Internet of Things, Connectivity, Network Topology and Theory and Cybersecurity

Dhanushga Lionel
Ontario Tech University
Ontario, Canada
dhanushga.lionel@ontariotechu.net

Abstract

The Internet of Things is a network that allows household/everyday objects to interact and communicate with each other. They can exchange data, allowing these objects to collaborate, and offer better services for the user. This paper examines topics that involve IoT, including Connectivity, Network Topology and Theory, and Cybersecurity issues that arise in IoT.

Introduction

Imagine a world without the Internet. No Instagram. No Snapchat. No more Facebook, even though no one under 25 uses it. No Youtube. No "...". Without the Internet, the world would be in a dystopian future in the Hunger Games.

The Internet is now less a tool and more a necessity of life. We can now communicate with people who aren't even on Earth. We can share memories with our families who live half a world away with just a click of a button.

The Internet can break or make businesses, both large and small. Some of the biggest companies in the world rely on the Internet to succeed. Companies like Google, Microsoft, … would not exist without the Internet.

Political campaigns are won or lost on the Internet. Almost 75% of Internet users went online to get political news and talk about their candidates during the 2008 campaign, and in 2012, more than a fifth of registered voters announced their candidate on Twitter or Facebook [1].

The Internet of Things, or IoT for short, is the next phase of evolution for the Internet, and ourselves. Now millions of interconnected devices, can communicate with each other, all for the goal of bettering the users life.

Network Theory

The main concept of the Internet of Things is connectivity. Without a base connection with other devices, everyday devices would not be able to communicate with each other. Network theory delves into how connections between devices are made and

decides which connections are the most crucial to the network. Network Theory is also considered a subcategory of Graph Theory and is part of a multitude of other theories involving physics, mathematics, etc [1].

In terms of network theory, a network (in terms of the Internet of Things) is considered a collection of nodes (collection of points) linked in pairs by lines [1]. The geometry of how the network is connected is considered the network Topology and can be divided into two subcategories: Physical and Logical topologies (discussed later) [2].

Networks can be seen as structures, forming a creation of elements surrounding the network. Elements within a network are for the most part independent and only limited by any outside variables (lack of data, lack of resources, etc.). [2]

Graph Theory-History

In Order to fully understand Network Theory, we must first take a look at Graph Theory. Graph Theory is the study of the mathematical properties of graphs and builds the theoretical foundation for modern network theory [2]. Graphs can be defined as mathematical structures that model pairwise relations between objects. Graph theory is a tool to look at the underlying structure of complicated objects and dynamic phenomena.

Graph Theory was first discovered as a paper by Leonhard Euler that involved solving the Königsberg Bridge problem. For some context of the problem, the German city of Konigsberg was settled on the river Pregel. It was set on both sides of the river and had two islands in which all of it was connected by seven bridges. The problem was discovering a route through the city that would cross each and every bridge once and only once. Euler declared that there was no such route. Euler pointed out that regular measurements and calculations wouldn't account for this type of issue and instead created a new kind of geometry. Euler was able to come up with the observation by constructing a network with 4 nodes and 7 edges.

Graph Theory-Concepts

In terms of graph theory, a Network is a graph with associated numerical values. Graph Theory involves many different concepts and properties. Below is some of the more important concepts and properties that form a big chunk of the theory:

Arcs

-connections between nodes [1]

-Arcs can either be directed (defined direction to node 1 to 2) or undirected (undefined direction between 2 nodes). These properties define if the graph is defined or undefined [1]

Connectivity

-defines number of arcs connected to a node.

- In undirected and unweight networks, the nodal degree is calculated from the sum of all edges connected to a network [1]

-in directed and weighted networks, the degree could be split into either an inward or outward degree [1]

-inward degree's equivalent to number of nodes connected to a certain node and vice versa for outward degrees

-The degree of the node decides the rate of speed at which the node can get data, the higher degree the node the bigger the chance of the node receiving data But if network is compromised, the first victims will be the higher degree nodes [1]

Network Topologies

A network topology refers to the layout of a network and how the different nodes in a network are linked together and how they send and receive messages [3]. Network topologies can be divided into 2 categories: Physical topologies (physical layout of devices on a network) and Logical topologies (the method on how signals act on network media or how data goes through the network from one device to the other) [1]. Topologies are used in many real life networks like smart homes, Bluetooth connectivity, etc. The 5 main types of topologies are: Mesh, Star, Bus, Ring, and Tree topology [3]. The main ones used nowadays are star and mesh topologies.

Star Topologies

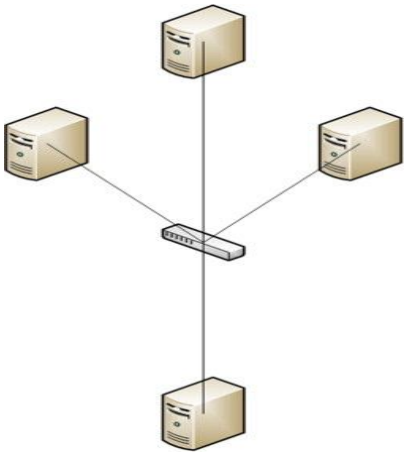

Figure 1: Star Topology

A star network is when multiple devices are connected to a central computer (referred to as a hub) [3]. These devices can communicate with each other by passing info through the hub [3]. Physical limitations may also occur (cable length, number of ports available on devices used for the network, etc.) but star topology handles this by extending into multiple star topologies with a central core in the multiple (referred to as a backbone of the network) [4].

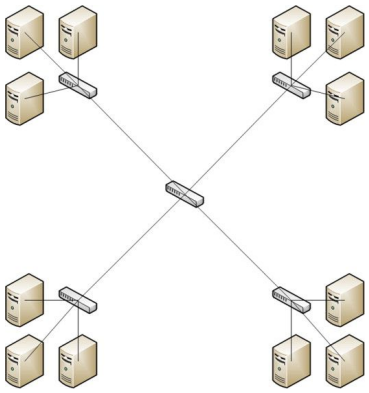

Figure 2: Star Topology with backbone

Advantages

1. Easy to Manage
2. High Speeds for data Transfer
3. Easy to expand network without future problems

Disadvantages

1. Network Performance entirely depends on the hub
2. If Hub goes down, then the entire network goes down

Mesh Topologies

A mesh network involves connecting all the computers to each other in a network. This setup allows for the devices to not only send signals but can relay data from the other nodes in the network [5]. Mesh networks can be divided into two categories: fully connected mesh network or partially connected mesh network. A full mesh involves connecting all devices to each other [5].

It is very redundant but can be expensive to implement. The main advantage is that the network traffic could be directed to other nodes if a node fails to function [5]. A partial mesh is more practical compared to a full mesh but is less redundant. A partial mesh doesn't allow for all computers to be connected with each other.

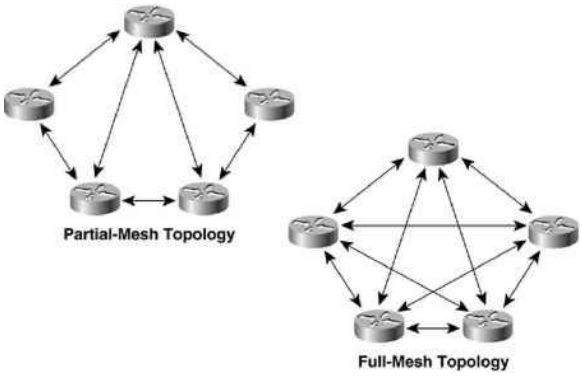

Figure 3: Mesh Topologies

Advantages

1. Provides high privacy and security
2. No traffic problems (since there is point to point links)
3. Fault identification is easy (due to being point-to-point links)

Disadvantages

1. Requires high number of cables and I/O ports for communication
2. Costly compared to other topologies

Hybrid Topologies

A hybrid topology is considered a combination of two or more topologies. This allows for the network to inherit both of the advantages and disadvantages of the network [6]. The most commonly used hybrid topologies are the Star-Ring topology and the Star-Bus topology.

Advantages

1. Combines the advantages of different topologies
2. Flexible
3. Good scalability
4. Very reliable

Disadvantages

1. Very Expensive
2. Design and structure can be complex

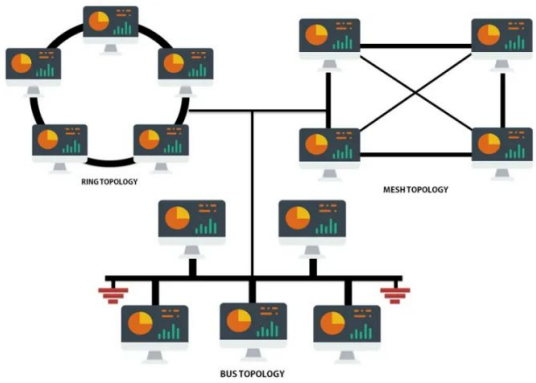

Figure 4: Hybrid Topology with ring, mesh and bus topologies

Cyber Security

While the Internet of Technology continues to expand, so to does the security concerns that come with IoT. The fundamental nature of the Internet and IoT is one of interconnectedness. While this is important, this also means that any internet connected resources can be attacked through a number of different methods. This makes cyber security issues paramount when talking about IoT.

An IoT architecture can be represented by 3 layers: application, transport and sensing. A more detailed architecture can be defined with 5 layers, Perception, Network, Middleware, Application, and Business [9]. In this section, 4 main key levels will be discussed, as shown in Figure 1 below. Each layer will be briefly described. Then more detail will be given to particular problems that face each layer, and then what the security is at different layers.

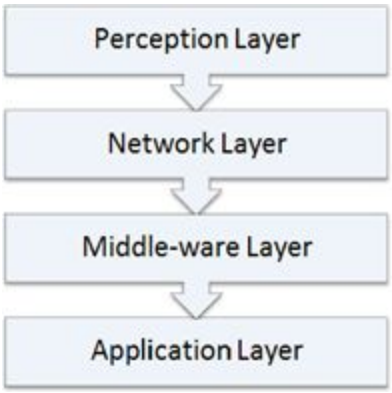

Figure 5: 4 Key Layer Architecture of IoT

1. Perception Layer

Consists of different kinds of data sensors like RFID, barcode and other sensor network. The purpose of the perception layer is to identify objects, and do something with the data obtained from the sensor.

2. Network Layer

Also known as the 'transmission layer'. It is responsible for securely transferring data from sensory devices to the information processing system.

3. Middleware Layer

This is the service-oriented layer. It makes automated actions based on the processed data results. It also links the IoT system with a database [6].

4. Application Layer

Layer that allows different IoT devices to communicate with each other. For example, smartphones can communicate with a smart door lock to tell it user is home, and to unlock the door [8].

5. Problems at Perception Layer

There are a number of challenges that plague the perception layer. These include unauthorized access to tags, cloning and spoofing, eavesdropping and replay, DoS and Man-in-the-Middle Attack [2] [5].

5.1 Unauthorized access to tags: RFID systems can be accessed easily, with the data being susceptible to modification, or deletion. This is because a large number of RFID systems do not have proper authentication systems. Due to this, tags can be accessed easily, without authorization [3].

5.2 Cloning and Spoofing: Tags can be easily cloned by duplicating data from original tag. Due to this, the sensor reader cannot tell the difference between the original and cloned tag [4]. Spoofing is using cloned tag to gain access to secured system [5].

5.3 Eavesdropping and Replay: Unauthorized RFID reader can listen to the conversation between the tag and reader, and obtain important and/or confidential data. Replay follows eavesdropping, and is when one part of the communication in an RFID system is recorded, and then replayed later to the receiver to gain access or steam information [5]. Since RFID is wireless, it is very easy for hackers to get any confidential and/or important data from the tag-to-reader, or vice-versa.

5.4 Denial of Service: DoS attacks can happen when system is jammed through noise interference, radio signal blocking, or removing/disabling RFID tags [5].

5.5 Man-in-the-Middle Attack:
Man-in-the-Middle Attack happens during the

transmission of a signal. Attacker intercepts for communication between reader and tag, and manipulated information [5].

6.Problems at Network Layer

Issues that face the network layer include sybil attacks, sinkhole attacks, sleep deprivation attacks, malicious code injection, DoS attacks, and man-in-the-middle attacks [2]. DoS and Man-in-the-middle attacks have already been explained in section 1.1.4 and 1.1.5 respectively.

6.1 Sybil Attack: Sybil attack is a type of attack where a node in the network operates multiple identities to gain authority in the system. The main purpose is to gain a majority influence in the network, and carry out dangerous actions [10].

6.2 Sinkhole Attack: This attack makes compromised nodes look attractive to other nodes. Because of this, the data is rerouted to the compromised node. This can also lead to a DoS attack [11].

6.3 Sleep Deprivation Attack: The deployment of sensors, especially in hostile environments makes it vulnerable to battery drainage attacks, because it is hard, if not impossible, to replace the battery of the power of sensor nodes[12]. This type of attack is to keep the nodes awake, resulting in more battery consumption, and as a result the lifetime of the battery is greatly diminished, which causes the nodes to shut down [13].

6.4 Malicious Code injection: Compromised node is injected with malicious code, that could result in complete shutdown of network, or even giving full control of network to attacker [14].

7. Problems at Middleware Layer

Types of attacks that haunt the middleware layer include unauthorized access, DoS attacks and malicious insider attacks. DoS attacks have been already explained in section 5.4.

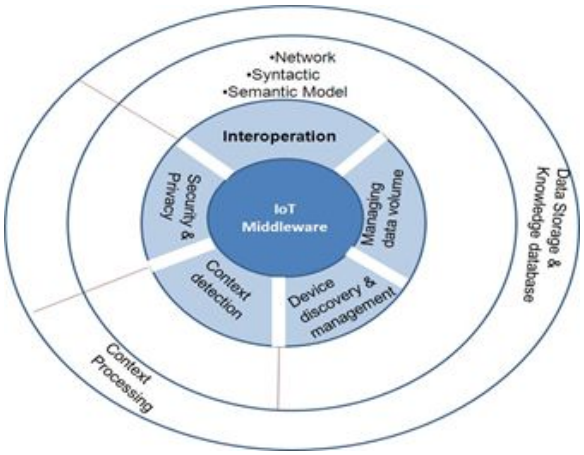

Figure 6: Components of middle-ware layer

7.1 Unauthorized Access: Attackers can get access to the middleware layer. Because the middleware layer has interfaces with application and data, attackers can cause damage to system by forbidding access to much needed services, or deleting existing data.

7.2 Malicious Insider: Malicious insider attack can occur when someone on the inside tampers with the data.

8. Problems at Application Layer

Application layer challenges include malicious code injection, DoS attacks, spear-phishing attacks, and sniffing attacks. Malicious code injection and DoS attacks have been explained in section 6.4 and 5.4 respectively.

8.1 Spear-Phishing Attacks: Is the targeted attempt to steal sensitive information, such as account credentials or financial information.

This can be achieved by acquiring personal details about victim such as friends, hometown, employer, location, and online shopping [15]. Attack can be then be an email, or message, disguised as coming from a trust-worthy source. When that email is opened, sensitive information from host device can then be retrieved.

8.2 Sniffing Attacks: Is an attack, that can intercept data by capturing network traffic using a sniffer.

9. Security measures at Perception Layer

There are protective measures for the Perception Layer. These include the following:

9.1 Authentication: Devices need to be authenticated before entering network. Some possible attacks that a simple authentication algorithms can be protected from include brute force attack, collision attack etc.

9.2 Data Privacy: Privacy of data needs to be guaranteed. It can be accomplished by encryption algorithms, which prevents unauthorized access to the sensor data while being collected or forwarded to network layer.

9.3 Data Integrity: To make sure of no data tampering, each device should have error detection systems, such as checksum, parity bit etc [16].

10. Security measures at Network Layer

These are the protective measures for the Network Layer. These include the following:

10.1 Authentication: With proper authentication methods, and point-to-point encryption, illegal access to sensor is prohibited.

10.2 Data Confidentiality: Data confidentiality can be ensured by preventing illegitimate access of nodes network layer. Point-to-point encryption can also be utilized. This makes data confidential.

10.3 Data Integrity: Data integrity can be ensured by using cryptographic hash functions, which ensures that data is not tampered with.

10.4 Data Privacy: Safety control mechanism can monitor the network layer for any intrusion.

11. Security measures at Middleware Layer

These are the protective measures for the Middleware Layer. These include the following:

11.1 Authentication: Similar to authentication process at other layers.

11.2 Intrusion Detection: Intrusion detection techniques provide solutions for various security threats by generating alarm for each individual suspicious activity in the system.

11.3 Data Fragmentation: data is fragmented and stored on various servers. This allows for minimum data exposure in case of a leak.

12. Security measures at Application Layer

These are the protective measures for the Application Layer. These include the following:

12.1 User validation: User needs to be valid to use system. This prevents security breach, that can cause data stealing or unauthorized access.

12.2 Firewalls: Authentication password and encryption method can break. Therefore a firewall should be used to monitor traffic.

12.3 Risk Assessment: Risk assessment detect threats to the system.

References - Cybersecurity Section

[1] Dewey, C. (2014, March 12). 36 ways the Web has changed us. The Washington Post. Retrieved from https://www.washingtonpost.com/news/arts-and-entertainment/wp/2014/03/12/36-ways-the-web-has-changed-us/

[2] U.farooq, M., Waseem, M., Khairi, A., & Mazhar, S. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications, 111(7), 1–6. doi: 10.5120/19547-1280

[3] Al-Sudani, A. R., Zhou, W., Liu, B., Almansoori, A., & Yang, M. (2018). Detecting Unauthorized RFID Tag Carrier for Secure Access Control to a Smart Building . International Journal of Applied Engineering Research, 13(1), 749–760. Retrieved from https://www.ripublication.com/ijaer18/ijaerv13n1_103.pdf

[4] Kamaludin, H., Mahdin, H., & Abawajy, J. H. (2018). Clone tag detection in distributed RFID systems. Plos One, 13(3). doi: 10.1371/journal.pone.0193951

[5] Smiley, S. (2018, March 27). 7 Types of Security Attacks on RFID Systems. Retrieved November 12, 2019, from https://blog.atlasrfidstore.com/7-types-security-attacks-rfid-systems.

[6] Bandyopadhyay, Soma & Sengupta, Munmun & Maiti, Souvik & Dutta, Subhajit. (2011). Role Of Middleware For Internet Of Things: A Study. International Journal of Computer Science & Engineering Survey. 2. 10.5121/ijcses.2011.2307.

[7] M. B. Yassein, M. Q. Shatnawi and D. Al-zoubi, "Application layer protocols for the Internet of Things: A survey," *2016 International Conference on Engineering & MIS (ICEMIS)*, Agadir, 2016, pp. 1-4. doi: 10.1109/ICEMIS.2016.7745303
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7745303&isnumber=7745290

[8] Application Layer Protocol Analysis & the Internet of Things. (n.d.). Retrieved November 12, 2019, from https://study.com/academy/lesson/application-layer-protocol-analysis-the-internet-of-things.html .

[9] Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018, September 13). Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends. Retrieved November 18, 2019, from https://www.hindawi.com/journals/wcmc/2018/5349894/.

[10] HoodaCheck, P., & Hooda, P. (2019, January 10). Sybil Attack. Retrieved November 18, 2019, from https://www.geeksforgeeks.org/sybil-attack/.

[11] Baskar, R., Raja, P. C. K., Joseph, C., & Reji, M. (2017, March). Sinkhole Attack in Wireless Sensor Networks-Performance Analysis and Detection Methods. Retrieved

November 18, 2019, from http://www.indjst.org/index.php/indjst/article/view/90904.

[12] Bhattasali, T., Chaki, R., & Sanyal, S. (2012, March 1). Sleep Deprivation Attack Detection in Wireless Sensor Network. Retrieved November 18, 2019, from https://arxiv.org/abs/1203.0231.

[13] Pirretti, M., Zhu, S., Vijaykrishnan, N., Mcdaniel, P., Kandemir, M., & Brooks, R. (2006). The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense. International Journal of Distributed Sensor Networks, 2(3), 267–287. doi: 10.1080/15501320600642718

[14] Muscat, I. (2019, July 1). What is Code Injection. Retrieved November 18, 2019, from https://www.acunetix.com/blog/articles/code-injection/.

[15] What is Spear-phishing? Defining and Differentiating Spear-phishing from Phishing. (2019, October 24). Retrieved November 18, 2019, from https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing.

[16] Aziz, Tariq, and Ehsan-Ul Haq. “Security Challenges Facing IoT Layers and Its Protective Measures.” International Journal of Computer Applications, vol. 179, no. 27, 2018, pp. 31–35., doi:10.5120/ijca2018916607.

References - Network theory and Topologies

https://onlinelibrary.wiley.com/doi/full/10.1002/9781118766804.wbiect246[1]
J. Colchester, "Network Theory: An Overview", Complexity Labs, Barcelona (2017) [2]
https://www.webopedia.com/quick_ref/topologies.asp [3]
https://www.sciencedirect.com/topics/computer-science/star-topology [4]
https://computernetworktopology.com/what-is-mesh-topology-advantages-disadvantages/ [5]
https://computernetworktopology.com/hybrid-topology/ [6]