IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Review of various Security Attacks on IOT Technology

[1]Shivam Sharma, [2]Dr Anita Ganpati
[1]Research Scholar, [2]Professor
[1]Department of Computer Science,
[1]Himachal Pradesh University, Shimla, India

Abstract: IoT is one of the most emerging technologies in the field of Computer Science. Numerous technologies are connected to the internet through various wireless means. There are a lot of technologies that IoT works on such as Wi-Fi, Bluetooth, Zigbee, WiMAX, NB-IoT, LORA, NFC, etc. These technologies have their protocols, and various features such as Range, frequency, data rates and much more. These technologies are also in danger of various types of attacks on them due to which user's data is compromised. In this study, various studies proposed IoT technologies and their features along with the security attacks on them.
In this work, six technologies i.e., Wi-Fi, Bluetooth, Zigbee, WiMAX, NB-IoT, and LORA are compared and analysed after a deep analysis based on their general features along with the security attacks on them.

***Index Terms*- IoT, Wi-Fi, Bluetooth, Zigbee, WiMAX, NB-IoT, LORA**

1. Introduction

The Internet of Things, or IoT, is a brand new technology in the field of CS&IT in which smart gadgets are interconnected to the internet through various wireless means such as Wi-Fi, Bluetooth etc. Radio Frequency Identification (RFID) and Sensor Network Technologies are rising to meet this new challenge of invisibly embedded information and communication systems in the environment. The phrase "Internet of Things" is joined from the two words: the first one is "Internet," and the second one is "Things." The Internet is a universal network of interconnected computer networks that uses the standard Internet protocol suite (TCP/IP) to offer services to billions of users around the map[1]. The Internet of Things (IoT) has become a hot topic of discussion both inside and outside the business due to the tremendous expansion in the number of items linked to the internet through wired or wireless means[2]. The Internet of Things is expected to transcend all previous industrial revolutions, surpassing technological marvels such as the passenger train, the publishing industry, and energy. The fourth industrial revolution is marked by the "Internet of Things," as well as robotic systems, machine learning, nanotechnology, computing, biotechnology, 3D printing, and driverless or self-driven vehicles[3]. IoT, in particular, is an idea that has the potential to transform not only our lives but the way we operate[4]. Through fantastic solutions, technology may substantially improve privacy, power efficiency, schooling, healthcare, and many other dimensions of our normal routine life for consumers. By strengthening solutions, it can also strengthen the performance and decisions of businesses in the retail, distribution chain, manufacturing, agricultural and other industries. Everyday things such as automobiles, refrigerators, athletic gear, kitchen appliances, and even shoes along with watches can also be connected to the web. The Internet of Things (IoT) is the development of cell phones, programs, and everything else that is connected to the internet in order to incorporate more communication capabilities and extract relevant data using data analytics[4]. The Internet of Things, or IoT, has gained popularity as these technologies are employed for a variety of purposes including networking, transportation, smart learning, and business growth. The Internet of Things (IoT) has introduced the concept of hyper-connectivity, which permits individuals and organisations or companies to interact with one another from afar[2]. Nowadays, the IoT is being researched on both the personal and professional levels. Personally, the Internet of Things (IoT) plays a critical role in improving living standards through e-health, smart buildings along with smart schooling.

2. Overview of IoT Technologies

Everyday things, from healthcare gadgets to cell phones, smartwatches to surveillance cameras, including automobiles to industrial manufacturing lines, may be transformed smart using IoT innovation. Technological solutions typically contain security capabilities to protect smart objects and their applications against internet-based threats. IoT innovation is a crucial facilitator of smart, adaptable distributed systems, which may help to optimise organizational efficiency, cut costs, and create new income streams and marketing strategies. Organizations may become more productive by using IoT technology to improve and automate corporate operations and services, resulting in higher efficiency.

2.1 Wi-Fi

Wi-Fi allows technological gadgets such as cell phones and tablet devices to communicate with one another. The IEEE Wi-Fi protocol 802.11ah was just established. It runs at 2.4 & 5 GHz, which decreases operational complexity. The current Wi-Fi protocol, 802.11, is only functional at the closest access point and cannot serve consumers having vast residences. However, as an ultra-low-power variant of the protocols, IEEE 802.11ah solves this by providing a larger bandwidth and simpler communication, making it appealing for IoT deployments[5]. Wi-Fi networks are prevalent in a variety of interior settings, including residences, restaurants, retail stores, workplaces, colleges, and hospitals. Wi-Fi is now supported by the majority of cell phones, notebooks, and other portable gadgets. The goal of Wi-Fi location-based services is to use a W-LAN formed of wireless access points to accomplish positional object tracking activities in complicated situations (including wireless routers). It locates linked smartphones using a mixture of experimental testing and signal propagation simulations based on networking node position information[5].

2.2 ZigBee

The ZigBee Alliance has invented a different easily accessible wireless standard called ZigBee. ZigBee is reduced power, reduced cost, and low-data-rate wireless sensing and control networking that focuses on interoperability. It is simple to set up and can accommodate up to 65,000 nodes based on the configurations utilised[6]. ZigBee (IEEE 802.15.4) is a limited wireless PAN protocol that defines the physical & medium access control tiers and transfers up to 10 metres. This standard describes sixteen channels in the 2.4 GHz spectrum, but with a smaller range of 2 MHz and no overlapping. As a result, up to 16 ZigBee connections can operate simultaneously in the same region. In the "ZigBee Pro" Protocol, the most recent ZigBee version allows frequency band. This enables a ZigBee PAN to switch from one channel to another if the first becomes overloaded.[7]

2.3 Bluetooth

Bluetooth is brand-new wireless telecommunication technology. The goal of the concept would be to wirelessly link different devices in a small space, such as a workplace or a residence. The BT range, which is currently around 10 metres, limits the surroundings. Before adopting the innovation, a thorough examination of the security system is required. The data communicated over the Bluetooth piconet, particularly in the workplace, might be critical and demands robust protection[8]. Bluetooth was developed by Ericsson, a Swedish communications corporation, around 1994 to construct ad hoc, short-range wirelessly systems which enabled gadgets to communicate with each other. In 1998, Ericsson formed a Special Interest Group (SIG) with IBM, Intel, Nokia, and Toshiba that establish and support the open industry specification for Bluetooth technology. The first Bluetooth-enabled item, a headphone, was released in shops in 2000, and Bluetooth innovation was validated by IEEE for 802.15.1 two years later, in March 2002[9].

2.4 WiMAX

WiMAX, or 802.16, is wireless technology. In June 2004, the IEEE ratified the 802.16 standards. This technology has a distance of more than 48 kilometres and speeds up to 70Mbps. WiMAX is a network communication standard similar to Wi-Fi. WiMAX enables greater data speeds across greater ranges, effective capacity utilisation, and near-zero interruption. WiMAX is a replacement for Wi-Fi technology in several ways. Currently, engineers anticipate a WiMAX reader in a person's house, together with a Wi-Fi broadcaster for in-home connectivity, and computers and other gadgets capable of sending immediately to WiMAX antennas in the future[10]. The first generation of WiMAX, IEEE 802.16-2004, had intended to offer stationary and nomadic customers broadband wireless connection for the last mile. The service may extend up to 50 kilometres, letting people access the internet in no-line-of-sight situations. IEEE 802.16-2005 (Portable WiMAX) offers improved QoS and up to 120 km/h agility[11].

2.5 LORA

LoRa is indeed a wireless technology. The majority of wireless systems employ Frequency Shift Keying [FSK] for obtaining low energy. Most army and long-range domains will use the chirping spread bandwidth for lengthy communications and lower power consumption. LoRa also uses the Chirp Spread Spectrum for effective and reliable modulation. The most significant benefit of LoRa technology is its high transmission capacity[12]. The chirp spread spectrum transmission method is used by LoRa. Due to its sturdy characteristics and lengthy capability, this method has been employed in defence and aerospace telecommunication for decades. It has become commercially available for LoRa communications. Multipath and fading resistance is indeed provided[13].

2.6 NB-IoT

The Narrowband Internet of Things (NB-IoT) is a set of 3GPP technologies based on the long evolutionary (LTE) architecture. NB-IoT can cohabit and interact easily with upcoming 5G infrastructures, allowing for LTE-IoT installation possibilities. Current 4G LTE networks are still being used to evaluate the installation of multiple NB-IoT connections and services, especially as the abilities of current low wide-area network (LPWAN) technologies improve. Despite efforts to improve the present LTE broadband infrastructure, much machine-type communication (MTC) technologies remained inadequate. NB-IoT (also known as LTE-Cat- NB1) simplifies and optimises business-grade technological requirements to decrease wireless overhead and provide IP and non-IP data, making it a viable option for operators, gadgets makers, and corporate clients. By holding an available physical block of 180kHz both for uplink (UL) and downlink (DL) activities or by substituting one GSM channel of 200kHz without impacting the host network's capacity, the NB-IoT fits into the current system and supports optimum coexistence[14].

3. Literature Review

Alkhatib, H., et al. in [3] explained that computing devices will range in size from micro to mega by 2022, with wireless links allowing accessibility to interconnected services. The virtual connection will allow necessary computer resources to be integrated to offer consumers smooth solutions. Through developing a human-computer interface, the ensuing ecosystem will provide ongoing, unbroken solutions that improve efficiency, production, cooperation, and accessibility to intelligence and information.

The advantage of technology, on the other hand, is what we create of it. The speed with which these technological developments benefit mankind will be determined by the rules and laws that precede their development. Technology is a facilitator; it is up to us to make the greatest use of it to develop humanity.

Dhillon, P., and Sadawarti, H. in [16] concluded that in the near future, Zigbee will play a key role in sectors such as building management, lighting controls, fire and intrusion alarm, traffic control, and war fields, among others, making computer and communication technologies more useable and accessible to consumers. These networks are simple to set up and less expensive than other technologies. A single chip would only set you back $5. However, as the protocol stack's memory space shrinks, the cost of Zigbee drops to roughly $2 per chip. Because the gadgets keep a list of trustworthy devices inside the system and frame fidelity to keep data from being manipulated by persons lacking cryptographic keys, Zigbee technologies are particularly valuable from a cybersecurity standpoint.

Kaushik, S. in [15] concluded by concentrating on the fundamental overview and architecture design, this study presented an overview of the technical features of Wi-Fi network technology. In the development of wireless networks, WiMAX and LTE will be equally significant. WiMAX is crucial because it opens up a whole new world of business possibilities. For wireless MANs, WiMAX is potential wireless communication technology. LTE-Advanced offers a smooth transition route for both LTE and HSPA, resulting in better end-user experiences with broadband services. It lowers the price for maintenance and installation while also introducing new economic potential to local installations. Only after implementation will the resilience and usefulness of end-to-end cybersecurity measures in WiMAX and LTE become obvious.

Madakam, S., et al. in [1] concluded that through different technologies and applications, IoT has progressively brought an ocean of technological advancements into our everyday lives, which in turn serves to make our living easier and more pleasant. IoT devices have several uses in healthcare, production, commercial, commuting, educational, government, mining, and habitat, among others. Despite the numerous advantages of IoT, there are significant limitations in IoT governance and deployment. The significant findings in the research are as follows, there is no universally accepted definition; at the architectural level, global standards are necessary; because innovations differ from one manufacturer to the next, they must be compatible; need to develop common protocols for improved global governance.

Pal, A., et al. in [4] outlined that in the context of modern ongoing research in the Internet of Things, networked sensors and devices, signal processing, machine learning, and AI, how do future healthcare systems look. They are now attempting to project into the future and sketch out the contours of a public health system which may emerge in 2050.

Liya, M. L., and Aswathy, M. in [12] concluded that the subject of LoRa effectiveness and implementation studies. The above study is mostly centred on a comparative study and developments in IoT LoRa connectivity. In the world of IoT, LoRa has several possibilities and bright prospects. LoRa WAN provides various benefits over other LPWAN systems, including extended battery lifespan, good variety, and inexpensive. The small data throughput of LoRa is indeed one of the key drawbacks.

Whitehurst, L. N., et al. in [17] explained security in ZigBee is a complicated subject that involves difficulties at the MAC, NWK, and APS levels. ZigBee networks are vulnerable to the same threats and vulnerabilities that affect 802.15.4 networks, including IV reuse, ACL loss, and DoS attacks. Because it wasn't as easy as picking an encryption scheme, the app developer should consider various forms of assault while implementing its security features. On a ZigBee network, the standard level of security is no security when no functionalities are configured. A network's key is only as safe as its privacy solutions at all stages of the stack. As a result, a suitable key management method for ZigBee networks becomes critical. Durability, effectiveness, and the capacity to develop are all important aspects of managerial applicability.

Singh, G., et al. in [18] explained that for low data rates, low power consumption, and extended battery life, ZigBee is by far the most promising technology protocol. ZigBee connections are self-healing and dependable. These systems are simple to set up and less expensive than other techniques. The intricacy of ZigBee networks is the key concern nowadays. Privacy is a major issue since attackers can easily breach ZigBee connections, and far too much innovation makes the people sluggish.

Khan, R., et al. in [2] concludes that the Internet of Things (IoT) incorporates intelligence into sensor equipment to enable autonomous communication, exchange of information, and wise decision-making. IoT only shifts human-human, human-device, and device-device communication from one to the other. This piece of work offered a quick overview of the Online, suggested a general framework for IoT, discussed potential uses for the next as well as several current worldwide IoT initiatives, and then discussed some of the major issues with IoT technology. Although the IoT adoption may be challenging and need major research resources to overcome the obstacles, it will likely soon offer enormous economic, organizational, and individual advantages.

Koutras, D., et al. in [21] concluded that the fast implementation of IoT within the healthcare profession predicts that the complexity and scale of WSN and wireless sensor connectivity in healthcare care will keep rising. In this article, IoT standards are reviewed in light of new research, along with their possibilities and possible security risks when used in medical IoT networks. As used in the medical treatment industry, the authors first established a taxonomy of communication systems by kind of medical equipment. Then, the authors methodically listed and examined their security issues and suggested remedies that were appropriate for medical settings.

Baronti, P., et al. in [24] reviewed ZigBee/IEEE 802.15.4 specifications and current research on sensor networks. This study gives a summary of the fuel efficiency, communications, information management, and security products that have been adopted as standards and those that have been suggested in recent literature. The researchers found considerable variances in several instances, such as when regulations and the key research findings converged (as in the instance of privacy).

4. Results and Analysis

Comparison of different IoT Technologies on General Features such as Protocol, range, frequency, data rate, power, topology, and cost which are used to assess the properties of different IoT technologies. Following are the features that are taken into consideration for a successful comparison analysis in this study :

Protocol
The Institute of Electrical and Electronics Engineers has established an IEEE protocol (IEEE). This organisation is a specialized group that develops protocols and guidelines for a variety of innovations.

Range
The Range defines how much distance the specific technology covers.

Frequency
The number of times a repeated event occurs per unit of time is known as frequency. It is used to measure specific IoT technology.

Data Rate
Data Rate is the speed of a particular IoT technology upon which it is compared.

Power
It is the total amount of consumption of electricity, a specific technology consumes.

Topology
The organization of the technologies (links, nodes, etc.) of an IoT system is known as topology. Every technology has its own topology.

Cost
The amount of cost required to establish each technology.

table 1: comparative analysis of various iot technologies based on general features.

Ref.	Features → Technology ↓	Protocol	Range	Frequency	Data Rate	Power	Topology	Cost
[1], [5], [15]	**Wi-Fi**	802.11	150m	2.4 GHz, 5 GHz	High	High	Star, Mesh	Low
[6], [7], [16], [17], 18]	**Zigbee**	802.15.4	150m	2.4 GHz	Low	Low	Star, Mesh, Tree	Low
[8], [9]	**Bluetooth**	802.15.1	0.5-1m to 100m	2.4 GHz	Low	Low	Star, Bus	Low
[10], [11], [19]	**WiMAX**	802.16	48 km	N/A	High	High	N/A	High
[12], [13]	**LORA**	802.15.4	10-15 km	1 GHz	Low	Low	Star	Low
[14]	**NB-IoT**	3GPP in LTE	8-25 km	200 KHz	Low	Low	N/A	Low

In table 1, each of the technology i.e., Wi-Fi, Zigbee, Bluetooth, WiMAX, NB-IoT and LoRa has its own Protocols. They have different ranges according to their capabilities. Each of them has different frequencies, rates of data transmission, power consumption and cost. Every technology has its own topology but the topology of WiMAX is not available.

Types of attacks and causes are the another two key dimensions used to assess the security issues of different IoT technologies. Following are the attacks that are taken into consideration for a successful comparative analysis in this study :

Types of attacks
There are several types of attacks on various IoT devices that are described below.

Causes
It explains the major causes that occur due to these attacks.

table 2: types of attacks and their causes on various technologies of iot.

Ref.	Technologies of IoT	Attacks	Causes
[20], [21], [22]	**Wi-Fi**	• DDOS • EDDOS • Harvesting and Forging Data	• Send malicious activities to delete the resources of the targeted system. • Maximum energy consumption
[17], [23], [24]	**Zigbee**	• Physical attacks • DOS attacks • Replay attacks	• Copy device memory and passwords. • Overload the bandwidth and processors.
[9], [25], [26]	**Bluetooth**	• Bluebugging • Bluejacking • Bluesmack • Helomoto	• Attackers can take control of the victim's phone. • Send unsolicited messages to open Bluetooth devices. • Buffer overflow attack using L2CAP echo messages.
[27], [28], [29]	**WiMAX**	• Jamming • Scrambling	• Scrambling is difficult to detect as it is also difficult to achieve. • Compromises with the level of authentication.
[30], [31], [32]	**LORA**	• Replay • Wormhole	• Unwanted entities attack security protocols, resending or duplicating lawful transmitted data. • Malicious equipment collects messages through one gadget and sends them to another gadget which is far away to repeat the collected data.
[33], [34], [35]	**NB-IoT**	• Social Attack • Bandwidth Spoofing • Lack of physical security • Insecure default credentials	• An eavesdropper examines the data provided by the target. • The attackers obtain bandwidth, allowing connectivity between both the ground station and the gadget to be hijacked.

In table 2, each of the technologies i.e., Wi-Fi, Zigbee, Bluetooth, WiMAX, NB-IoT and LoRa have their own security attacks. They all are suffering from different attacks. Each attack causes damage to the technologies and the gadgets attached to them.

5. Conclusion

IoT is a promising technology which helps to make our lives easier and simple with the help of various technologies and applications. The IoT Technologies have become prominently important in the present scenario as almost each and every device near us is connected to the internet which makes these devices smart.

The main objective of this study is to have a deeper knowledge of various IoT technologies such as Wi-Fi, Bluetooth, ZigBee, WiMAX, NT-IoT and LoRa. Every gadget around us is connected to Wi-Fi such as Smart Watch, Smart Phones, Smart LED and many other devices. In this work, various attacks have been discussed in various technologies. In Wi-Fi, there are several attacks such as DDOS attacks, EDDOS attacks, Harvesting and Forging of Data attacks have been discussed. In ZigBee, Physical attacks, DDOS and replay attacks have been discussed. Attacks such as Bluebugging, Bluejacking, Bluesmack and Helomoto have been discussed in Bluetooth. In WiMAX, Jamming and Scrambling have been discussed. Also, attacks such as Replay and Wormhole have been discussed. In last, Social attacks, Bandwidth Spoofing, Lack of physical security and Insecure default credentials have been discussed in NB-IoT. All these attacks can cause major issues in the security of the sensitive data of the user.

6. Future Scope

In this work, a review of six IoT technologies is done i.e., Wi-Fi, Bluetooth, ZigBee, WiMAX, NT-IoT and LoRa on the basis of various general features along with security attacks. In future, more security loops in these technologies can be detected and also how to prevent these attacks using various techniques. In future, more technologies can be discussed such as RFID, WSN etc on these general features as well as on security attacks.

Reference

1. Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(05), 164.
2. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In 2012 10th international conference on frontiers of information technology (pp. 257-260). IEEE.
3. Alkhatib, H., Faraboschi, P., Frachtenberg, E., Kasahara, H., Lange, D., Laplante, P., ... & Schwan, K. (2015). What will 2022 look like? The IEEE CS 2022 report. Computer, 48(3), 68-76.
4. Pal, A., Mukherjee, A., & Dey, S. (2016). Future of healthcare—sensor data-driven prognosis. In Wireless World in 2050 and Beyond: A Window into the Future! (pp. 93- 109). Springer, Cham.

5. Samuel, S. S. I. (2016, March). A review of connectivity challenges in IoT-smart home. In 2016 3rd MEC International conference on big data and smart city (ICBDSC) (pp. 1-4). IEEE.
6. Aju, O. G. (2015). A survey of zigbee wireless sensor network technology: Topology, applications and challenges. International Journal of Computer Applications, 130(9), 47-55.
7. Challoo, R., Oladeinde, A., Yilmazer, N., Ozcelik, S., & Challoo, L. (2012). An overview and assessment of wireless technologies and co-existence of ZigBee, Bluetooth and Wi-Fi devices. Procedia Computer Science, 12, 386-391.
8. Träskbäck, M. (2000, November). Security of Bluetooth: An overview of Bluetooth security. In Helsinki University of Technology, Department of Electrical and Communications Engineering, seminar material for the course Tik-86.174 "Bluetooth technology & utilization.
9. Lonzetta, A. M., Cope, P., Campbell, J., Mohd, B. J., & Hayajneh, T. (2018). Security vulnerabilities in Bluetooth technology as used in IoT. Journal of Sensor and Actuator Networks, 7(3), 28
10. Sidhu, B., Singh, H., & Chhabra, A. (2007). Emerging wireless standards-wifi, zigbee and wimax. World Academy of Science, Engineering and Technology, 25(2007), 308-313.
11. Muntean, V. H., & Otesteanu, M. (2010, November). WiMAX versus LTE-An overview of technical aspects for Next Generation Networks technologies. In 2010 9th International Symposium on Electronics and Telecommunications (pp. 225-228). IEEE.
12. Liya, M. L., & Aswathy, M. (2020, October). LoRa technology for Internet of Things (IoT): a brief survey. In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 8-13). IEEE.
13. Devalal, Shilpa, and A. Karthikeyan. "LoRa technology-an overview." 2018 second international conference on electronics, communication and aerospace technology (ICECA). IEEE, 2018.
14. Gbadamosi, S. A., Hancke, G. P., & Abu-Mahfouz, A. M. (2020). Building upon NB-IoT networks: A roadmap towards 5G new radio networks. IEEE Access, 8, 188641-188672.
15. Kaushik, S. (2012). An overview of technical aspect for WiFi networks technology. International Journal of Electronics and Computer Science Engineering (IJECSE, ISSN: 2277-1956), 1(01), 28-34.
16. Dhillon, P., & Sadawarti, H. (2014). A review paper on zigbee (ieee 802.15. 4) standard. International journal of engineering research and technology, 3.
17. Whitehurst, L. N., Andel, T. R., & McDonald, J. T. (2014, April). Exploring security in ZigBee networks. In Proceedings of the 9th Annual Cyber and Information Security Research Conference (pp. 25-28).
18. Singh, G., Bhardwaj, R., & Mehla, S. (2012). ZigBee: A Review 1
19. More, S., & Mishra, D. K. (2012, November). 4G revolution: WiMAX technology. In 2012 Third Asian Himalayas International Conference on Internet (pp. 1-4). IEEE.
20. Tushir, B., Dalal, Y., Dezfouli, B., & Liu, Y. (2020). A quantitative study of ddos and e-ddos attacks on wifi smart home devices. IEEE Internet of Things Journal, 8(8), 6282- 6292.
21. Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., & Douligeris, C. (2020). Security in IoMT communications: A survey. Sensors, 20(17), 4828
22. Westerlund, O., & Asif, R. (2019, February). Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things. In 2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS) (pp. 1-10) IEEE .
23. Durech, J., & Franeková, M. (2014, January). Security attacks to ZigBee technology and their practical realization. In 2014 IEEE 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI) (pp. 345-349). IEEE.
24. Baronti, P., Pillai, P., Chook, V. W., Chessa, S., Gotta, A., & Hu, Y. F. (2007). Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards. Computer communications, 30(7), 1655-1695.
25. Browning, D., & Kessler, G. C. (2009). Bluetooth hacking: A case study. Journal of Digital Forensics, Security and Law, 4(2), 57
26. Albahar, M. A., Haataja, K., & Toivanen, P. (2016). Bluetooth MITM vulnerabilities: a literature review, novel attack scenarios, novel countermeasures, and lessons learned. International Journal on Information Technologies & Security, 8(4).
27. Habib, M., & Ahmad, M. (2010, February). A review of some security aspects of WiMAX and converged network. In 2010 Second International Conference on Communication Software and Networks (pp. 372-376). IEEE.
28. Simion, D., Ursuleanu, M. F., & Graur, A. (2012, May). An overview on WiMAX security weaknesses/potential solutions. In 11th International Conference on Development and Application Systems, Suceava, Romania (pp. 110-117).
29. Alezabi, K. A., Hashim, F., Hashim, S. J., Ali, B. M., & Jamalipour, A. (2016). Authentication process enhancements in WiMAX networks. Security and Communication Networks, 9(17), 4703-4725.
30. Aras, E., Ramachandran, G. S., Lawrence, P., & Hughes, D. (2017, June). Exploring the security vulnerabilities of LoRa. In 2017 3rd IEEE International Conference on Cybernetics (CYBCONF) (pp. 1-6). IEEE.
31. Li, C., & Cao, Z. (2022). Lora networking techniques for large-scale and long-term iot: A down-to-top survey. *ACM Computing Surveys (CSUR)*, *55*(3), 1-36.
32. Santamaria, M., & Marchiori, A. (2019, November). Demystifying LoRa WAN security and capacity. In 2019 29th International Telecommunication Networks and Applications Conference (ITNAC) (pp. 1-7). IEEE.
33. Kumar, V., Jha, R. K., & Jain, S. (2020). NB-IoT security: A survey. Wireless Personal Communications, 113(4), 2661-2708.
34. Mentsiev, A. U., & Magomaev, T. R. (2020, May). Security threats of NB-IoT and countermeasures. In IOP conference series: materials science and engineering (Vol. 862, No. 5, p. 052033). IOP Publishing.
35. Jha, R. K., Kour, H., Kumar, M., & Jain, S. (2021). Layer based security in narrow band Internet of Things (NB-IoT). Computer Networks, 185, 107592.