Volume: 5, Issue: 3
Page: 101-115
2021

International Journal of
Science and Business
Journal homepage: ijsab.com/ijsb

IJSAB International

Security Issues and Vulnerability of IoT Devices

Kurdistan Ali & Shavan Askar

Abstract:

The principle of linking intelligent device to the internet is taken out in the internet of things. This model facilitates the relation across the Cloud between the intellectual real items and the separate contact parties, such as the servers, the cellular devices. Internet of things is entering in all aspects of life including home, industries, medical care, cars, sensors, but the main and very important open challenges in this area is security issues. IoT security is very weak this is due to heterogeneous devices used in this field. Therefore, the expansion of security weak points will bring serious dangers to users' security, and property. This paper discuss the security aspects in the IoT communication protocols and Security threats of multiple layers dependent on the security concepts of data confidently, data integrity and privacy, it also discusses and investigates the main IoT protocols that used to communicate between IoT based nodes and sensors. Furthermore, vulnerability in different protocols are reviewed and compared.

IJSB
Literature review
Accepted 1 February 2021
Published 3 February 2021
DOI: 10.5281/zenodo.4497707

Keywords: *Internet of Things, Security, Privacy, Vulnerabilities, ZigBee, LoRaWaN, 6LoWPAN*

About Author (s)

Kurdistan Ali, Information System Engineering, Erbil Polytechnic University, Erbil, Iraq. Email: Kurdistan.hamaali@epu.edu.iq.
Shavan Askar (Corresponding Author), Assistant Professor, Erbil Polytechnic University, Erbil, Iraq. Email: shavan.askar@epu.edu.iq.

1. Introduction

The most popular and practical online system is the Internet of Things. It links to the Internet with different sensors and controllers and helps to achieve direct communication between individuals and things. The main future of the Internet appears to be that. The quantity and variety of devices have grown quickly, With the strength of the IoT industry, particularly in previous seasons, (Yu et al., 2020). The IoT devices share a similar architectural style. Under this framework, each layer (edge, middleware, and application) carries its collection of security risks that must be taken into account. In addition, Large combinations in development tools make IoT protection a difficult issue to address (Zhang et al., 2014).For this purpose, it will help their adoption and future product iterations to create a well-defined security model for IoT devices (Williams et al., 2017). IoT, like more vulnerabilities and security threats, presents pressing security challenges. It also need new and smarter IoT security approaches, in particular approaches capable of handling complex, unpredictable and often asymmetric threats on a scale (Roukounaki et al., 2019). In addition, interconnected devices have a direct effect on the lives of users, new technologies and protocols require a well-defined classification of security threats and a proper security structure that can mitigate security challenges in terms of privacy, data integrity, and IoT availability (Andrea, Chrysostomou, & Hadjichristofi, 2015).Cyber-attacks targeting it are growing as IoT devices become popular. And these attacks, both at home and around the world, create business and operation delays, intelligence leaks, and financial damage, disrupting economic growth and the safety and security of regular activities. Cyber-attacks on IoT devices result in financial and social disruption, social awareness with the need for IoT device security will further expand. A massive amount of data creates by The Internet of Things is a big challenge to be handled, other obstacle includes the limitation of the current network structure that are incapable to handle real-time sensitive applications using IoT, therefore Software Defined Networking is expected to be a suitable network infrastructure for such applications (Askar, 2017; Fizi & Askar, 2016; Askar, 2016; Keti & Askar, 2015). This paper's contents will be organized as follows: section 2 presents brief information about security aspects, section 3 presents an IoT layers and security theaters, section 4 Security mechanisms for IoT services, section 4 describes IoT protocols and communication, and finally, section 5 provides a description and ideas for possible directions for research about IoT protocols.

2. Security Aspects

With growing IOT-based systems, there is a need to introduce its security concepts. To achieve this goal, we have to know the basics of IoT and its implementation on the advanced network technologies and applied it within the available networks (e.g. wireless sensors, node-based sensor networks) Therefore, using these systems, all security issues and threats of each communication technologies are transferred by definition into the IoT system. In addition, it is possible to establish new security risks resulting from the coexistence and interaction of different systems and open IoT security protocols. The key IoT security goal is to protect data, as confidential user information can also be found in the data obtained from physical devices (Andrea et al., 2015; Sulaiman & Askar, 2015; Fares & Askar, 2016).

2.1 Confidently

Data confidentiality is characterized as a major principle for IoT solutions that are especially important in the business area. Thus it suggests that existing data confidentiality techniques might not be applicable because of two key constraints: the volume of data produced and the usefulness of complex data sources in managing access to data. The authors in (Miorandi et al., 2012) Appropriate identity management is often listed as an important component in guaranteeing data confidentiality. Most IoT devices need to be listed as secure to deal with details. The confidentiality can be achieved by cryptographic algorithms. Before implementing, existing various modulation algorithms should be evaluated based on the IoT system's operation, functionality and criticality (Chowdhury, & Noll, 2011). It reflects the quality of research on confidentiality and the significant issues involved with it. It also shows the value of authenticity and the reliability of the foundations of data along with (Suo, Wan, Zou, & Liu, 2012). The confidentiality required for sensors is not as critical as reliability and authenticity as the hacker can achieve the same values only by putting a fake sensor next to the authorized one note that the key sensitivity to confidentiality exists in contact, storage, identification and authentication in the sense of the IoT (Mendez, Papapanagiotou, & Yang, 2017). Confidentiality depends on the ability to guarantee the personal data by ensuring only the enabled users with a protected contact. The data can be viewed only by an authorized user. A data encryption system can achieve confidentiality if each part of information is converted into cipher text and followed by a two-step authentication procedure, where components allow access only if all equipment and identity verification are passes via the authentication process in which the user is immediately accessible. The sensors ensure that sensor network nodes do not connect to adjacent nodes on the Internet of Things and tags do not send their data to unrecognized readers (Swamy, Jadhav, & Kulkarni, 2017).

2.2 Integrity

Modifiability and error resistance due to physical faults is the key objective of IoT integrity. Sensor networks, like RFID, often face other problems that limit their ability to solve credibility issues, because many of their components spend most of their time without being involved. The data can either be changed by attackers when it is stored in the node or as it moves across the network. Protections for reading and writing and also authentication mechanisms are standard solutions. Password-based implementations that take into consideration in security, like as flaws relating to password duration and random, often maintain data integrity. Also, because of the limited resources available, the resources used in specific IoT systems don't support traditional cryptographic approaches. In addition to different contexts, IoT integrity needs to be secured, like as quality service. Restrictive operating systems, such as Multi Level Protection (MLS), help machines to prevent malicious code manipulation running with high privileges. However, MLS methods have not been widely implemented, since they can be considered costly and also incompatible with other IoT applications in some situations. Other tools for preserving integrity use values stored publicly to prevent compromise (Fongen, 2012). For integrity purposes, hardware mechanisms have often been suggested by the use of Reliable System , a danger strategy is defined (Mendez et al., 2017).

2.3 Privacy

Data protection requires interconnected machine self-aware actions, security, resistance to heterogeneity, powerful encryption techniques; protected cloud storage, management control of data, and also security policies (Roman, Najera, & Lopez, 2011).

2.4 Self-organization

Self-organization helps the IoT framework to execute the particular role it is meant to fulfill while providing a structure for the sharing between resources in a way that can benefit a number of vertical utilize cases (Hu & Zhu, 2012). It also offers functionality for intelligent IoT applications, since they are supposed to be part of multiple impartial functional networks. In these cases, there is the interaction of autonomous systems which can connect and reply according to their internal state. Under any unforeseen scenario, redundant devices can be easily integrated into the IoT self-organization model to function as a system crash. In a case where one is losing, this will re-task a computer. By increasing its usability, affordability, and capabilities, this self-organizing feature can result in the durability and manageability of IoT products. Optimum network capability, scalable running, service quality (QoS), scalability, reliable and reactive delivery of services, and IoT devices can work together to share resources as they coordinate themselves to promote energy use. This will also lead to lowered demand for data transmission (Athreya & Tague, 2013).

2.5 Access control

The designed access controls of the operating system, automatic or role-based, have the advantage of controlling the rights for application modules and apps so that they only access certain services allocated to them. Access control means that threat has limited access to all areas of the device in the event of an attack. Access control structures based on computers are close to access control schemes based on networks, such as Microsoft Active Directory. If anyone attempts to intercept corporate keys and gains access to the network, access to those compromised data is limited to certain parts of the network that are authorized by the keys (Jurcut et al., 2020).

3. Security Threats

The IoT framework has three layers, namely the edge layer, the network layer and the application layer. Internet support technologies (such as network processing, computer technology, middleware technology, etc.) are used by certain applications as the processing layer.

3.1 Edge layer

The IoT was introduced with the purpose of relating the digital and tangible terms to each other. Designers want to join millions of devices connected, and they can be strong enough to make selects. The IoT edge layer is consist of smart devices which may have sensor, actuators and a microcontroller which have high processing power and capability of connectivity with the networks through which it can connect to the application. The unit will allow us to gather data from the area with all these features. Because all the data that we have to process is gathered by this layer, we need to take care of data protection and also ensure that this is accurate information from sensors. Devices will be connecting to the network with the help of Bluetooth, GPRS, Wi-Fi and Zigbee (Arshad et al., 2020). This layer contains different kinds of sensors that can be physically attacked at one spot for a long time, such as RFID, ZigBee, and WSN. The most frequent attacks are hardware attacks on the edge layer. Different IoT devices, such as smart technology, video games, collect information about us and some hackers can exchange or access this information for illegal reasons. Tampering Node and Hardware Jamming are general attacks on the edge layer, replacing or destroying the node in the first attacker to gain access to the node by collecting the cryptographic keys while the attacker can substitute a section of the hardware node in the latter and can gain routing table by catching the gateway node (Rao & Haq, 2018; Askar et al., 2011; Al Majeed et al., 2014). Other types of attack are injecting a noise in data and denial attack where the data containing incorrect or inaccurate information that happens during transmission or attacking a programmed file is used to fail the control of the node and decrease the battery life.

3.2 Network layer

This layer is included in the transfer of data from the edge layer through the network. The thread for this layer is enhanced because data from various heterogeneous devices is received by this layer.

3.2.1 Man-in-Middle

In this threat, the attacker is not there to appear directly on a network device, they use the IoT authentication mechanism to communicate with the two sensor nodes to get all the sensitive data (Rao & Haq, 2018).

3.2.2 Router Gateway

The connection between the sensors and the internet gateway is disconnected or fake information can be injected between node sensors and routers using DoS or routing table attacks.

3.2.3 Sniffing

All information from the network and sensors can be obtained during communication between the nodes using a simple sniffer request (Arshad).

3.3 Application layer

Due to vulnerability problems, the program can be hacked as well as closed down effortlessly. In the application software code that activates the application to break down, the malevolent attack may be due to the virus. Applications are often abortive in taking authenticated applications for which they are intended to inaccurately execute or offer the service. In the application layer, the security risk of data delaying results in an increase if the attacker knows the vulnerabilities of the application. Malevolent code attacks and helpless software where a worm will be detected and applied to internet-enabled nodes such as security cameras and air conditioning or car Wi-Fi that will be used to overcome the car's steering wheel are some general threats to this layer. Another attack known as phishing is spoofing the user's confirmation credential and the attackers will find a weak point of the end nodes through a reverse engineering model and divide it into different steps to perform vulnerabilities step by step.

4. Main Security Mechanisms For IoT Services

4.1 Cryptography

Securing data such as user identities, bank credit card numbers, etc. is referred to as Cryptography, using cryptographic algorithms to relay these messages across the network. In network defense, several encryption algorithms are used. Symmetric, public-key, and Cryptographic protocols are split into three basic groups. They are categorized as: Symmetric algorithms where one key is used to encrypt and decrypt data that use two keys, i.e. private and public keys, Depending on the amount of keys that are used for encryption and decryption. For encryption, the public key is used, and the private key is used for decryption (Surendran, Nassef, & Beheshti, 2018). Rivest-Shamir-Adelman, Data Encryption Standard, Advanced Encryption Standard are some of the essential cryptographic algorithms accessible. While these algorithms are important for information technology security, a large range of computational resources, such as time for the CPU, storage and batteries energy, are consumed. Based on the key size used, the strength of symmetric key encryption varies. In addition, Unclassified information is protected from attackers by using the DES algorithm that uses the same key for encryption and decryption operations (Pawar & Ghumbre, 2016).

4.2 Lightweight cryptography

Lightweight block ciphers work with a transformation defined by a symmetric key on fixed-length bits. This flexible primitive uses more complex operations and is implemented using the substitution and permutation networks (SPN). SPN includes a number of rounds of substitute boxes and permutation boxes generating a network to create a cipher text block, which then applies a plaintext block and key to mathematical operations. The advantage of the symmetric nature of the Cipher text is that the processes of encryption and decryption are almost equivalent, divided by the opposite of the key schedule. The nearly halved size of the requisite code or circuitry may then be comfortably added. The very low latency of lightweight block ciphers (Gebotys, 2006). Based on the design of the restrictions they begin to solve, such as length, speed or energy, lightweight blocks may usually be designed for various things. PRESENT, KLEIN and ZORRO are three of these light-weight block ciphers. PRESENT was already developed and applied successfully in hardware that can be designed to have a very low number of gates (McCann, Eder, & Oswald, 2015).

4.3 Hardware security

There are several important limitations to hardware-based security primitives and protocols. Three are dominant among them. It's just that Silicon Physical Unlovable Functions (PUFs) appeared as a successful basic hardware security with a growth potential for Radio Frequency Identification (RFID) tags, safety communication protocols, Core network defense, collection of cryptographic key, user authentication of applications, before the advent of the public physical feature (Huang & Wang, 2019). The procedure has very limited hardware for processing and no operational expenses for slowdown and energy. The key idea would be to include only a limited subset of concerns, but it is dependable under a wide range of circumstances. While the multitude of issues used is drastically diminished from the initial amount of challenges, the number of items used for problems is still increasing in their cardinality. This method extends many different (PUFs) structures. Primitive optical (PUFs) hardware protection is the second. It is an electronic signal with very small gate amounts, high throughput, and super energy requirements, but it is initialized using stable analog (PUFs). The protected and trusted flow of information, the removal of side channels and the latency of just a few gate numbers of public key security protocols can therefore be directly combined with standard digital designs and facilitated.

4.4 Random number generator

In general, A black box that takes input and generates incoming messages within a specified range is a random number generator. Pseudo-RNGs and True-RNGs are classified into two main groups (Wallace et al., 2016). Pseudo-RNGs are easy to execute and suitable for many applications, and a TRNG is often required, particularly for super accurate systems. The reason for this is that PRNG was built from a computing algorithm which has testable properties. It also destroys the random number it generates since the code behind the PRNG is broken (Randa, Samie, & Jennions, 2020). A True-RNG, from the other side, a concrete structure that has inherent randomness is used to produce a RNG that can be extracted. This refers to non properties in the case of TRNG. However, these systems have limited randomness and can be easily dominated, achieve data security against cyber-attacks. Their unpredictability makes TRNG based on hardware more stable than PRNG based on software (Carboni et al., 2018).

5. IoT-Based Security Communication And Protocols

5.1 ZigBee

ZigBee is a wireless and based on the IEEE 802.15.4 standard. It was launched in 2004 by the ZigBee Alliance and in the form of (WPAN). Primarily defined by very low powered demands and lower utilization speeds (Dementyev, Hodges, Taylor, & Smith, 2013). As shown in figure 1. The protocol can reduce the battery replacement speed and has a transfer rate of up to 25000 bps, with a range of up to 1 kilometer. In the ZigBee protocol, safety assumes a key role. The Advanced Encryption Standard (AES) is the encryption algorithm used in ZigBee. Such a highly stable and accurate algorithm ensures the secrecy and reliability of wireless communications(Vaccari et al., 2017). Two separate security models are given by ZigBee: standard security model, implemented simple security model due to its vulnerability to threats, and High Security, each of which is used because it guarantees better security during communications. If data is unencrypted on a ZigBee network, a hacker can control all network information and can also sniff/capture packets that have been transmitted. Instead, if communication is protected, an unauthorized attacker may only execute attacks that do not enable network access, It is very hard to observe the network key supported by ZigBee and decipher the messages sent, including access denial or bumping (Vaccari et al., 2017). The AES 128-bit encryption algorithm is implemented by ZigBee security, which also provides security resources such Key transmission, structure security and device control, as key generation. Each layer responsible for uniqueness frame is responsible for automatically swapping the key for each input and output node, and without the need to decrypt and encrypt, data is transmitted at each step. Security features provided by the ZigBee standards will be covered, including in the sense of secure sets and strong encryption. (Dini & Tiloca, 2010).

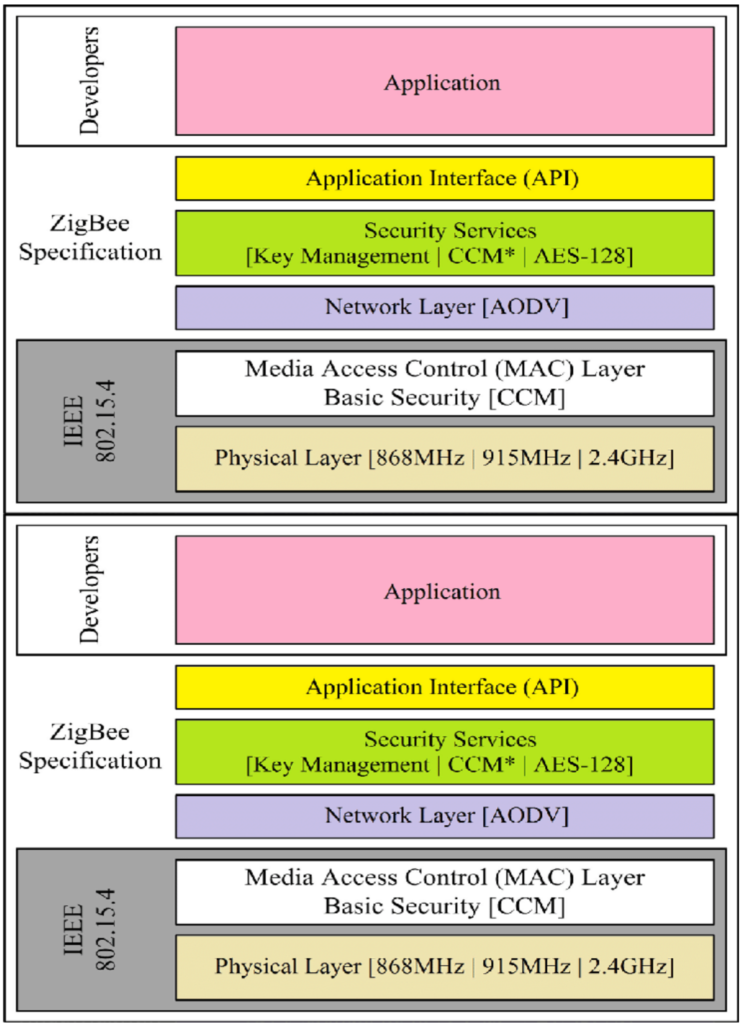
Developers
Application
ZigBee Specification
Application Interface (API)
Security Services [Key Management | CCM* | AES-128]
Network Layer [AODV]
IEEE 802.15.4
Media Access Control (MAC) Layer Basic Security [CCM]
Physical Layer [868MHz | 915MHz | 2.4GHz]
Developers
Application
ZigBee Specification
Application Interface (API)
Security Services [Key Management | CCM* | AES-128]
Network Layer [AODV]
IEEE 802.15.4
Media Access Control (MAC) Layer Basic Security [CCM]
Physical Layer [868MHz | 915MHz | 2.4GHz]

Figure 1 ZigBee stack (Charan, Usmani, Paulus, & Saeed, 2016)

ZigBee Networks are subject to multiple kinds of attacks. In keeping with the safety criteria of ZigBee Networks (Grover & Sharma, 2016), This attacks can be grouped into five kinds of attacks:

Eavesdropping: An external attack in which an hacker may attempt to passively overhear or listen to the conversation on the network and take the data.

Denial of Service: That arise when hackers use a PC to send movements with the ultimate aim of interfering with the network's radio frequencies (2.4 GHz). This kind of DoS can also be found on the data link layer where, for example, IEEE 802.15.4 or ZigBee, have a particular mission to interrupt the communication protocols.

Node Compromise: It is a sort of act by which an attacker catches and exploits or reprogrammed a valid node in the network.

Sinkhole and Wormhole: It is a situation in which the malware network device by spreading fake routing data gathered packets to it, which in turn upsets the network's routing operation. In a Wormhole Attack, an attacker gathers packets for one network connection, passes them to another place of the network, and then replays them into a network to generate confusion about the routing, forwarding and other significant actions of the node.

Physical Attack: The attacker's ability to obtain physical access to a network device.

5.2 Bluetooth low energy

Unlike standard Bluetooth, BLE is designed for sensor networks with a small data rate of up to 1 Mbit/s, with an emphasis on power efficiency, it was released and BLE is conflicting with Bluetooth Classic. Both run in the 2.4 GHz frequency range with a separate range of wavelength channels. The software is supported and distributed by the Bluetooth SIG (Lonzetta et al., 2018). BLE specifies a set of software features that can be applied by devices. A model is a collection of services that a system offers and, including its purpose, each machine may introduce a variety of modules. BLE has so far been restricted to linking only two devices. The Mesh interface was implemented by Bluetooth SIG, making multi-to-many connectivity. Encrypted data is optional in BLE and is performed during the connected components' matching process. Exchanging the (AES) encryption key is a critical part of protecting the connection. The joining method is a key contributor to Bluetooth security problems(Cope, Campbell, & Hayajneh, 2017). During various phases of the connection process, attacks can be carried out, both before the matching process is finished and after the devices are matched. Pairing in BLE is not considered stable up to version 4.1, since there is no eavesdropping security that can lead to key loss. The risk of requiring linking devices to regenerate their keys makes this much more risky. In addition, The common keys will have a negotiable length of almost as 7 bytes and the amount of authentication issues is endless (Cope et al., 2017). Encryption and other authentication enhancements remain optional except with the changes in later releases and are not introduced by many vendors. On the application layer, some suppliers impose encryption, but application vulnerabilities or poor security against particular threats are very popular (Seri & Vishnepolsky, 2017). Finally, while all the encryption keys of the BLE standard are used correctly by the vendor, it does not ensure quality. The flexibility of the design which contributes to defects in security created by a procedure, including big limitations such as arbitrary code execution (Krejčí, Hujňák, & Švepeš, 2017).

Some attacks on BLE are shown below:

5.2.1 MAC Spoofing

The attack is carried out before encryption is formed and when connection keys are created during the creation. By producing link-keys, devices are able to authenticate each other. Attackers will replicate another user during the attack (Luckett, McDonald, & Glisson, 2017). The attacker is also capable of terminating communications or intercepting/modifying data by using special methods.

5.2.2 Man-in-the-Middle

During the attack, the instructions are conveyed mistakenly between both the computers. Without exchanging the hidden keys, this allows protection (Cao et al., 2016). The user assumes that the matching was successful, because the two computers are matched with the hacker.

5.3 LoRaWAN

The Low-Power, Wide-Area Networks are applied to relate the Internet of Things with billions of devices. By having a long battery life, Narrow and broadband networks enable LPWAN developments. The broad range of low-cost equipment and connectivity. The Long Scale Large-Area Network (LoRaWAN) is an integrated LPWAN with a wide range and power and low cost and energy usage. There is a stars technology for LoRaWAN networks, as shown in Figure 2. Where edges are send messages to transmitting these messages to a main controller. Two security layers are included in the LoRaWAN standard: first for the network and second for the program (Dönmez & Nigussie, 2018). It needs to be customized and enabled when an edge is connected to the LoRaWAN network. The edge can be activated either through Over The-Air-Activation or through Personalization Activation. When the system is installed or reset. OTAA requires computers to perform a joint process before sending any network data messages. For that one, before the joining process, the end system must be modified. For a particular end-device, Application key is 128 key. That key is delegated by the user to the device and is derived from the implementation root key that is handled by the end user. When the edge device enters a LoRaWAN network via OTAA, the computer stores the Device Address , the Application Identifier , the Network Session Key, and the Application Session Key after activation (Aras, Ramachandran, Lawrence, & Hughes, 2017). An end-node and server use the network session key to calculate and validate the message integrity code (MIC). The end-device and the server use it to encode and decode the payload of data messages unique to the program. It can also be used to compute and validate a MIC at the application stage. For verifying application data, AppKey is used. Computer has its own unique set of session keys, so it does not affect the safe communication of other devices within the LoRaWAN network if a device is compromised. LoRa is a physical layer of Spread Spectrum modulation schemes used in LoRaWAN (Dönmez & Nigussie, 2018). Via a non-LoRaWAN network with higher throughput, usually Ethernet, Wi-Fi, 3G/4G or satellite, the gateway forwards the LoRaWAN frames from the end-devices to a central network server. In addition, the gateway controls traffic in both directions as well. The network server is responsible for interpreting edge sent packets and transmitting information to the application for action. LoRaWAN specifies three distinct edge device classes with various capabilities. (Vatcharatiansakul, Tuwanut, & Pornavalai, 2017):

Class A: After the frame is transmitted, the edge devices that use ALOHA control for multiple access transmissions check for a reply during the two transmitter windows after the frame is transmitted, meaning that the mechanism can be disabled to save electrical power for long periods. Lowest power usage, high latency of unicast user manual.

Class B: The edge devices are configured for systems needing higher transmitter traffic. For external transmitter traffic without uplink transmissions, a Class B recipient routinely uses hello message through the windows clock synchronization gateway. It is the low latency transmitting class of unicast and multicast messages for medium power use.

Class C: When they submit a frame, the edge devices continuously feel the absence of the channel, so they assume to be connected to a power source. That is the large capacity usage without unicast and multicast latency messages being began sending. Some attacks on LoRaWAN are described below:

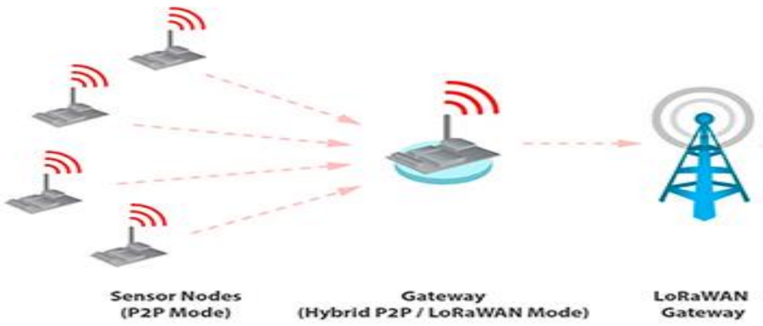

Figure 2 LoRaWAN star-of-stars topology

5.3.1 Wormhole Attacks

Through using off shelf hardware, devices in the LoRaWAN network can be jammed. This can be executed against the LoRaWAN network in combination with a replay attack. For this method of attack, one compromised computer gathers data through one device and passes them to another remotely located device to retrieve the captured packet. This can be effectively initiated by malicious actors (Aras et al., 2017).

5.3.2 Replay Attacks

A replay attack is intrusions on the authentication process, re-sending or transferring the unauthorized entity's exact file transfers. This attack is touch messages or a local network to trick the system or module. The organization should know the contact frequencies and channels for sniffing data from communication between devices in order to carry out an attack on wireless networks. In LoRaWAN, communications between end devices and gateways cannot be decrypted without an AppSKey, as it encrypts the entire content of the LoRaWAN document. Furthermore, as the MIC test will fail to interfere with the results, it is not possible to do it without NwkSKey. While the malicious will send back the message successively, using frame counters specified in LoRaWAN specifications, these messages or attacks can be detected and discarded (Aras et al., 2017).

5.3.3 Bit Flipping Attack Analysis

In a LoRaWAN network, another attack that can be used is bit-flipping. It is entails altering unique parts of cipher text to shift data without first needing to decode it. Since devices utilize AES in CTR (Counter) mode in a LoRaWAN environment, this causes a bit flipping attack to be carried out as the CTR mode clearly executes an XOR logical operation for plaintext encryption (Ingham, Marchang, & Bhowmik, 2020).

5.4 6LowPAN

A LoWPAN is a group of small devices that connect via a low-power wireless standard, with finite resources in energy, memory, throughput, power computing. It forms a wireless sensor network with up to 250kbits/second of available throughput (Hennebert & Dos Santos, 2014)**.**The Internet Protocol (IP) could be optimized for low-power, low-bandwidth and low-cost networks communicating through the IEEE 802.15.4 specification in order to allow those networks to be connected to the Internet. The IETF modular 6LoWPAN adaptation layer achieves the suitability of IPv6. LoWPAN follows both star and peer-to-peer topology, but due to unknown radio frequency, mobility and battery drainage, the topology can be modified periodically. Figure 3 the variance between 6LoWPAN's protocol stacks and a standard IP network is shown. IP is really the only protocol in the standard model often used connect various protocols to several upper layer protocols from both the data link and physical layer. However, 6LoWPAN uses the 6LoWPAN stack to connect its WSNs to the Internet, a mix of the LoWPAN adaptation layer and IPv6. The 6LoWPAN data link and physical layer use protocols defined for the sensors while the transport layer typically does not use the Transmission Control Protocol for efficiency, reliability and complexity reasons (Le, Loo, Lasebae, Aiash, & Luo, 2012). Whether per hop between two adjacent devices in 6LoWPANs between source and destination nodes, protection will be required. In particular, edge communication between 6LoWPAN sensor devices and other external or Internet organizations would entail adequate protection protocols for the Iot devices, maintaining the secrecy of the data transmitted.

Some common attacks on 6LoWPAN are described below:

5.4.1 Black hole

The attacker node loses all data packets quietly in the Black Hole attack, close to a hole that draws in everything. In this manner, all network routing packets via that node are lost (Pongle & Chavan, 2015).

5.4.2 Fragmentation Attack

The attacker will insert fragments in the fragmentation chain in this attack since there is no authentication system on the receiver side to verify that the fragment obtained is not a spoofed or duplicated fragment. (Hummen et al., 2013).

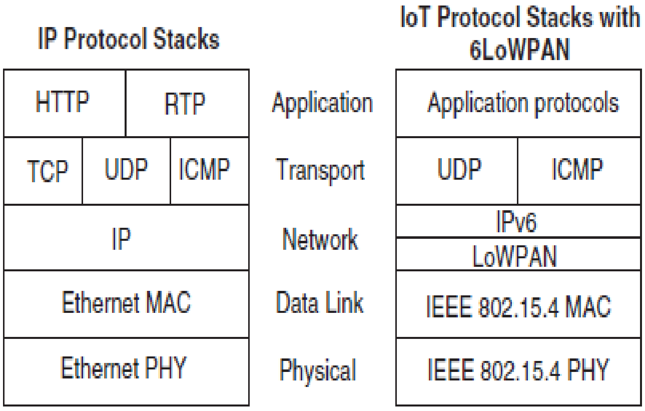

Figure 3 differences between IP protocols stack and 6LoWPAN protocol stack (Le et al., 2012)

6. Discussion

The vulnerabilities of the main security protocols and their suggested solutions in IoT based sensors can be summarized in the following paragraphs;

Four-byte message integrity code (MIC) is used by LoRaWan to protect against malicious, However LoRaWan uses 128 AES key in its CMAC mode to calculate the key but attackers without knowing the key can forge any packets by brute forcing MIC, the mentioned weak point should be well concerned while using this kind of protocol. In 6LoWPAN network every client that has access to the IoT-based sensors, this will raise a threat to user authentication and authorization. The vulnerabilities of this network are during the data transmission between end-users and sensors. The robust authentication should be implemented which avoids any breaks to network integrity and user identity. BLE have no user authentication in its implementation and there is no end to end safety at all. The application programmer should add additional user and application level security which leads lots of work and time consuming however it's the only solution. The main weakness is the key that is used to secure the link which can easily be modified by the adversaries, Therefore the encryption and decryption of the key at each layer have to be well secured during communication.

Finally, ZigBee is one of the protocols that are well received in IoT network community this is due to low power transmission and preserving lots of energy. Practically ZigBee security has many threats which are raised during setup and pairing. During this stage a small signal added with noise will be send to the pairing channel that the failure of the communication. With the use of a Network Key used by all devices, a ZigBee network can be protected to encrypt all network frames and avoid unwanted access and use of the ZigBee network by invalid devices.

7. Conclusion

As technology continues to advance, the number of devices that uses internet is increased which is known of internet of things, this includes the basic device such as lamp to huge machinery and industries such as robotics, sensors, smart traffic light and near intelligent computers. Despite of fast and vast growing in this area it faces the main issue which is the security of the devices and users. Because of the security vulnerabilities will bring serious dangers to users' security and property this paper discusses the main challenges and solution in this field. This paper discusses and examines the main IoT protocols that used to communicate between IoT based devices and their vulnerabilities and weaknesses to the attackers. Starting from LoRaWan which uses 128 AES key in C-Media Access Control mode and 6LWPAN which implements authentication and authorization between the clients during the transmission, ending with BLE and Zigbee, the first one the programmer should be aware to authenticate the users in each stage while the latter one works like Bluetooth by applying pairing technique between clients. Finally, after reviewing and comparing the protocols, vulnerabilities of each protocol is summarized as mentioned in discussion section with LoRaWan the key can easily be calculated by attackers and 6LoWPAN need advanced authentication of user identity during implementation. Zigbee uses low energy during transmission that is why it is usually used in this area but it lacks the security issues during setting up the devices. BLE links can easily be broken by attackers so the encrypting and decryption in each layer have to be secured during the transmission.

References

Al Majeed, S., Askar, S., Fleury, M. (2014). H.265 Codec over 4G Networks for Telemedicine System Application. UKSim-AMSS 16th International Conference on Computer Modelling and Simulation (UK), Cambridge (pp. 292-297), doi: 10.1109/UKSim.2014.59.

Alam, S., Chowdhury, M. M., & Noll, J. J. W. P. C. (2011). Interoperability of security-enabled internet of things. 61(3), 567-586.

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). Internet of Things: Security vulnerabilities and challenges. Paper presented at the 2015 IEEE Symposium on Computers and Communication (ISCC).

Aras, E., Ramachandran, G. S., Lawrence, P., & Hughes, D. (2017). Exploring the security vulnerabilities of LoRa. Paper presented at the 2017 3rd IEEE International Conference on Cybernetics (CYBCONF).

Arshad, M. J. Evaluating Security Threats for each Layers of IoT System.

Askar S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Evaluation of Classified Cloning Scheme with self-similar traffic. 3rd Computer Science and Electronic Engineering Conference (CEEC), Colchester, 2011, pp. 23-28, doi: 10.1109/CEEC.2011.5995819.

Askar, S. (2016). Adaptive Load Balancing Scheme For Data Center Networks Using Software Defined Network. Journal of University of Zakho, Vol. 4(A), No.2, Pp 275-286,

Askar, S. (2017). SDN-Based Load Balancing Scheme for Fat-Tree Data Center Networks. Al-Nahrain Journal for Engineering Sciences (NJES), Vol.20, No.5, pp.1047-1056

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Service differentiation for video applications over OBS networks. 1*6th European Conference on Networks and Optical Communications*, Newcastle-Upon-Tyne, pp. 200-203.

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). A novel ingress node design for video streaming over optical burst switching networks. Optics Express, Vol. 19 (26), pp. 191-194

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Adaptive Classified Cloning and Aggregation Technique for Delay and Loss sensitive Applications in OBS Networks. in Optical Fiber Communication Conference/National Fiber Optic Engineers Conference 2011, OSA Technical Digest (CD) (Optical Society of America, 2011), paper OThR4.

Athreya, A. P., & Tague, P. (2013). Network self-organization in the Internet of Things. Paper presented at the 2013 IEEE international workshop of internet-of-things networking and control (IoT-NC).

Cao, X., Shila, D. M., Cheng, Y., Yang, Z., Zhou, Y., & Chen, J. J. I. I. o. T. J. (2016). Ghost-in-zigbee: Energy depletion attack on zigbee-based wireless networks. 3(5), 816-829.

Carboni, R., Chen, W., Siddik, M., Harms, J., Lyle, A., Kula, W., . . . Ielmini, D. J. I. E. D. L. (2018). Random number generation by differential read of stochastic switching in spin-transfer torque memory. 39(7), 951-954.

Charan, P., Usmani, T., Paulus, R., & Saeed, S. (2016). Performance Evaluation of AODV Protocol for Energy Consumption and QoS in IEEE 802.15.4 Based Wireless Sensor Network Using QualNet Simulator (Vol. 08).

Cope, P., Campbell, J., & Hayajneh, T. (2017). An investigation of Bluetooth security vulnerabilities. Paper presented at the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC).

Dementyev, A., Hodges, S., Taylor, S., & Smith, J. (2013). Power consumption analysis of Bluetooth Low Energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario. Paper presented at the 2013 IEEE International Wireless Symposium (IWS).

Dini, G., & Tiloca, M. (2010). Considerations on security in zigbee networks. Paper presented at the 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing.

Dönmez, T. C., & Nigussie, E. J. P. c. s. (2018). Security of lorawan v1. 1 in backward compatibility scenarios. 134, 51-58.

Fares, N., Askar, S. (2016). A Novel Semi-Symmetric Encryption Algorithm for Internet Applications. Journal of University of Duhok, Vol. 19, No. 1, pp. 1-9

Fizi, F., & Askar, S. (2016). A novel load balancing algorithm for software defined network based datacenters, International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom), Graz, 2016, pp. 1-6, doi: 10.1109/COBCOM.2016.7593506.

Fongen, A. (2012). Identity management and integrity protection in the internet of things. Paper presented at the 2012 third international conference on emerging security technologies.

Gebotys, C. H. J. I. T. o. V. L. S. I. S. (2006). A table masking countermeasure for low-energy secure embedded systems. 14(7), 740-753.

Grover, J., & Sharma, S. (2016). Security issues in wireless sensor network—a review. Paper presented at the 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO).

Hennebert, C., & Dos Santos, J. J. I. I. o. T. J. (2014). Security protocols and privacy issues into 6LoWPAN stack: A synthesis. 1(5), 384-398.

Hu, W., & Zhu, H. (2012). A methodology to enable self-organization in the internet of things based on negotiation mechanism. Paper presented at the Proceedings of 2012 International Conference on Measurement, Information and Control.

Huang, Z., & Wang, Q. J. W. W. W. (2019). A PUF-based unified identity verification framework for secure IoT hardware via device authentication. 1-32.

Hummen, R., Hiller, J., Wirtz, H., Henze, M., Shafagh, H., & Wehrle, K. (2013). 6LoWPAN fragmentation attacks and mitigation mechanisms. Paper presented at the Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks.

Ingham, M., Marchang, J., & Bhowmik, D. J. I. I. S. (2020). IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN.

Jurcut, A., Niculcea, T., Ranaweera, P., & LeKhac, A. J. a. p. a. (2020). Security considerations for Internet of Things: A survey.

Keti, F., Askar, S. (2015). Emulation of Software Defined Networks Using Mininet in Different Simulation Environments. *6th International Conference on Intelligent Systems, Modelling and Simulation*, Kuala Lumpur, 2015, pp. 205-210, doi: 10.1109/ISMS.2015.46.

Krejčí, R., Hujňák, O., & Švepeš, M. (2017). Security survey of the IoT wireless protocols. Paper presented at the 2017 25th Telecommunication Forum (TELFOR).

Le, A., Loo, J., Lasebae, A., Aiash, M., & Luo, Y. J. I. J. o. C. S. (2012). 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach. 25(9), 1189-1212.

Lonzetta, A. M., Cope, P., Campbell, J., Mohd, B. J., Hayajneh, T. J. J. o. S., & Networks, A. (2018). Security vulnerabilities in Bluetooth technology as used in IoT. 7(3), 28.

Luckett, P., McDonald, J. T., & Glisson, W. B. J. a. p. a. (2017). Attack-graph threat modeling assessment of ambulatory medical devices.

McCann, D., Eder, K., & Oswald, E. (2015). Characterising and comparing the energy consumption of side channel attack countermeasures and lightweight cryptography on embedded devices. Paper presented at the 2015 International Workshop on Secure Internet of Things (SIoT).

Mendez, D. M., Papapanagiotou, I., & Yang, B. J. a. p. a. (2017). Internet of things: Survey on security and privacy.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. J. A. h. n. (2012). Internet of things: Vision, applications and research challenges. 10(7), 1497-1516.

Pawar, A. B., & Ghumbre, S. (2016). A survey on IoT applications, security challenges and counter measures. Paper presented at the 2016 International Conference on Computing, Analytics and Security Trends (CAST).

Pongle, P., & Chavan, G. (2015). A survey: Attacks on RPL and 6LoWPAN in IoT. Paper presented at the 2015 International conference on pervasive computing (ICPC).

Randa, M., Samie, M., & Jennions, I. K. J. E. (2020). Delay-Based True Random Number Generator in Sub-Nanomillimeter IoT Devices. 9(5), 817.

Rao, T. A., & Haq, E. J. I. J. o. C. A. (2018). Security challenges facing IoT layers and its protective measures. 975, 8887.

Roman, R., Najera, P., & Lopez, J. J. C. (2011). Securing the internet of things. 44(9), 51-58.

Roukounaki, A., Efremidis, S., Soldatos, J., Neises, J., Walloschke, T., & Kefalakis, N. (2019). Scalable and configurable end-to-end collection and analysis of iot security data: Towards end-to-end security in IoT systems. Paper presented at the 2019 Global IoT Summit (GIoTS).

Seri, B., & Vishnepolsky, G. J. A., Tech. Rep. (2017). The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks.

Sulaiman, S., Askar, S. (2015). Invetigation of the Impact of DDoS Attack on Network Efficiency of the University of Zakho. Journal University of Zakho, Vol. 3(A) , No.2, Pp 275-280.

Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: a review. Paper presented at the 2012 international conference on computer science and electronics engineering.

Surendran, S., Nassef, A., & Beheshti, B. D. (2018). A survey of cryptographic algorithms for IoT devices. Paper presented at the 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT).

Swamy, S. N., Jadhav, D., & Kulkarni, N. (2017). Security threats in the application layer in IOT applications. Paper presented at the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC).

Vaccari, I., Cambiaso, E., Aiello, M. J. S., & Networks, C. (2017). Remotely Exploiting AT Command Attacks on ZigBee Networks. 2017.

Vatcharatiansakul, N., Tuwanut, P., & Pornavalai, C. (2017). Experimental performance evaluation of LoRaWAN: A case study in Bangkok. Paper presented at the 2017 14th International Joint Conference on Computer Science and Software Engineering (JCSSE).

Wallace, K., Moran, K., Novak, E., Zhou, G., & Sun, K. J. I. I. o. T. J. (2016). Toward sensor-based random number generation for mobile and IoT devices. 3(6), 1189-1201.

Williams, R., McMahon, E., Samtani, S., Patton, M., & Chen, H. (2017). Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach. Paper presented at the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI).

Yu, M., Zhuge, J., Cao, M., Shi, Z., & Jiang, L. J. F. I. (2020). A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices. 12(2), 27.

Zhang, Z.-K., Cho, M. C. Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K., & Shieh, S. (2014). IoT security: ongoing challenges and research opportunities. Paper presented at the 2014 IEEE 7th international conference on service-oriented computing and applications.

Cite this article:

Kurdistan Ali & Shavan Askar (2021). Security Issues and Vulnerabilities of IoT Devices. *International Journal of Science and Business, 5*(3), 101-115. doi: https://doi.org/10.5281/zenodo.4497707

Retrieved from http://ijsab.com/wp-content/uploads/690.pdf

Published by

IJSAB International