A Review of Network Evolution towards a Smart Connected World

Olivia Haring
School of Information Technology
University of Cincinnati
Cincinnati, OH, USA

Sylvia Worlali Azumah
School of Information Technology
University of Cincinnati
Cincinnati, OH, USA

Nelly Elsayed
School of Information Technology
University of Cincinnati
Cincinnati, OH, USA

ABSTRACT

With the rapid innovations in technology, wireless internet-connected devices are more ubiquitous than ever and can be found in virtually every aspect of both our personal and professional lives. In this paper, we propose a comprehensive literature review that focuses on various network components that create connectivity among different devices, specifically Wireless Sensor Networks (WSNs), Radio-Frequency Identification (RFID) tags, Internet of Things (IoT) devices, and how these devices helped usher in the 4th Industrial Revolution, or Industry 4.0. This paper focuses on the protocols, architecture, uses, security concerns, and solutions used in these network technologies, as well as their differences and similarities.

General Terms

A Review of Network Evolution Towards a Smart and Connected World

Keywords

Internet of Things, Industry 4.0, wireless sensor network, RFID, networks

1. INTRODUCTION

The Internet of Things (IoT) is where the digital and physical worlds collide. IoT was first described as an internet-based information service. Much like how the internet revolutionized the way humans communicate with one another, IoT has helped usher in a new computing era. A report issued by Cisco estimates that there will be over 500 billion internet-connected devices that utilize sensors by 2030 [1].

From rudimentary wireless sensor networks (WSNs) to Radio-Frequency Identification (RFID), to the most complex of the Internet of Things (IoT) devices that form the backbone of smart factories, smart homes, and even entire smart cities, the technologies that underlie IoT devices have significantly changed the way humans interact with one another, their surroundings, and society as a whole. This comprehensive overview focuses on the history, application, architecture, challenges, solutions, and future of such technologies.

In this paper, we provide a comprehensive exploration of the evolution of different devices' networks. We discuss the inception of wireless sensors and RFID technology, how these technologies are interconnected to form complex IoT systems, and what this means for future advancements in industrialization.

2. WIRELESS SENSOR NETWORKS

Wireless sensor networks (WSNs) are comprised of many sensors that communicate by transmitting digital packets of information [2]. WSNs can contain anywhere from one sensor to hundreds of thousands of sensors. When these sensors are clustered together, they form what are referred to as nodes. These nodes are autonomous and extremely limited in their resources, due to the fact that they have minimal power supplies, processing capabilities, storage, etc. The lean nature of WSNs proves to be both an advantage and disadvantage [3].

2.1 History of WSNs

The first utilization of wireless sensor networks began in the 1950s with the United States military and the utilization of the "Sound Surveillance System" (SOSUS). This technology was used to detect enemy submarines and utilized acoustic sensors that measure the amplitude of ocean waves. Similar technology remains in use by the US military to this day [4, 5].

2.2 Architecture of WSNs

Wireless sensor networks are comprised of many sensors that communicate by transmitting digital packets of information [6]. WSNs can contain anywhere from one sensor, to hundreds of thousands of sensors [5]. When these sensors are clustered together, they form what is referred to as "nodes". These nodes are autonomous and extremely limited in their resources, due to the fact that they have minimalistic power supplies, processing capabilities, storage, etc. The lean nature of WSNs proves to be both an advantage and disadvantage [7].

WSN nodes are commonly arranged in a mesh, star, or hybrid (also know as tree) topology as shown in Figure 1 [8–11]. These nodes collect information from individual sensors and transmit that information to other nodes [12]. These sensor nodes are relatively simplistic when compared to today's modern technology and typically consist of a microcontroller, transceiver, external memory/storage, and at least one sensor [13]. However, it is common to have WSNs with hundreds, or even hundreds of thousands, of individual nodes. The overall architecture of a WSN includes these sensor nodes, an end-user, and a backend infrastructure that allows the end user to access these sensor nodes [14]. The underlying architecture will vary depending on what the purpose of the WSN is [4].

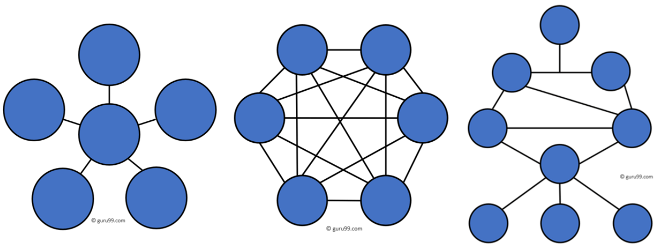


Fig. 1. Example of a star, mesh, and hybrid topologies.

2.3 Types of WSNs

While there are countless applications for individual sensors, there are five main types of WSNs: underground, underwater, terrestrial, multimedia, and mobile [3, 10].

2.3.1 Terrestrial WSNs. In terrestrial WSNs, hundreds or thousands of wireless sensors are deployed in a specific area. The sensors are either distributed in an unstructured (ad hoc) or structured (preplanned) fashion. When distributed ad hoc, the sensors are randomly distributed within the target area. As the name implies, preplanned distribution involves advanced planning to ensure optimal placement of the sensor nodes.
For terrestrial WSNs, the ability to reliably communicate and transmit data is crucial, especially in the oftentimes challenging environments they are deployed in. While battery power is limited in this type of WSN, it is possible to equip the sensor nodes with backup power supplies, such as solar cells [10, 15].

2.3.2 Underground WSNs. In underground WSNs, sensors are placed underground, most often in caves, mines, or simply burying them. Additional nodes are located above ground so that information can be transmitted from the sensors to the base station where the data is then collected and analyzed. Underground WSNs are more costly than terrestrial WSNs when it comes to their equipment, deployment, and ongoing maintenance. Since sensors in this type of deployment must reliably communicate through soil, rocks, water, and other earthen material, they incur increased costs. There is also the concern of signal loss because of the harsh underground environment. Unlike terrestrial WSNs, underground sensor deployment requires careful planning. As with terrestrial WSNs, underground sensor nodes have limited battery power and capacity, and once they are deployed underground, it is difficult and oftentimes impossible to repair, replace, or recharge sensor batteries [10, 15].

2.3.3 Underwater Wireless Sensor Network. In underwater wireless sensor network (UWSN), sensor nodes and autonomous underwater vehicles are used to gather data from aquatic environments. This is also a very costly deployment type, and as a result, fewer sensor nodes are deployed compared to underground or terrestrial WSNs. In this deployment type, typical communication is accomplished via transmission of acoustic waves. Special challenges for underwater WSNs include limited bandwidth, transmission delays, signal feeding issues, and the high rate of sensor node failure as a result of harsh environmental conditions. Sensor nodes that are placed underwater must be able to configure themselves and adapt to the challenging oceanic environments in which they are deployed. Underwater sensor nodes also have very limited battery capacity which cannot be replaced or recharged once they are deployed, so battery conservation is critical in UWSNs [10, 15].

2.3.4 Wireless Multimedia Sensor Network. The fourth type of wireless sensor networks are Wireless Multimedia Sensor Network (MWSN). This deployment type consists of a network of wireless, interconnected sensors that can retrieve multimedia content such as video, audio images, and sensor data from the environment in which they are deployed. This type of wireless sensor network consists of a number of low-cost sensor nodes equipped with cameras and microphones. Multimedia center nodes are deployed in a pre-planned fashion to ensure adequate coverage of the area being surveyed. There are a number of unique challenges to this type of WSN, including higher bandwidth requirements, higher energy consumption, and quality of service provisioning [10, 15].

2.3.5 Mobile Wireless Sensor Network. The final type of wireless sensor networks are mobile WSNs. This deployment type consists of a group of sensor nodes that are able to move independently and interact with their physical environment. These nodes have the ability to sense, compute, and communicate just as static nodes would. One difference is that mobile nodes are capable of re-positioning and reorganizing themselves within the network. A mobile WSN can be deployed in one way,then the nodes can eventually spread out to gather information as needed. Information gathered within a mobile node can be communicated to another mobile node if they are within range of one another. Another key difference is that mobile WSNs use dynamic routing, as opposed to the fixed routing used within static WSNs [10, 15].
Common concerns and challenges with mobile WSNs include deployment, navigation, coverage, maintenance, data processing, and battery life.
Regardless of which type of deployment is used, wireless sensor networks all share several traits with one another: scalability, reliability, responsiveness, mobility, and power efficiency [4]. All wireless sensor networks should have the capacity for scalability. Users should be able to expand the network and add or remove nodes as required, in a relatively easy fashion. Wireless sensor networks should also be generally reliable. There are many different methods for reducing the power usage of sensor nodes, which result in an increase in the lifetime of the network, and sensor consistency. Wireless sensor networks should also be responsive. Due to their simplistic architecture, wireless sensor networks should have a quick response time, even when things such as harsh environmental conditions are taken into consideration. Wireless sensor networks should also have a high degree of mobility, as this is the fundamental feature of WSNs. Since it is an inherently wireless network, mobility is an absolute necessity. Due to their deployment for long periods of time and the need for consistent and ongoing data transmission,power efficiency is crucial for wireless sensor networks [16].

2.4 WSN Communication Protocols

There is not one single communication protocol that is universally used in the deployment and life cycle of wireless sensor networks [4]. Instead, there are numerous protocols used at the transport, network/routing, datalink, and physical layers which are utilized depending on the purpose of the WSN in question. Due to the inherent restraints of WSNs, it is imperative to be mindful of energy consumption, latency, and load balancing when determining the appropriate protocol(s). In addition, emerging research has proposed cross-layer protocols to address various shortcomings in existing protocols.

Historically, research has focused primarily on protocols concerning the network or routing layer because this is the layer that typically varies the most depending on the WSNs purpose. The three main types of network layer architectures are categorized as either data-centric, hierarchical, or location-based [17].

2.4.1 Data-Centric. In data-centric routing protocols, also known as flat-based routing, all nodes in the WSN have the same role in that they transfer data via flooding. A potential issue with this protocol is that implosion is possible, meaning that two nodes send similar packets, inadvertently consuming large amounts of energy, and thus shortening the life of the WSN [17, 18].

2.4.2 Hierarchical-Based. In hierarchical-based, also referred to as cluster-based, two network layers are utilized: one to select the head cluster, and the other to send the actual data. The primary goal of this protocol is to bundle the nodes in such a way that preprocessing of data can be performed, so as to reduce energy consumption [17, 18].

2.4.3 Location-Based. In location-based routing protocols, the physical location where data originated from is used to transport information to a desired region or regions in the WSN, as opposed to sending it throughout the entire network. Except for the most simplistic, virtually all WSNs collect location information in order to calculate the distance between two nodes, and subsequently determine the energy usage [17, 18].

2.4.4 Data-centric. In data-centric routing protocols, also known as flat-based routing, all nodes in the WSN have the same role in that they transfer data via flooding. A potential issue with this protocol is that implosion is possible, meaning that two nodes send similar packets, inadvertently consuming large amounts of energy, and thus shortening the life of the WSN [17, 18].

2.4.5 Physical Layer. The physical layer is where tasks related to radio frequency and actual computations occur. Challenges in the physical layer include finding affordable radio transceivers that are energy-efficient, are not prone to significant radio interference, but also complex enough to perform the required tasks needed of the WSNs [19].

2.4.6 Cross-Layer Protocols. There has been a great deal of emerging research concerning cross-layer protocols for WSNs with the underlying goal of improving overall performance. These enhancements are often specific to the type of WSN and their precise priorities for improvement. Historically, there has been a focus on the interaction between the physical, data link, and routing layers. For example, existing research on cross-layer protocols have been proposed for specific objectives such as maximizing successful packet transmission, sleep duration, throughput, minimizing energy consumption, or just optimizing the overall performance of a WSN [20, 21].

2.5 Security Concerns and Solutions

Due to the unique nature of wireless sensor networks and their overall simplicity, traditional cybersecurity measures and techniques are not necessarily possible or effective. WSNs are traditionally left unattended and often do not have predefined infrastructures. Once data is transmitted, it is very easy for a malicious actor to sniff or spy on network traffic.Oftentimes sensor nodes are not made tamper-proof due to strict budget requirements, sensor nodes are not always made tamper proof, and therefore have no protection against physical security attacks. One of the inherent security benefits of WSNs is that they can be deployed in very harsh environments that are not easily accessible to everyday people. Cryptographic algorithms are generally used to address common security issues such as confidentiality, integrity, authentication, and availability. However, these cryptographic solutions are oftentimes simplified due to the resource limitations of wireless sensor networks. This in turn reduces the effectiveness of these security measures. Because of this, it is recommended there be a second line of defense when deploying a wireless sensor network. These defenses can include elements such as intrusion detection systems, and trust and authentication models. However, one of the fundamental flaws in wireless sensor networks remains their limited battery capacity, which limits the level of sophistication that can be used in security solutions [22].

3. RADIO FREQUENCY IDENTIFICATION

Radio frequency identification (RFID) is a type of wireless, automated technology that utilizes radio signals to identify tiny integrated circuit transponders known as RFID tags. These tags are equipped with antennas that communicate with their reading devices (RFID readers) using electromagnetic fields. It is also common for there to be a back-end database that collects information related to the physical objects that have RFID tags on them.

There are three commonly used types of RFID tags, each with their own advantages and disadvantages. The first is known as an active, or battery powered RFID tag. These tags need battery power to function,which makes them much more costly, and therefore less common. These tags typically have enough battery power to last several years, possess the ability to read and write data, and can transmit signals over the greatest distance [23]. The second type of RFID tag is known as a passive RFID tag. These tags do not contain a battery, but instead work by using electromagnetic energy that is transmitted from the reader to the tag. Since they do not contain a battery, they are much more cost efficient, economical, and often much smaller then active tags. The third type of RFID tag is referred to as a semi-passive tag. While these tags contain a battery that primarily functions to ensure data integrity, it is the signal sent from the reader that actually generates power which allows signal transmission from the tag to the reader [23].

Passive RFID tags typically work on three different radio frequencies: low frequency, high frequency, and ultra-high frequency. High frequency communication is also known as Near Field Communication or NFC [24–26]. Figure 3 shows the description of the RFID frequencies and their real-world applications.

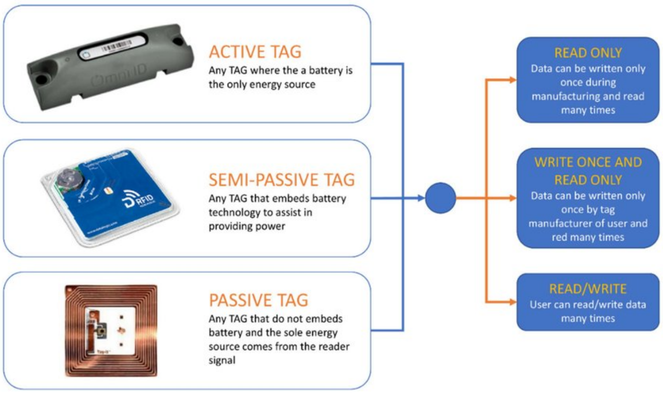
3.1 History of RFID

A precursor to RFID technology was first observed in 1945 during WWII and was used by Soviet spies. This rudimentary technology rebroadcast radio waves with added audio information.

The concept of RFID as we know it today was first envisioned by Harry Stockman in his 1948 paper “Communication by Means of Reflected Power.” However, it would take more than 30 years for Stockmans vision to become technologically feasible.

By the 1970s, corporations had made considerable advancement in the development of RFID technology. Notable examples include Raytheon’s Raytag in 1973 and Richard Klensch of RCA developing an electronic identification system in 1975.

The 1980s is when RFID technology began to actually be implemented. However, the means by which RFID was implemented varied. In the United States, there was a focus on implementing this technology for transportation, employee and personnel access,


ACTIVE TAG
Any TAG where the a battery is the only energy source
SEMI-PASSIVE TAG
Any TAG that embeds battery technology to assist in providing power
PASSIVE TAG
Any TAG that do not embeds battery and the sole energy source comes from the reader signal
READ ONLY
Data can be written only once during manufacturing and read many times
WRITE ONCE AND READ ONLY
Data can be written only once by tag manufacturer of user and red many times
READ/WRITE
User can read/write data many times

(b)

Fig. 2. The three types of RFID technology.

and to a lesser degree, animal monitoring. In Europe, there was a larger focus on RFID for animal monitoring. Despite the lesser focus on transportation applications, the European country of Norway became the first to implement RFID technology as a means of collecting tolls. This was followed closely in the United States in 1989 when the Dallas North Turnpike became the first to use RFID for toll collection. Soon after, the Port Authority of New York and New Jersey implemented RFID-based toll collections for buses going through the Lincoln Tunnel.

The 1990s saw an increased implementation of RFID as a means of toll collection throughout the United States, and there were over three million RFID tags installed on rail cars in North America by the end of the decade.

The 21st century ushered in a new era for RFID technology, as major advances resulted in the smallest ever RFID technology– so small it could be manufactured as a thin, adhesive label that could be attached to virtually any surface. Connecting this breakthrough technology to the internet is what ultimately helped RFID become a critical component of numerous IoT devices [27, 28].

3.2 Uses for RFID Technology

Due to passive RFID tags costing only cent to manufacture and having the ability to be applied virtually anywhere in the form of stickers, this technology is a cost-effective way to turn just about any item into a "smart" item. Much like wireless sensor networks, RFID tags are particularly useful in challenging environments since they require little to no human supervision once they are deployed. RFID tags can typically be read through a number of environmentally challenging conditions, such as snow, ice, fog, or when objects cannot be directly touched, such as items on pallets in warehouses. Oftentimes, readers do not need to have direct contact with the RFID tag in order to be read. This is beneficial in occupational situations where the object in question may be exposed to paint, grime, mud, etc.

RFID technology is seen in virtually every industry imaginable, from inventory control systems in retail stores, toll collection, logistics and supply chain management, animal tracking, employee identification badges, healthcare, consumer smart devices, and more. RFID tags can even be implanted into the human body and were approved by the FDA in 2004 [25, 29, 30].

3.3 RFID Communication Protocols

RFID tag technology utilize low frequency (125134 kHz), high frequency (13.56 MHz), and ultra-high frequency (300 MHz-3GHz) radio signals to communicate wirelessly with a reader. Figure 2 shows the three types of RFID radio signals to communicate wirelessly with a reader technology types. Unlike WSNs, the various types of RFIDs have well-established industry standards regarding communication protocols [26, 31].

The most commonly utilized standard for high frequency RFID tags is ISO/IEC 15693, which was most recently updated in 2019. This standard is applicable to what are commonly referred to as vicinity cards or RFID tags that have a maximum read distance of 1 meter. As with the standard for LF RFID tags, ISO/IEC 15693 provides precise technical parameters for HF RFID tags, including the physical layer used between the reader and tag, and the anti-collision methodology used to detect and communicate with a specific tag when several tags are present.

The most commonly utilized standard for high frequency RFID tags is ISO/IEC 15693, which was most recently updated in 2019. This standard is applicable to what are commonly referred to as vicinity cards or RFID tags that have a maximum read distance of one meter. As with the standard for LF RFID tags, ISO/IEC 15693 provides precise technical parameters for HF RFID tags, including the physical layer used between the reader and tag, as well as the anti-collision methodology used to detect and communicate with a specific tag when several tags are present.

While both active and passive tags operate on the ultra high frequency range (300 to 100MHz), only two frequency ranges are actually utilized. These ranges include 433 MHz for active tags, and a range of 860-890 for passive tags. Unlike WSNs, passive UHF RFID tags have a widely accepted industry standard known as the Electronic Product Code (EPC) Class1 (C1) Generation2 (Gen2) standard, informally referenced as EPC Gen 2 [30, 32–34].

3.4 RFID Security Concerns and Solutions

As with any ubiquitous technology, there are numerous security concerns. These include concerns regarding consumer privacy, physical tampering, and malicious cyberattacks.

3.4.1 Consumer Privacy. Since RFID technology is essentially undetectable, this can result in both profiling and location tracking of consumers without their consent or knowledge. Existing publications and literature regarding consumer privacy concerns of RFID technology can be categorized into five general themes. The first is the undetectable and concealed nature of RFID tags. Tags can be embedded in or on almost any object without the consumer knowing. Another criticism is that RFID technology provides the ability to mass-identify objects. Each RFID tag consist of unique identifying information. In a worst-case scenario, this could lead to the creation of a globalized system in which every physical object is identified and linked to its owner at the point of sale, or when it is transferred. There is also concern regarding the inherent ability to collect massive amounts of data. Since a primary function of RFID data that is collected is the creation of databases, databases containing this tag data could be linked to personally identifying information. This particular concern is especially worrisome as computing power continues to increase. RFID tags also allow the opportunity to profile and track people. If personally identifying information were to be linked with unique information contained in RFID tags, individuals could be tracked or profiled without their consent or knowledge. Finally, the ability for tag readers to function without being directly in contact with tags has created additional privacy

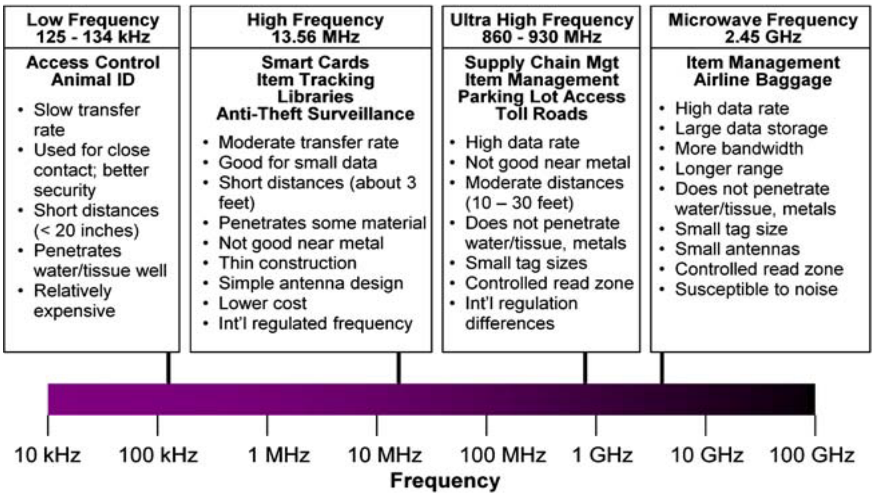


Fig. 3. An overview of RFID frequencies and their real-world applications.

concerns. Readers could be incorporated into virtually any setting where people gather, resulting in information being easily accessible and collected into databases [29].

3.4.2 Physical Tampering. Passive RFID tags inherently have poor physical security and are extremely prone to physical manipulation. This can include things such as attacks that permanently or temporarily disable the tags, or physically removing or destroying the tag. When RFID tags are used as anti theft measures in retail settings, it is possible for malicious customers to simply remove the RFID tag and walk out of the store with the merchandise.

While RFID tags can be used in challenging environments, they are still susceptible two possible destruction as a result of extreme environmental conditions, such as temperatures that are too high or too low, or damage caused by rough handling. Active RFID tags can also be made inoperable by merely removing or discharging the battery. RFID tags are very sensitive to static electricity, and their electronic circuits can be instantly damaged by electrostatic discharge . This is especially concerning in warehouse environments, as conveyor belt picking systems often carry a large amount of static electricity. There are also several special privacy protecting devices that people can purchase, or create themselves, such as "RFID zappers."

There are also security concerns surrounding RFID readers. Handheld RFID readers can be destroyed, removed, or even stolen if they are left unattended. RFID readers oftentimes include sensitive information such as keys and other cryptographic credentials. Theft of RFID readers could potentially allow malicious attackers to gain access to the back-end database where sensitive information such as personally identifiable information or company trade secrets may be stored [35].

In order to safeguard RFID systems against low-tech attacks such as permanently or temporarily disabling tags, traditional countermeasures should be used, such as increased physical security with guards, fences, gates, locked doors and cameras. Whenever possible, it is advisable to not merely stick an RFID tag directly on an item, but embedded in the item and or packaging itself to prevent tampering. In retail settings, stores will often have alarm systems that are triggered if a tag is not deactivated at the point of sale [29].

3.4.3 Cyberattacks. Tags with little to no protection are especially vulnerable to eavesdropping, traffic analysis, spoofing, denial of service, and other cyber attacks. It is possible to initiate a denial of service attack by flooding an area with radiofrequency energy, thereby incapacitating RFID readers. RFID tags are inherently designed to be readable by any compliant reader. This in theory could allow any user with a reader to scan tagged items, often from significantly far away, potentially releasing sensitive information to malicious actors.

It is also possible to mimic genuine RFID tags by writing correctly formatted data onto blank RFID tags. This could allow for spoofing of data. Malicious actors could also flood a system with an overwhelming amount of data, more than it was designed to handle. Theoretically, a person could remove a tag, and then place it on other items, causing the system to record useless data, and thereby devaluing the back end database. This is especially concerning for larger corporations that widely use RFID tags for inventory control and security measures, such as retail stores.

Unauthorized readers can impact privacy by accessing tags that are lacking access control. Even if the tag content is secure it can still be tracked by the predictable tag responses; "location privacy" can be affected by a traffic analysis attack. Attacker can also threaten the security of systems, which depends on RFID technology, through the denial of service attack [34].

RFID tag standards incorporate a 64-bit region that cannot be modified and remains unique to the tag itself. This can be used to authenticate the tag and defends against tag spoofing. A number of different attacks,such as replay attacks, can be rebuffed through the use of hidden authentication schemes such as serial numbers, or rudimentary key cryptography specific to RFID tags that has been developed by researchers [34, 36].

RFID tags are indiscriminate, they are designed to be readable by any compliant reader. Unfortunately, this lets unauthorized readers scan tagged items unbeknownst to the bearer, often from great distances.

Attackers and anti-RFID activists can mimic authentic RFID tags by writing appropriately formatted data on blank RFID tags, and could also remove RFID tags and plant them on other items, causing RFID systems to record useless data, discrediting and devaluing RFID technology [27].

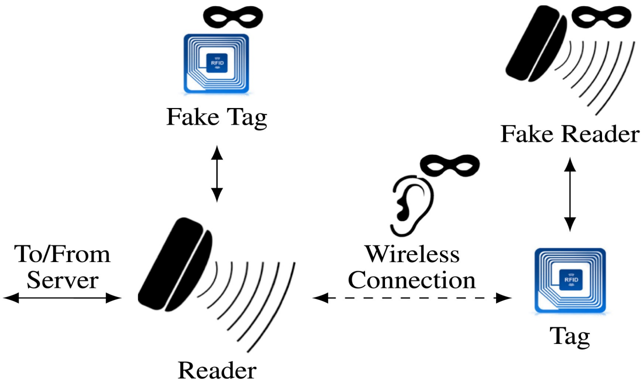


Fig. 4. Fake RFID tags and readers are just one of the many security concerns surrounding this technology.

4. INTERNET OF THINGS

The Internet of things or IoT is a system of internet-connected objects (or things), that are embedded with sensors or other data-collecting technology that enables them to send and receive data [37, 38].

4.1 History of IoT

The term "Internet of Things" is credited as being coined in 1999 by Kevin Ashton, an employee of the Massachusetts Institute of Technology. He described it as "a system of interconnection between the physical world and the Internet through the use of RFID and pervasive sensor devices that identify and observe the real world."
However, a rudimentary interconnection between everyday objects and the internet had already been developed in the early 1980s. Employees at Carnegie Mellon University connected a soda vending machine to the Internet in order to check the inventory and availability of drinks in the machine [39].

4.2 IoT Architecture and Communication Protocols

There is no single or general agreement about the architecture of IoT that is recognized by world's researchers and professionals. Various IoT architectures have been proposed which range from three layers to more complex architectures with seven or more layers. In each of these layers, you will find previously discussed protocols such as those found within WSNs and/or RFID, since IoT devices often contain these technologies.
At its most simplistic form, there are three layers to IoT architecture: the perception, network, and application layers as shown in Figure 5.
The five-layer IoT architecture consists of the following layers: perception, transmission/network, middleware, application, and business [40, 41]. The five-layer IoT architecture is shown at Figure 6.

4.3 IoT Security Concerns and Solutions

The fact that there is an overall lack of standardization and regulation around IoT security is itself a major security concern. Many IoT devices are composed of rudimentary technology such as RFID and WSNs, meaning that they lack the hardware capacity to support a vigorous security infrastructure.
Especially in the context of industrial IoT such as factories, manufacturing plants, or general corporate settings, smart devices can prove to be extremely lucrative targets for threat actors. These can be targets for professional cyber criminals with significant training, which can result in severe financial damages and major consequences for the victim organizations.
For all IoT devices, but especially those that are particularly sophisticated or contain sensitive or valuable data, it is advisable to implement a number of cybersecurity best practices. These can include things such as two factor authentication, biometrics, digital certificates, and ensuring there are antivirus, antimalware, firewalls, and intrusion prevention and detection systems present. It is also advisable that all data between IoT devices and back-end systems be encrypted [35, 40, 42, 43].

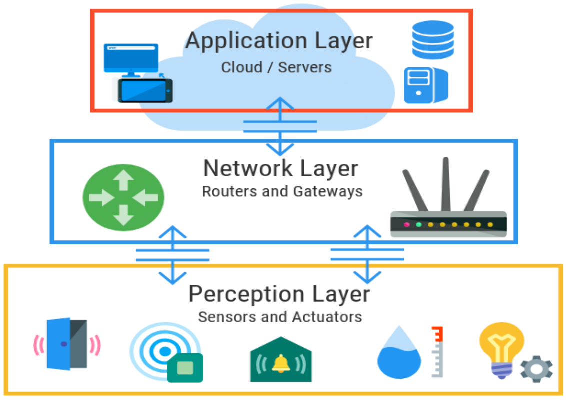


Fig. 5. The three layer model of IoT architecture.

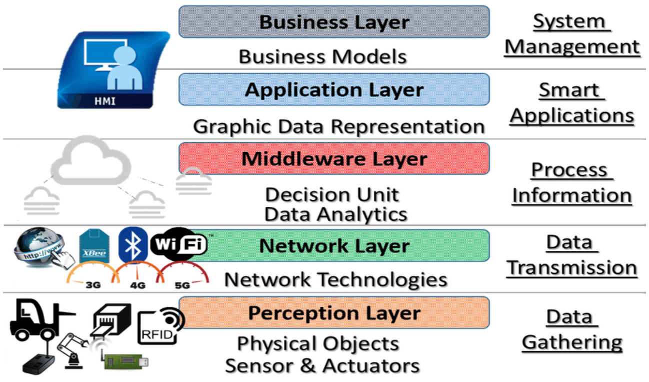


Fig. 6. The five layer model of IoT architecture.

5. INDUSTRY 4.0

The Fourth Industrial Revolution, also known as Industry 4.0, is a term coined to refer to the rapid transformation into automation of traditional manufacturing and industrial practices the smart technology. Industry 4.0 has led to the creation of what is known as "smart factories." Technologies such as machine-to-machine communication are integrated with the Internet of Things and manufacturing processes to increase automation, improve communication, and increase the self-monitoring, analyzing, and diagnosing of machinery without the need for human intervention. Technology associated with Industry 4.0 is heavily reliant upon cyber-physical systems such as sensors that collect and analyze huge amounts of data which is then used by machine operators, manufacturers, and other stakeholders to improve efficiency and output. Advancements in computing power and processing speed allows for systems which can scan huge sets of data and produce insights that can be acted upon quickly by humans. Industry 4.0 and Big Data go hand-in-hand, as these technologies allow collection of data at scales never before thought possible [38,44,45].

6. CONCLUSION

While there have been vast technological breakthroughs regarding IoT technology, we have only scratched the surface of what this technology is truly capable of. IoT is like the Wild West in that it is largely unregulated, with every company hoping to strike gold. There remain a number of concerns that need to be resolved for this technology to continue advancing. These issues include security and privacy, storage, energy usage, and the communication, compatibility, and standardization between different IoT devices.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. (CNS-1801593). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

7. REFERENCES

[1] A. H. M. Aman, E. Yadegaridehkordi, Z. S. Attarbashi, R. Hassan, and Y. Park, “A survey on trend and classification of internet of things reviews,” 2020. ID: 1.

[2] S. Tree, “Wireless sensor networks,” *Self*, vol. 1, no. R2, p. C0, 2014.

[3] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, “Wireless sensor networks: a survey on recent developments and potential synergies,” *The Journal of supercomputing*, vol. 68, pp. 1–48, 2013; 2014.

[4] M. Kocakulak and I. Butun, “An overview of wireless sensor networks towards internet of things,” in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1–6, 2017.

[5] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” *Computer networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[6] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, *Wireless sensor networks*. Springer, 2006.

[7] M. A. Perillo and W. B. Heinzelman, “Wireless sensor network protocols.,” 2005.

[8] R. Bruno, M. Conti, and E. Gregori, “Mesh networks: commodity multihop ad hoc networks,” *IEEE communications magazine*, vol. 43, no. 3, pp. 123–131, 2005.

[9] T. Baykas, L. Goratti, T. Rasheed, and S. Kato, “On the spectrum efficiency of mesh and star topology wide area wireless sensor networks,” in *2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*, pp. 1819–1823, IEEE, 2014.

[10] M. K. Singh, S. I. Amin, S. A. Imam, V. K. Sachan, and A. Choudhary, “A survey of wireless sensor network and its types,” in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 326–330, IEEE, 2018.

[11] Q. Mamun, “A qualitative comparison of different logical topologies for wireless sensor networks,” *Sensors*, vol. 12, no. 11, pp. 14887–14913, 2012.

[12] M. J. McGrath and C. N. Scanaill, “Key sensor technology components: hardware and software overview,” in *Sensor technologies*, pp. 51–77, Springer, 2013.

[13] M. A. M. Vieira, C. N. Coelho, D. j. da Silva, and J. M. da Mata, “Survey on wireless sensor network devices,” in *EFTA 2003. 2003 IEEE Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No. 03TH8696)*, vol. 1, pp. 537–544, IEEE, 2003.

[14] L. M. Borges, F. J. Velez, and A. S. Lebres, “Survey on the characterization and classification of wireless sensor network applications,” *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 1860–1890, 2014.

[15] A. Ali, Y. Ming, S. Chakraborty, and S. Iram, “A comprehensive survey on real-time applications of wsn,” *Future internet*, vol. 9, no. 4, p. 77, 2017.

[16] B. Kan, L. Cai, and L. Zhao, “An accurate energy model for WSN node and its optimal design,” in *2007 International Conference on Communications, Circuits and Systems*, pp. 328–332, IEEE, 2007.

[17] S. K. Singh, M. Singh, D. K. Singh, *et al.*, “Routing protocols in wireless sensor networks–a survey,” *International Journal of Computer Science & Engineering Survey (IJCSES)*, vol. 1, no. 2, pp. 63–83, 2010.

[18] K. Akkaya and M. Younis, “A survey on routing protocols for wireless sensor networks,” *Ad hoc networks*, vol. 3, no. 3, pp. 325–349, 2005.

[19] H. M. A. Fahmy, “Protocol stack of wsns,” in *Wireless Sensor Networks*, pp. 55–68, Springer, 2016.

[20] S. Nedevschi, L. Popa, G. Iannaccone, S. Ratnasamy, and D. Wetherall, “Reducing network energy consumption via sleeping and rate-adaptation.,” in *NsDI*, vol. 8, pp. 323–336, 2008.

[21] D. Resner, G. M. de Araujo, and A. A. Fröhlich, “Design and implementation of a cross-layer IoT protocol,” *Science of Computer Programming*, vol. 165, pp. 24–37, 2018.

[22] D. E. Boubiche, S. Athmani, S. Boubiche, and H. Toral-Cruz, “Cybersecurity issues in wireless sensor networks: Current challenges and solutions,” *Wireless personal communications*, 2020.

[23] J. Curtin, R. J. Kauffman, and F. J. Riggins, “Making the MOSTout of RFID technology: a research agenda for the study of the adoption, usage and impact of rfid,” 2007.

[24] R. Weinstein, “RFID: a technical overview and its application to the enterprise,” *IT professional*, vol. 7, no. 3, pp. 27–33, 2005.

[25] E. Ngai, K. K. Moon, F. J. Riggins, and Y. Y. Candace, “RFID research: An academic literature review (1995–2005) and future research directions,” *International Journal of Production Economics*, vol. 112, no. 2, pp. 510–520, 2008.

[26] “Rfid,”

[27] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, “The evolution of RFID security,” *IEEE pervasive computing*, vol. 5, no. 1, pp. 62–69, 2006.

[28] J. Landt, "The history of RFID," *IEEE potentials*, vol. 24, no. 4, pp. 8–11, 2005.

[29] K. Jung and S. Lee, "A systematic review of RFID applications and diffusion: key areas and public policy issues," *Journal of open innovation*, vol. 1, no. 1, pp. 1–19, 2015.

[30] D. M. Dobkin, *The RF in RFID: UHF RFID in practice*. Newnes, 2012.

[31] A. Ibrahim and G. Dalkılıc, "Review of different classes of RFID authentication protocols," *Wireless Networks*, vol. 25, no. 3, pp. 961–974, 2019.

[32] J. Al-Kassab and W.-C. Rumsch, "Challenges for RFID cross-industry standardization in the light of diverging industry requirements," *IEEE systems journal*, vol. 2, no. 2, pp. 170–177, 2008.

[33] N. Adhiarna and J.-J. Rho, "Standardization and global adoption of radio frequency identification (RFID): strategic issues for developing countries," in *2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*, pp. 1461–1468, IEEE, 2009.

[34] J. H. Khor, J. H. Khor, W. Ismail, W. Ismail, M. I. Younis, M. I. Younis, M. K. Sulaiman, M. K. Sulaiman, M. G. Rahman, and M. G. Rahman, "Security problems in an RFID system," *Wireless personal communications*, vol. 59, no. 1, pp. 17–26, 2011.

[35] K. Lounis and M. Zulkernine, "Attacks and defenses in short-range wireless technologies for IoT," 2020. ID: 1.

[36] R. Pateriya and S. Sharma, "The evolution of RFID security and privacy: A research survey," in *2011 International Conference on Communication Systems and Network Technologies*, pp. 115–119, IEEE, 2011.

[37] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of things (IoT) communication protocols," in *2017 8th International conference on information technology (ICIT)*, pp. 685–690, IEEE, 2017.

[38] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of things is a revolutionary approach for future technology enhancement: a review," *Journal of Big Data*, vol. 6, no. 1, p. 111, 2019. ID: Kumar2019.

[39] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. Aswathy, "A state of the art review on the internet of things (IoT) history, technology and fields of deployment," in *2014 International conference on science engineering and management research (ICSEMR)*, pp. 1–8, IEEE, 2014.

[40] M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, "Iot elements, layered architectures and security issues: A comprehensive survey," *Sensors (Basel, Switzerland)*, vol. 18, no. 9, p. 2796, 2018.

[41] N. M. Kumar and P. K. Mallick, "The internet of things: Insights into the building blocks, component interactions, and architecture layers," *Procedia computer science*, vol. 132, pp. 109–117, 2018.

[42] C. Li and B. Palanisamy, "Privacy in internet of things: From principles to technologies," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 488–505, 2019. Cited By :21.

[43] Y. Lu, A. Wang, and S. Liu, *A mutual authentication lightweight RFID protocol for IoT devices*, vol. 1227 CCIS. 2020.

[44] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," *Business & information systems engineering*, vol. 6, no. 4, pp. 239–242, 2014.

[45] A. Kravets, A. A. Bolshakov, M. V. Shcherbakov, O. Library, and I. Network, *Cyber-physical systems: industry 4.0 challenges*, vol. 260. Cham: Springer, 2020; 2019.