Volume XXIV 2021
ISSUE no.1
MBNA Publishing House Constanta 2021

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Attacks on IoT devices for power consumption

To cite this article: S. BÎRLEANU, D. GLAVAN, C. RĂCUCIU and R. MOINESCU, Scientific Bulletin of Naval Academy, Vol. XXIV 2021, pg.111-116.

Submitted: 27.02.2021
Revised: 15.06.2021
Accepted: 22.07.2021

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-21-I1-013

Attacks on IoT devices for power consumption

S Bîrleanu, D Glăvan, C Racuciu, R Moinescu

sorin.birleanu@mta.ro

Abstract: The Internet of Things (IoT) is a network of physical objects that contain electronics embedded in their architecture to communicate and feel the interactions between them or with the external environment. In the coming years, IoT-based technology will provide advanced levels of service and will virtually change the way people live their daily lives. Advances in medicine, engineering, business, agriculture, smart cities and smart homes are just some of the categorical examples in which the IoT is strongly established. In other words, IoT is the connection of any device (from mobile phones, vehicles, appliances and other embedded elements with sensors and actuators) to the Internet, so that these objects can exchange data with each other in a network. It is interesting to note that the difference between IoT and the Internet is the absence of human role.

1. Introduction

Given the rapid development of IoT technology lately, smart homes, smart homes, smart cars have been created that bring extra convenience, but also other benefits in people's lives. To build such smart environments requires the development of mobile phones, home appliances and other things that we use every day. Thus, lately the number of used IoT devices has increased considerably. These devices, which have some limitations, such as power and memory limitations, are most prone to information attacks, causing data loss or other unwanted problems. Thus, in the implementation of an IoT system, security should take the first place in carrying out this process. IoT is the communication between man and devices, this representing the process of sending and receiving messages through verbal or nonverbal means. In digital life, communication means the transfer of data from one place to another through electrical signals. Due to the development of technology lately, we are permanently connected to friends / colleagues / relatives, offering the possibility of communication through text messages, voice, e-mail, so people lead a better life and are always connected to what is happening around them. All these means of communication use the Internet, it connects the entire population offering the possibility of communication at any time and from any location. The main concern at the moment, regarding IoT systems, is to offer a security with a high degree of trust.

2. Internet of things

The Internet is ubiquitous in our lives. From PCs, smartphones, tablets, game consoles to TVs and set of top-boxes. The concept of "Internet of Things" has grown and it is expected that the future belongs to these everyday devices, equipped with sensors. Connected together to work together, to understand what we do and automatically to make our lives easier. Of course, we are able to control them via smartphone or tablet and at some point we will certainly have voice control. IoT includes all devices that can detect aspects of the real world such as: temperature, light, the presence or absence of people or objects, etc. IoT collects this information and acts on it. Smart devices use Wi-Fi internet technology to communicate with each other, or sometimes directly through the Cloud. Ideally, the central access point is owned by the user, via smartphone, tablet or laptop wherever they are. This Internet of Thing concept lends itself to fantastic ideas. Imagine when you go on vacation, your home goes into vacation mode, lighting the house sometimes to give the impression that someone is at home, thus removing

thieves. Today's cars, for example, have different systems to control engine operation, safety elements, communication frames, etc.

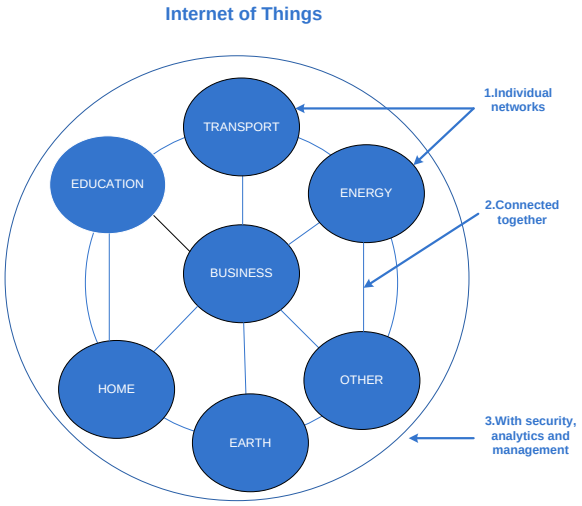

Figure 1 – Internet of Things

IoT protocol stack is not standardized as TCP/IP or OSI protocol suite. Most of the IoT security protocols are designed to operate in multiple layers to provide security. There are different types (3 layers, 5 layers, 7 layers) of IoT architecture and protocol stack. One model is shown in Figure 3:

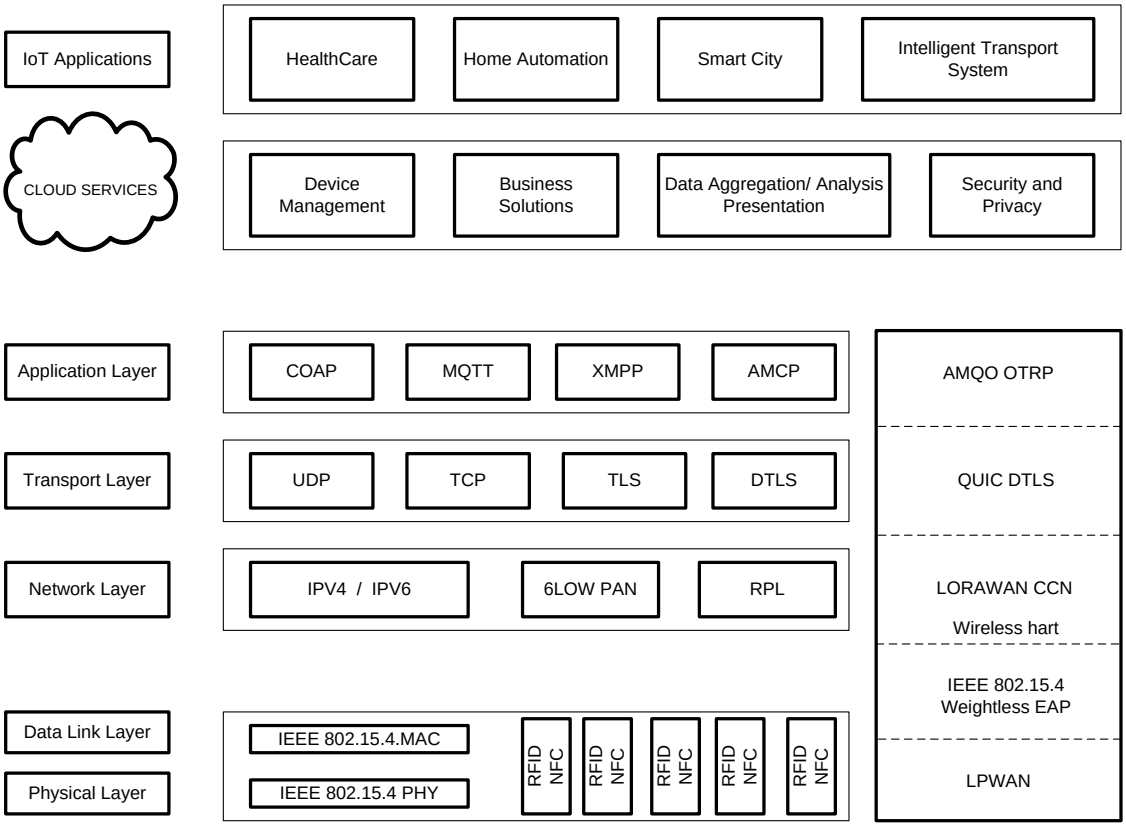

Figure 3 – IoT Architecture and protocol stack [9]

Physical Layer - The perception layer is the physical layer, which has sensors for sensing and gathering information about the environment.. The issues to be considered in physical layer of an IoT network are power, bandwidth and energy consumption. Low-power WAN (LPWAN) is a wireless wide area network technology that interconnects low-bandwidth, battery-powered devices with low bit rates over long ranges. Different LPWAN technologies offer varying levels of security. Most include device or subscriber authentication, network authentication, identity protection, advanced standard encryption (AES), message confidentiality and key provisioning.

Data Link layer - IEEE 802.15.4 is the most commonly used IoT standard for MAC. It defines a frame format, headers including source and destination addresses, and how nodes can communicate with each Other, to provide link layer security. Increasing the transmission power also increases the data rate in wireless communication. The wireless communication protocol used are: Bluetooth Low Energy, Wi-Fi, Zigbee Smart Energy, WirelessHART, Weightless, EAP (Extensible Authentication Protocol).

Network Layer - The network layer of IoT serves the function of data routing and transmission to different IoT hubs and devices over the Internet. Routing Protocol for Low-Power and Lossy Networks (RPL) is distance-vector protocol that can support a variety of datalink protocols. In network layer, security is usually provided by IPv6 over Low power Wireless Personal Area Network (6LoWPAN) in devices with lowpower and computing ability in WSN and internet. CCN (Content concentric Networking) is a protocol used to deliver content as packets and has been designed to deal with scalability, mobility and security.

Transport Layer – Transport Layer focuses on end-to-end communication and provides features such as reliability, congestion avoidance, and guaranteeing that packets will be delivered in the same order that they were sent. QuiC (Quick UDP Internet Connections) protocol provides multiplexed connections over UDP and provides security protection similar to TLS/SSL in order to reduce connection latency. Datagram Transport Layer Security (DTLS) is a communications protocol designed to protect data privacy and preventing eavesdropping and tampering. It is based on the Transport Layer Security (TLS) protocol, which is a protocol that provides security to computer-based communications networks.

Application Layer - Application layer defines all applications that use the IoT technology or in which IoT has deployed. The application layer security issues include user authentication, privacy, access control, middle ware security. Constrained Application Protocol (CoAP) is a specialized web transfer protocol designed to enable simple, constrained devices to join the IoT even through constrained networks with low bandwidth and low availability. AMQP (Advanced Message Queuing Protocol) is a protocol for message oriented middleware that is designed to take care of message queuing routing, reliability and security. MQTT (Message Queuing Telemetry Transport) is a publish-and-subscribe protocol, meaning that instead of communicating with a server, client devices and applications publish and subscribe to topics handled by a broker.

3. Threats and attacks

Following are some of threats and attacks in IoT networks:

• Denial of Service - The attacker sends massive service requests to the IoT device, which cannot handle this massive traffic, which results in delay or blockage of service to the users. It is typically accomplished by flooding the targeted devices or network resources with redundant requests in order to make it impossible or difficult for authentic user to use the devices.

• Eaves dropping - The attacker passively listens to network communications to gain access to private information, such as node identification numbers, routing updates, or application sensitive data.
• MQTT Attack - IoT servers that use MQTT on internet is subjected to attack because of unauthenticated and unencrypted communication. MQTT servers are also vulnerable to SQL injection and cross-side scripting. The MQTT servers used for firmware updates, may be used to update malicious code [8].
• Malware Attack - Malwares attacks target IoT devices authentication and authorization.
• Ransomware - In a ransomware attack, the attacker steal data from any interface gateway or cloud aggregator, gets hold of critical data that is required for day-to-day activity of an organization and demands money in some form to release the data.

One of the most sensitive security threats is DoS attack. Hardware failures and power issues are security issues in the physical layer. Despite this classification, the problems in these layers trigger the security of the entire system.

4. DoS Attack

Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks are a method by which computational resources are made unavailable to their legitimate users. Although the methods by which these attacks are carried out are very varied, these types of attacks are aimed at making a web page or a web service work slowly or not at all. The main targets of DoS attacks are web servers for banking, or Internet name resolution services. These attacks are usually carried out by simple requests, repeated to the target stations until they begin to respond very difficult to legitimate users or are unable to respond at all. DoS attacks are a violation of the acceptable use of resources policies of all Internet service providers. These attacks also violate the laws of most states. These attacks target a variety of targets in different areas:

- Politics;
- Finance;
- Entertainment;
- Social networks.

Most DoS attacks target network bandwidth or connectivity. To deplete bandwidth, the attacker creates a large stream of data on the network so that a legitimate user can no longer use the service provided by the network because its resources become depleted. An attack on connectivity is performed by a large number of requests on a server, so that it will no longer be able to respond to legitimate user requests because its resources will be occupied by the attacker's requests.

A Distributed DoS (DDoS) attack is an attack that uses multiple computers to launch a coordinated DoS attack on one or more targets. Using client / server technology, the attacker is able to significantly enhance the effectiveness of the DoS attack by leveraging the resources of several unwittingly complicit computers, which are used as attack platforms.Some of the most commonly used attacks are Ping of Death, ICMP Flood, UDP flood, Slow-loris, HTTP Flood, SYN Flood, etc.

An attack by exhausting connections is the SYN flooding attack, this is done by sending a SYN message by the attacker to a server, without the attacker completing the third step of the handshake, this occupying part of the server's memory until the connection expires, often after 75 sec. Because these "semi-open" connections occupy OS memory, they limit their number, so the attacker will launch a series of requests to connect to the server, until it reaches this limit, causing any other connection

requests to be rejected. The TCP SYN Flood attack uses TCP three-way handshake. This is presented in the following figure and includes the following steps:

1. The client requests a connection and sends a SYN message to the server.
2. The server sends a synchronization-confirmation message (SYN-ACK) for client confirmation.
3. The client sends the ACK message back to the server and the connection is established.

In such a case, the attacker repeatedly sends SYN packets to each open port on the target system. The server will respond by sending SYN-ACK packets and will wait for the client's ACK message. The attacker does not send an ACK message and the server cannot close the connection during this time. Eventually, the server connection table will be full and unable to provide services to authorized users. ICMP Flood Attack is an attack in which the attacker tries to overwhelm a targeted device with ICMP echo request packets, causing the target to become inaccessible to normal traffic. When attack traffic comes from multiple devices, the attack becomes a DDoS or distributed denial of service attack.

5. Monitoring an attack

A series of tests were performed on certain types of attacks on the systems, and the parameters of the targeted energy consumption system were analyzed. In the first part, an ICMP Flooding attack was carried out on an Android device. Once the attack was triggered, it was found that the processor load increased to 91-93% and a data transmission with a speed of 5Mb / sec.

In the case of the SYN Flooding attack on the same device, the processor load increased to 85-88%. A significant difference between the two attacks is the use of the network, SYN Flooding having a different value of the transmitted and received data. In this case, a data reception was found with a speed of approximately 21 Mb / sec.

In the case of an ICMP Flooding attack performed on Windows, it is found that the payload of the processor increases to 80, and the data transmission is performed at a speed of approximately 75 Mb / s. Regarding the SYN Flooding attack, a payload of 85% was observed, and the data transmission speed is 200 Mb / sec.

During these attacks, there was a consumption of 55W with SYN Flooding on Windows, respectively 51W with ICMP Flooding. In the case of Android devices, a much higher power consumption of about 61W was obtained.

6. Conclusion

This paper presents the behavior of an IoT system, which depends on the types of DoS attacks that are performed (which operating systems consume more / less resources). A comparison of attacks on Windows and Android devices is shown and processor and network loads were analyzed. In terms of power consumption, it is found that Windows is more efficient than Android. The main problem of IoT devices is power consumption, IoT devices cannot be used in case of attacks. As a future work, it is intended to extend the study to other operating systems as well as the study of other types of information attacks.

REFERENCES

[1] ITU Strategy and Policy Unit (SPU). The internet of things. ITU Internet Reports 2005: The Internet of Things, 7th edition

[2] D. Evans. 2011 *The internet of things: How the next evolution of the internet is changing everything*

[3] S. A. Kumar and H. Srivastava 2016 *Security in internet of things: Challenges, solutions and future directions*
[4] A. Srivastava, A. Tyagi, Anupama Sharma, and B B Gupta 2011 *A Recent Survey on DDoS Attacks and Defense Mechanisms*
[5] Yan-Ling Hwang, Wei-Tai Cai, Chia-Hao Lee, and KaiWei Chang 2015 *Trap: A three-way handshake server*, 2015.
[6] Asmaa Munshi, Nouf Ayadh Alqarni 2020 *DDOS Attack on IOT Devices*
[7] Congyingzi Zhang , Robert Green 2014 *Communication Security in Internet of Thing: Preventive Measure and Avoid DDoS Attack Over IoT Network*
[8] Higginis KJ 2017 IoT devices plagued by lesser known security hole. https://www.darkreading.com/cloud/iot-devices-plagued-by-lesser-known-security-hole-/d/d-id/1329320
[9] J. Cynthia H. Parveen Sultana M. N. Saroja J. Senthil 2018 Security Protocols for IoT, https://www.researchgate.net/publication/328078416_Security_Protocols_for_IoT