it will be intermittent, low-speed, and lossy (where attenuation and interference might result in lost but largely unimportant data. In contrast to networks like the conventional Internet, much of the communication will be machine-to-machine and take the form of brief bursts of data [4].

The distinctive needs for the frontier of the burgeoning Internet of Things are made clear by examining the features of the conventional internet. Data networks have often been created with greater capacity than is customary, or over-provisioned need to carry the amount of information. Even the traditional Internet, which is ostensibly "best effort," is vastly over-provisioned in many ways. The Internet wouldn't function if it weren't for the fact that sender-to-receiver connections are at the core of protocols like TCP/IP. Even the tremendous expansion of the Internet over the last two decades has not outgrown the capabilities of gadgets like routers, switches, and PCs, in part because Moore's Law offered a "safety valve" in the shape of ever-rising processing speeds and memory capacities.

Bibliography

[1] M. A. Rahim, M. A. Rahman, M. M. Rahman, A. T. Asyhari, M. Z. A. Bhuiyan, and D. Ramasamy, “Evolution of IoT-enabled connectivity and applications in automotive industry: A review,” *Vehicular Communications*. 2021. doi: 10.1016/j.vehcom.2020. 100285.

[2] A. Zaidi, Y. Hussain, M. Hogan, and C. Kuhlins, “Cellular IoT Evolution for Industry Digitalization,” *Cell. IoT Evol. Ind. Digit.*, 2019.

[3] M. Beale, H. Uchiyama, and J. C. Clifton, "IoT Evolution: What's Next?," *IEEE Wireless Communications*. 2021. doi: 10.1109/MWC.2021.9615126.

[4] M. Z. Gündüz and R. Daş, "Internet of things (IoT): Evolution, components and applications fields," *Pamukkale Univ. J. Eng. Sci.*, 2018, doi: 10.5505/pajes.2017.89106.

ISBN 978-81-962235-1-9 April 2023

CHAPTER - 9

MICROCONTROLLER

Dr. Hasan Hussain
Associate Professor, Department of Computer Science and Engineering,
Presidency University, Bangalore, Karnataka, India.
Email Id: -hasan.hussain@presidencyuniversity.in

A controller consists of a highly integrated chip with all the components. A CPU, RAM, some kind of ROM, I/O ports, and timers are typically included. A microcontroller, in contrast to a general-purpose computer, which likewise has all of these parts, is made to control a specific system. Consequently, the components can be streamlined and reduced, which lowers the cost of production [1]. Embedded microcontrollers are another name for microcontrollers. This only indicates that they are a component of an embedded system, a smaller unit or system. Automotive engine control systems, implanted medical devices, remote controls, office equipment, appliances, power tools, toys, and other embedded systems are just a few examples of the automatically controlled goods and gadgets that employ microcontrollers.

The microprocessor-based system is not intended to be programmed by the end user in the same way that a PC is defined as an embedded system; rather, it is created for controlling a function or set of functions. An integrated system is created to carry out a certain function. Microcontrollers or digital signal processors are the two types of processing cores found in embedded systems. Generally referred to as "chips," microcontrollers can be placed with other microcontrollers in a hybrid system of application-specific integrated circuits (ASIC). Generally speaking, input is always provided by a detector, or more precisely, a sensor, and output is sent to the activator, which can start or stop the functioning of the machine or operating system.

Generally speaking, input is always provided by a detector, or more precisely, a sensor, and output is sent to the activator, which can start or stop the functioning of the machine or operating system. A mix of both hardware and software makes up an embedded system. Hardware for embedded systems is a special investigation in the application domain, making each one unique [2]. Processors, microcontrollers, IR sensors, and other components make up hardware. In contrast, the software acts as the system's "brain" and comprises the programming languages that enable hardware to function. As a result, programming embedded systems may be a very diverse experience.

Robotics

The field of technology known as robotics is concerned with the creation, maintenance, use, and application of robots. Robots are machines that can perform a complicated series of tasks automatically, particularly ones that can be programmed by computers. Robotics must be able to carry out certain duties under given restrictions, whether or not these restrictions are automated or managed by a person. Robots are described as electromechanical devices that can do human tasks automatically or under computer direction. It is a machine that can operate either automatically or with the aid of some regulating machinery. The definition of a robot is "a machine capable of automatically performing a complicated set of tasks, especially one that can be programmed by a computer [3].

Our robot's job is a rather easy one. The robot must be built so that it will advance until it encounters an obstruction. It will turn left or right in response to an impediment, depending on the amount of open space in front of it. Upon identifying any obstructions depending on the

ISBN 978-81-962235-1-9 April 2023

number of IR rays registered by the IR sensors (left and right), it travels in one of two directions: left or right. Although the mission is straightforward, this robot is self-sufficient.

A procedure often consists of user tasks that demand human involvement. Consider utilizing a software robot, or both, to automate a user task if it involves repeated tasks, such as extracting and transferring data across systems. Instead of using a user task to act, utilize a robot task. A robot task is work carried out by a robot that is integrated into a robotic process automation tool, with Automation Anywhere. The data that is accessible to each robot task implicitly defines the interface that is particular to that activity [4]. User interface (UI) views are used to create the user interface (UI) when a robot job is manually replayed. Robot tasks are therefore only supported in cases where the process application is dependent on the UI toolkit. The task UI will not be built and a runtime error will be shown if the UI toolkit is not in the dependent list and a robot job is manually initiated.

Procedure

- Create a process app in Workflow Center, then launch it in Process Designer.
- Make a procedure. Automatically created and plugged into the workflow is an inline user task.
- Choose one of the following choices to include a robot task in the process:
- Expand Activity, choose Robot Task, then add the robot task to the process and wire it up if you wish to add a robot task as a new activity.
- Click the task on the diagram, then go to Implementation and choose the Robot Work activity type. This will turn any existing task into a robot task.
- Create the necessary input, output, and private variables in the process editor by selecting Variables.
- The interface and data map for the robot job will be made using these variables at the same time.
- Select the robot task in the process diagram, then go to the Data Mapping properties.

By completing the following sub-steps, you may define the interface and add input and output variables to the data mapping:

- To add the input variables, click the Add a new input (+) symbol next to the Input Mapping section. This displays a list of the declared variables.
- Go to the list and pick a variable. It is included in the section titled "Input Mapping."
- Click the Add a new input icon (+) once more if you want to include more variables in the input mapping. (By selecting the X button next to the variable name, you may remove any input variable from the mapping.)
- To add the output variables, click the Add a new output icon (+) next to the Output Mapping section. This displays a list of the variables you can change.

Bibliography

[1] V. Naga and R. Gunturi, “Micro Controller Based Automatic Plant Irrigation System,” *Int. J. Adv. Res. Technol.*, 2013.

[2] D. Adanta, Warjito, D. Febriansyah, and Budiarso, “Simple micro controller measurement devices for pico hydro turbines,” *Int. Rev. Mech. Eng.*, 2019, doi: 10.15866/ireme.v13i8. 17453.

[3] D. D. C. Lu and Q. N. Nguyen, “A photovoltaic panel emulator using a buck-boost DC/DC converter and a low cost micro-controller,” *Sol. Energy*, 2012, doi:

10.1016/j.solener.2012. 02.008.

[4] A. Syed, Z. T. H. Agasbal, T. Melligeri, and B. Gudur, "Flex Sensor Based Robotic Arm Controller Using Micro Controller," *J. Softw. Eng. Appl.*, 2012, doi: 10.4236/jsea.2012. 55042.

ISBN 978-81-962235-1-9 April 2023

CHAPTER - 10

IR SENSORS

Dr. Saira Banu Atham
Professor & HOD, Department of Computer Science and Engineering,
Presidency University, Bangalore, Karnataka, India.
Email Id: - sairabanuatham@presidencyuniversity.in

An electrical gadget known as an infrared sensor uses infrared radiation to sense information about its environment. The heat of an item may be measured via infrared sensors electromagnetic radiation known as infrared light has longer wavelengths than visible light. From the visible spectrum's nominal red edge at 700 nm to 0.1 mm, there is light. These wavelengths are equivalent to a frequency range of around 430 THz to 300 GHz. In a motion detector, an emitter sends out IR rays that bounce off of objects in their path and eventually reach the sensor itself, which is located in the middle of the device. This component could have many separate sensors, each built of piezoelectric ceramic materials, whether natural or synthetic [1].

This little circuit board has these pyroelectric components incorporated into it. They are connected in such a way that the motion detector will sound an alert when the sensor detects an increase in heat in a tiny area of its field of vision. It is rather typical for an infrared sensor to be added to motion detectors, such as those used in the home or business security systems. On the sensor face of the majority of motion detectors, a specific kind of lens known as a Fresnel lens is installed. A motion detector equipped with a series of these lenses may concentrate light coming from various angles, giving the sensor a view of the whole space. Some motion detectors are equipped with tiny parabolic mirrors in place of Fresnel lenses.

Some motion detectors include tiny parabolic reflectors used in place of Fresnel lenses, which accomplish the same thing. An infrared sensor may be compared to a camera that takes a quick snapshot of an area's it then emits infrared radiation. How electricity travels from the pyroelectric materials through the remainder of the circuit will vary if there is a dramatic change in one region of the field of vision, particularly if it moves. This will set off an alert on the motion detector. The gadget won't be activated even if the temperature of the entire area of vision changes. This prevents sudden light flashes and normal temperature variations from activating the sensor and setting off false alerts. The usage of infrared motion detectors in home security systems.

These motion detectors often won't detect movement from anything weighing less than 40 pounds (18 kg). Household pets will be able to move about the house without their owners after this adjustment is made owners have to be concerned about a false alarm. Sensors with an 80-pound (36 kg) allowance are also offered for houses with large dogs. Two IR sensor components will be installed on the left and right sides of the robot used in this project [2].

Infrared light is a spectrum of light that is a thousand times broader than visible light. Physically, infrared light is defined as having a wavelength between 0.7 and 0.1 mm. Since light with a wavelength greater than 7 10-5 m cannot be seen by human eyes, IT. Figure 1. The infrared bands in the electromagnetic spectrum. The human eye is unable to see light. Beyond everything else, infrared radiation is identical to visible light since it shares the same

ISBN 978-81-962235-1-9 April 2023

characteristics, including the ability to be focused and reflected like regular visible light, assisting the project's IR receiver in detecting it.

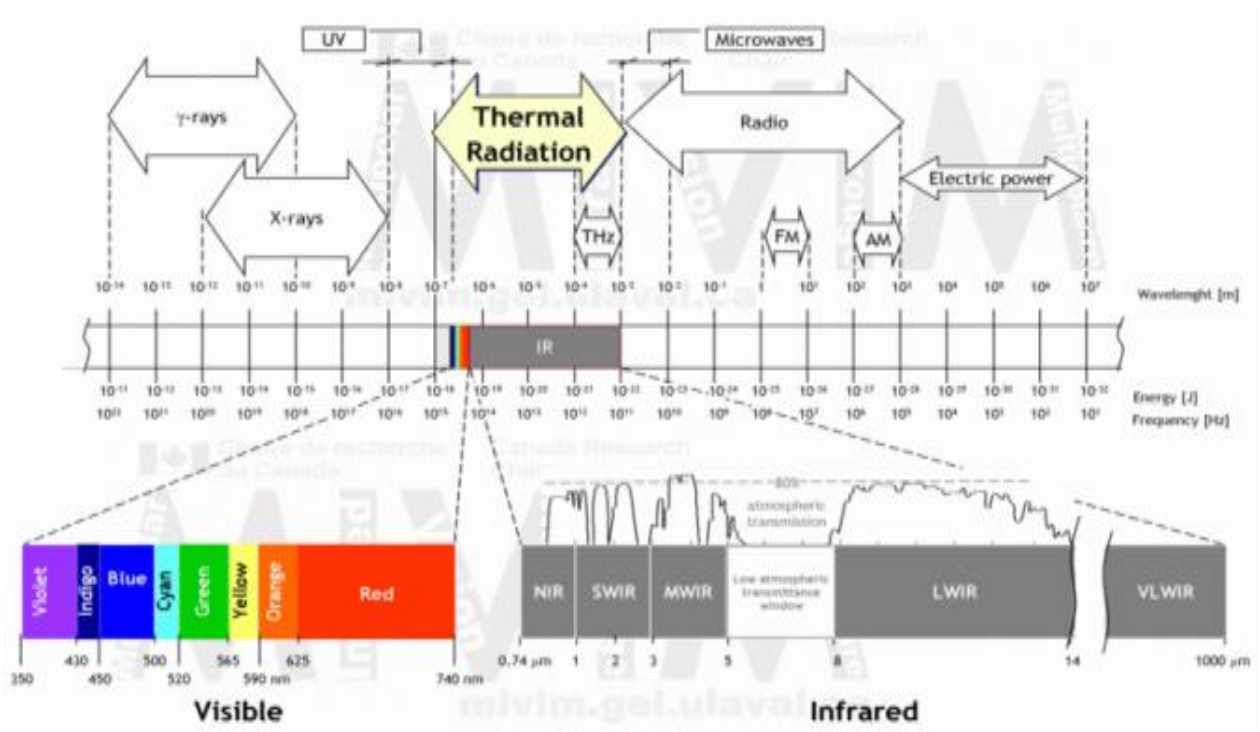


Figure 1: The infrared bands in the electromagnetic spectrum.

Electromagnetic radiation (EMR) known as infrared (IR), sometimes referred to as infrared light, has wavelengths that are longer than those of visible light. As a result, it is not apparent to the human eye. The wavelength range of infrared radiation is often thought to range from about 1 millimeter (300 GHz) to the notional red edge of the visible spectrum, which is around 700 nanometers (430 THz). Needs verification sometimes the terahertz radiation spectrum includes longer IR wavelengths (30 m to 100 m). Infrared wavelengths account for almost all of the black-body radiation emitted by things close to room temperature [3]. IR is a kind of electromagnetic radiation that has qualities similar to both a wave and a particle, the photon, and propagates energy and momentum as well as exerts radiation pressure. Long known that flames produce intangible heat, pioneering scientist Occurs Available in two types demonstrated in 1681 that glass, although transparent to sunlight, blocked radiant heat. In 1800, astronomer Sir William Herschel used the action of infrared radiation on a thermometer to determine that it is a sort of invisible radiation in the spectrum with lower energy than red light. Herschel's research finally revealed that a little more than half of the Sun's energy hits the Earth as infrared. The climate of the Earth is significantly influenced by the ratio of infrared radiation that is absorbed and released [4]. When shifting rotational-vibrational motions, molecules produce or absorb infrared radiation. Through a modification of the dipole, it stimulates the vibrational modes of a molecule.

Bibliography

[1] H. K. Saxena, T. Malik, and A. Bhardwaj, “Automated traffic light system with roadblocks using IR sensors and Arduino,” *Int. J. Eng. Adv. Technol.*, 2019, doi: 10.35940/ijeat.A9660.109119.

[2] T. M. Prasath, S. Geetha, R. K. Kanna, and R. Vasuki, "IR sensor based drowsiness detecting during driving system," *Indian J. Public Heal. Res. Dev.*, 2019, doi: 10.5958/0976-5506.2019.04001.4.

[3] D. Vijayakumar, G. Ramesh, C. Jayabalan, S. Palani, and M. Selvam, "Micro controller based smart helmet by IR motion sensors," *Int. J. Eng. Adv. Technol.*, 2019, doi: 10.35940/ijeat.F7889.088619.

[4] I. Inayah, "Analisis Akurasi Sistem Sensor IR MLX90614 dan Sensor Ultrasonik berbasis Arduino terhadap Termometer Standar," *J. Fis. Unand*, 2021, doi: 10.25077/jfu.10.4.428-434.2021.

ISBN 978-81-962235-1-9 April 2023

CHAPTER - 11

ECONOMICS AND TECHNOLOGY OF THE IOT

Dr. Komalavalli
Professor, Department of Computer Science and Engineering,
Presidency University, Bangalore, Karnataka, India.
Email Id: - komalavalli@presidencyuniversity.in

One of the great promises of introducing IPv6 to the old Internet was that it would offer all the address space required to link every device ever required for all of the time, such as the Internet of Things, regardless of how big it got inside that constrained. Therefore, the promise is fulfilled. The current potential number of hosts communicating devices on an IPv6 Internet is 3.410*38* due to several peculiarities in the manner that just a portion of the IPv6 address space has been published. This is a sizable sum that is unlikely to be surpassed by the expansive Internet of Things. Because of this, a lot of experts and producers especially those with a vested interest have smugly asserted that IPv6 is already ready for the Internet of Things [1]. There are more IP addresses accessible than sand grains, therefore all that has to be done is for the world to carry on as usual. This "head in the sand" strategy, however, misses the important economic component that will drive the cost at the endpoints and will determine how the Internet of Things is deployed just as it has for almost every previous networking technology. Hardware and software, supervision and administration, and security are the three main areas where these expenditures add up and make a new approach to the Internet of Things necessary.

Functionality Costs Money:

Today, the great majority of these low-end, basic devices have no CPUs, memory, or storage, and are not even remotely data-connected. This is a crucial point: the Internet of Things will connect previously unconnected gadgets in the future. These devices are often made to be produced and sold at the lowest cost with the biggest profit margin. Particularly for those offered in underdeveloped nations, they must be very affordable. But these are some of the sectors where the Internet of Things will expand the fastest. The development of a common, affordable solution would enable billions of devices that would otherwise stay off the grid, never be created, or joined to the IOT to fulfill its great potential [2].

Inexpensive Devices:

Knowing these financial realities makes it evident that adding more hardware and software to everyday objects like toasters, lightbulbs, and moisture sensors is not essential for their fundamental tasks. The hardware (e.g., appliances) required to run established protocols like IPv6 is a deal-breaker. Even in big numbers, it has been projected that adding IPv6 to devices might cost an additional $50. Note that extra Wi-Fi or Ethernet components, as well as greater power and heat dissipation, are required in addition to the CPUs and memory devices. Fortunately for the growth of the Internet of Things, these basic gadgets don't need anything close to the complexity provided by IPv6.

Fortunately for the growth of the Internet of Things, these basic gadgets don't need anything close to the complexity provided by IPv6. Instead, straightforward broadcasting, receiving, and modulation methods will be enough, even incorporating options that don't use radio waves, such as infrared and government-in-power networking. Costs of adding simple IOT networking to sensors and appliances will shortly reach $1 or less, assuming integration into silicon packages. The important thing to remember is that this hardly qualifies as "networking" in the conventional sense: it is only broadcasting a state or receiving a straightforward command, with no error checking, routing, or other standard networking features. IOT devices are

ISBN 978-81-962235-1-9 April 2023

typically "dumb," yet they are incredibly effective at a certain purpose. It is simple to see at the most fundamental level.

IOT devices are typically "dumb," yet they are incredibly effective at a certain purpose. At the most fundamental level, it is simple to understand that this cost argument alone is evidence that the expenditures and the effort in developing a new solution for IOT devices are unquestionably worth it necessary. Not doing so would have the effect of substantially preventing the development of many of these new ideas and technology. Others would cost too much to implement, which would reduce their utility. How much at what expense to wealth, progress, and development? Additionally, as previously mentioned, 1,000 bytes of data are added to even the smallest payloads by conventional, one-size-fits-all networking protocols like IPv6. These lost bytes go unnoticed in today's environment of overprovisioned resources.

As explained throughout this book, the new architecture that is emerging for the Internet of Things must adopt a completely different strategy. Only locally relevant and probably non-unique names are used for end devices. There is no issue with this because networking intelligence at far fewer and hence more controllable locations across the design [3]. Furthermore, it is unnecessary to monitor or regulate each manufacturer of end devices. There is little "damage" that the Internet of Things (IOT) can do to the network as a whole because the end devices only offer a few restricted networking capabilities, and this is readily regulated by a far smaller number of "smarter" devices. In contrast to IPv6, which mandates that every device has the capability.

Compared to IPv6, which mandates that every device has the capabilities and management to operate as a "peer" on the network, this strategy is completely different. If the Internet of Things is composed of peers that must all be controlled, it will simply not scale. Like a giant ant, the Internet of Things will grow via expertise, personal liberty, and local impact. Costs are drastically decreased in this approach. A cliché that is ultimately true. There are few security vulnerabilities and back doors since connections with the end devices in this new Internet of Things architecture are so simple and focused. Compare this once more to "peer-to-peer" the IPv6 Internet, where numerous IP devices are susceptible to attack [4]. Tries to crack coming from anywhere in the globe. Internet security breaches are estimated to have cost $115 billion worldwide (Symantec, 2012). Today's Internet has 2.4 billion peer-to-peer nodes, which roughly translates to $50 per node (user) each year annual losses The cost of IPv6 in the IOT is unacceptably large when multiplied by the estimated hundreds of billions of connected devices. The evolving architecture of the Internet of Things significantly lowers the risks and costs involved with networking the enormous population of appliances, actuators, and sensors by concentrating on restricted networking capabilities for the end devices.

Bibliography

[1] Q. Zhu, S. W. Loke, R. Trujillo-Rasua, F. Jiang, and Y. Xiang, “Applications of distributed ledger technologies to the internet of things: A survey,” *ACM Comput. Surv.*, 2019, doi: 10.1145/3359982.

[2] L. Tarricone and J. Grosinger, “Augmented RFID technologies for the internet of things and beyond,” *Sensors (Switzerland)*. 2020. doi: 10.3390/s20040987.

[3] C. Zhang and Z. Liu, “Application of big data technology in agricultural Internet of Things,” *Int. J. Distrib. Sens. Networks*, 2019, doi: 10.1177/1550147719881610.

[4] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, “Blockchain technologies for the internet of things: Research issues and challenges,” *IEEE Internet Things J.*, 2019, doi: 10.1109/JIOT.2018.2882794.

CHAPTER - 12

NETWORKING FUNCTIONALITY

Dr. Pallavi
Associate Professor, Department of Computer Science and Engineering,
Presidency University, Bangalore, Karnataka, India.
Email Id: - pallavi.r@presidencyuniversity.in

The propagator nodes depicted in the mesh contain the protocol intelligence, which is located elsewhere in the IoT network. In terms of technology, they resemble routers more than other commonly used networking devices, yet they perform differently way. Propagator nodes keep an eye out for data coming from any source. Propagator nodes choose whether to broadcast these transmissions to other propagator nodes or the higher-level integrator devices covered in the following section based on a straightforward set of criteria defining the "arrow" of transmission toward devices or away from devices. These propagator nodes must be very capable of discovery and self-organization to scale to the enormous size of the Internet of Things [1].

These propagator nodes must be very capable of discovery and self-organization to scale to the enormous size of the Internet of Things. They will identify more propagator nodes nearby, create basic routing tables of adjacencies and identify probable routes to the suitable integrators. Wireless mesh networking technology has been used to address similar problems in the past among many others, and although the topology algorithms are complicated, just a modest amount of data transmission is required. Pruning and refining broadcasts are one of the key abilities of propagator nodes. The "arrow" of data transmission from and to end devices may be mixed with other traffic and routed in that general direction. Propagator nodes may be the functional components that are most similar to the notion of peer-to-peer networking as it is now understood, but they offer networking on behalf of end devices and integrator functions at scales "below" and "above" themselves. Any of the widely accepted networking protocols may be employed, and propagator nodes will serve as crucial network translators (power line or Bluetooth to ZigBee or Wi-Fi, for example). The propagator nodes' general purpose has been described above, but many will also have an extra crucial capability: the ability to be controlled and "tuned" by integrator functions throughout the network. This will manifest as a fully functional propagator node with a software publishing agent.

This publishing agent will join the information "neighborhood" built by one or more integrator functions, the integrator function will apply higher-level management to specific propagator nodes, regulating features like data transmission frequency, network architecture, and other networking capabilities, in a similar way to a software-defined network [2]. The data streams from tens of thousands to millions of devices are evaluated and used in integrator functions. Integrator functions also send their transmissions to devices to get information or set values; naturally, the arrow of this data's transfer is present is directed towards the gadgets. The inputs that integrator functions can use range from big data to social networking trends, from Facebook "likes" to weather reports. The integrator functions in this new architecture serve as the IoT's human interface. As a result, they will be designed to compress the unfathomably vast volumes of data gathered over time to a straightforward collection of alerts, exceptions, and other reports that people can consume. Integrated scheduling and decision-making processes inside the integrator functions enable most of the IoT to run transparently and without human

ISBN 978-81-962235-1-9 April 2023

involvement. These processes use basic notions like "cluster" and "avoid". For an ordinary household using a smartphone, computer, or home entertainment system, one integrator function could be required. The integrator role might also be expanded to a large, international corporation, measuring and managing energy use throughout a corporation.

The filter gateway is an extra device at this third level of the design. With a link to the Internet and a connection to the integrator function, filter gateways are conceptually two-armed routers. General-purpose processors are used for integrator tasks. Similar to PCs, they are vulnerable to denial-of-service assaults and extremely massive data loads. Therefore, the filter gateway is a device that makes sure only relevant data is sent to the integrator function. To limit the traffic supplied to the integrator to the "region of interest," filter gateways may utilize a straightforward set of rules determined by the associated integrator function. Again, these communities may be based on location, purpose, time, or a variety of other characteristics [3].

The old Internet remains the only workable solution for scaling to billions of devices globally, despite the obvious and compelling reasons for a new architecture and protocol at the very edge of the Internet of Things backbone for moving Internet of Things traffic. To fully utilize the established global Internet infrastructure, the lightweight IOT protocols must eventually be packaged or converted to regular Internet protocols. The Internet of Things architecture offers an order to clearly define and convert capability at extensively featured propagator nodes. There are also less-featured propagator nodes that simply speak with light IoT protocols and rely on other propagator nodes for IP communication [4].

In these scenarios, the IPv6 connections may be activated depending on a specific event or circumstance, with the lightweight IoT protocols being utilized for regular or routine interactions. Fundamentally, cellular 4G and LTE networks as well as the conventional Internet must live with and cooperate with IoT network protocols. To allow for this interoperability without burdening the countless billions of simpler end devices is the primary problem facing the developing Internet of Things architecture. The basic "chirp" structure of IoT data and how it is sent via the Internet of Things. The number of more advanced end devices linked to the Internet of Things that contain mission-critical data, larger data requirements, and/or real-time data demands is comparatively modest albeit it is still billions. The expenditures of these gadgets can be justified, and they will connect directly over IPv6 due to the processing, memory, and entire protocol stack complexity. A video surveillance camera or sophisticated process controller are two examples. At the same integrator functions, IPv6 data to and from these devices may still be merged with thin IoT data streams. Intriguing hybrid gadgets that have both a simple IoT interface and a conventional IPv6 connection can also emerge. The light IoT protocols might be used in these circumstances for standard or routine interactions, with the IPv6 connection becoming active-based.

Bibliography

[1] S. Saponara, T. Bacchillone, E. Petri, L. Fanucci, R. Locatelli, and M. Coppola, “Design of an NoC interface macrocell with hardware support of advanced networking functionalities,” *IEEE Trans. Comput.*, 2014, doi: 10.1109/TC.2012.70.

[2] R. Ho and D. Vogel, “The impact of social networking functionalities on online shopping: An examination of the web’s relative advantage,” *Int. J. Bus. Inf. Syst.*, 2014, doi: 10.1504/IJBIS.2014.060834.

[3] A. Biral and A. Zanella, “Introducing purely hydrodynamic networking functionalities

into microfluidic systems," *Nano Commun. Netw.*, 2013, doi: 10.1016/j.nancom.2013.09.001.

[4] R. Marasco, E. Rolli, M. Fusi, G. Michoud, and D. Daffonchio, "Grapevine rootstocks shape underground bacterial microbiome and networking but not potential functionality," *Microbiome*, 2018, doi: 10.1186/s40168-017-0391-2.

ISBN 978-81-962235-1-9 April 2023

M/S CIIR (R&D) Publications
B-17, Sector - 6, Noida,
Uttar Pradesh, India.
201301
Email: info@ciir.in

April 2023
ISBN 978-81-962235-1-9