Attacks And Defense in Short Range Wireless Technologies for IOT

Mrs. Swapna Baadkar
Assistant Professor
Dept. of ECE
SJC Institute of Technology
Chikkaballapur, Karnataka
swapnab.ece@sjcit.ac.in

Sai Kiran S
Dept. Of ECE
SJC Institute of Technology
Chikkaballapur, Karnataka
saikiransri2932@gmail.com

1. ABSTRACT

The rapid growth of the Internet of Things (IoT) has led to the widespread adoption of short-range wireless communication technologies such as Bluetooth, Zigbee, NFC, and Wi-Fi. These technologies enable seamless device-to-device communication in smart homes, healthcare, industrial automation, and other IoT domains. However, their open and wireless nature introduces several security vulnerabilities. Common attacks include eavesdropping, replay attacks, man-inthe-middle (MITM), jamming, spoofing, and unauthorized access, all of which pose significant threats to data privacy, device integrity, and network availability. To mitigate these threats, robust defense mechanisms are essential. Techniques such as encryption, secure authentication protocols, frequency hopping, access control, and firmware updates play a crucial role in enhancing the security posture of IoT systems. Additionally, employing intrusion detection systems (IDS) and adopting secure pairing methods can further protect against evolving cyber threats. This paper provides a comprehensive overview of prevalent attacks targeting short-range wireless technologies in IoT and explores effective countermeasures. By understanding both the vulnerabilities and defenses, stakeholders can design more secure and resilient IoT systems capable of withstanding modern cyber threats while maintaining efficient and reliable communication.

2. PROBLEM STATEMENT

The increasing reliance on short-range wireless technologies such as Bluetooth, Zigbee, NFC, and WiFi in IoT devices has significantly enhanced connectivity and automation across various sectors. However, the inherent vulnerabilities in these wireless protocols expose IoT networks to a wide range of security threats, including eavesdropping, spoofing, denial-of-service attacks, and unauthorized access. These attacks can lead to data breaches, service disruptions, and loss of user trust. Despite the availability of security mechanisms, many IoT devices lack adequate protection due to limited computational resources, outdated firmware, or poor implementation practices. There is a critical need to identify and analyze the specific security challenges faced by short-range wireless technologies in IoT and to develop effective, lightweight defense mechanisms that ensure secure communication without compromising performance or energy efficiency.

3. OBJECTIVE

• To explore the role of short-range wireless technologies (e.g., Bluetooth, Zigbee, NFC, Wi-Fi) in IoT communication. • To identify the major security threats and vulnerabilities associated with these wireless technologies in IoT environments. • To classify different types of cyber-attacks, including eavesdropping, spoofing, replay, and denial-of-service. • To analyze the limitations of existing security mechanisms used in short-range wireless protocols. • To propose efficient and lightweight defense strategies suitable for resource-constrained IoT devices. • To recommend best practices for securing IoT networks, enhancing data confidentiality, integrity, and availability.

4. LITERATURE SURVEY

1. Kari m Lounis and Mohammed Zulkernine [1] 'Attack and Defenses in Short -Range Wireless Technologies for IOT'. In this paper, they have introduced an attack classification for wireless IoT attacks. This classification categorizes an attack based on which security service is compromised by the attack. We have adopted the classification to review the attacks that occurred in the last two decades on Wi-Fi, Bluetooth, ZigBee, and RFID wireless communication technologies. 2. M. N. K. Boulos and N. M. Al-Shorbaji [2] has described The Internet of Things is rapidly gaining a central place as key enabler of the smarter cities of today and the future. Such cities also stand better chances of becoming healthier cities. The WHO and associated national Healthy Cities networks have hundreds of member cities around the world that could benefit from, and harness the power of, IoT to improve the health and well-being of their local populations. 3. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao [4] has explained Internet of Things (IoT) is an innovative paradigm envisioned to provide massive applications that are now part of our daily lives. Millions of smart devices are deployed within complex networks to provide vibrant functionalities including communications, monitoring, and controlling of critical infrastructures. 4. D. E. Kouicem, A. Bouabdallah, and H. Lakhlef [5] This technology offers a huge business value for organizations and provides opportunities for many existing applications such as energy, healthcare and other sectors. However, as new emergent technology, IoT suffers from several security issues which are most challenging than those from other fields regarding its complex environment and resources-constrained IoT devices. A lot of researches have been initiated in order to provide efficient security solutions in IoT

5. METHODOLOGY

This study follows a structured and analytical methodology aimed at exploring the security vulnerabilities and countermeasures in short-range wireless communication technologies used in IoT. The focus was placed on four widely adopted technologies—Wi-Fi, Bluetooth, ZigBee, and RFID—due to their critical role in enabling communication among IoT devices. The process began with an extensive literature review to gather existing knowledge on these technologies, including their network architectures, communication protocols, and security implementations. Research articles, white papers, and technical documents were carefully reviewed to identify the common and advanced forms of

cyberattacks that have been observed in real-world IoT applications. Each technology was analyzed individually to understand how it functions, where it is commonly used, and what security mechanisms it employs. The attacks were categorized based on the specific security services they impact: authentication, confidentiality, integrity, and availability. For instance, attacks such as entity spoofing, message forgery, packet replay, sniffing, and tampering were examined in terms of how they are carried out, what vulnerabilities they exploit, and the level of damage they can cause to a network. The next phase involved the study of various defense mechanisms and security strategies designed to address these threats. This included evaluating the use of encryption protocols (like WPA3, AES, and CCMP), authentication techniques (such as digital certificates and challenge-response methods), and access control measures. Additionally, physical security, network configuration strategies, and upperlayer security protocols (like TLS and OWE) were considered as part of a multi-layered defense approach. Finally, a comparative analysis was conducted across the four technologies to highlight their respective strengths and weaknesses from a security standpoint. This analysis helped in identifying the most vulnerable areas and in suggesting practical improvements. The methodology ensures a holistic understanding of both the attack surface and the defense landscape in the context of short-range wireless communication for IoT systems.

6. ADVANTAGES

• Improved data communications lead to faster transfer of information within businesses and between partners and customers. For example, salespeople can remotely check stock levels and prices while on sales calls.

• Because wireless technology allows the user to communicate while on the move, you are rarely out of touch - you don't need extra cables or adaptors to access office networks.

• Office-based wireless workers can network without sitting at dedicated computers and can continue to do productive work while away from the office. This can lead to new styles of working, such as home working or direct access to corporate data while on customer sites.

• See more on employees working from home. • Wireless networks can be easier and cheaper to install, especially in listed buildings or where the landlord will not permit the installation of cables.

• Wireless networking could allow you to offer new products or services. For example, many airport departure lounges, train stations, hotels, cafes and restaurants have installed 'hot spot' Wi-Fi services to allow mobile users to connect their equipment to their 'home' offices while travelling.

DISADVANTAGES:

• Wireless transmission is more exposed to attacks by unauthorised users, so you must pay particular attention to security. See securing your wireless systems.

• You may experience interference if others in the same building also use wireless technology, or where other sources of electromagnetic (radio) interference exist. This could lead to poor communication or, in extreme cases, complete loss of wireless communication.

• In some buildings, getting consistent coverage can be difficult, leading to 'black spots' where the signal isn't available. For example, in structures built using steel reinforcing materials, you may find it difficult to pick up the radio frequencies used.

• Wireless transmission can be slower and less efficient than 'wired' networks. In larger wireless networks, the 'backbone' network is usually wired or fibre rather than wireless.

7. CONCLUSION

The Internet of Things (IoT) connects billions of heterogeneous devices, called Things, using different communication technologies and protocols to provide end-users, all over the world, with access to a variety of smart applications. It also invites cybercriminals who exploit the IoT infrastructures to conduct large scale, distributed, and devastating cyberattacks. The security of IoT infrastructures strongly depends on the security of its wired and wireless infrastructures. While the wireless infrastructure is thought to be the most outspread part in IoT, it is at the same time the most vulnerable and accessible for attackers. Hence, more focus should be placed on the security of wireless infrastructures of IoT. In this paper, we have introduced an attack classification for wireless IoT attacks. This classification categorizes an attack based on which security service is compromised by the attack. We have adopted the classification to review the attacks that occurred in the last two decades on Wi-Fi, Bluetooth, ZigBee, and RFID wireless communication technologies. These wireless communication technologies are considered to be the most used for shortrange wireless communications in IoT. We have also discussed possible countermeasures that can be applied to mitigate, or at least detect, certain attacks. In the future, we will survey and classify mid and long range IoT wireless communication technologies, such as LoRa, Sigfox, NB-IoT, WiMAX, UMTS, 4G/LTE, and 5G, which are largely used in largescale IoT applications. They believe that the application of these mechanisms will not last for too long. In fact, as IoT is rapidly transforming the Internet into a Thing to Thing communication system, the need for new authentication protocols, mainly thing-to thing authentication protocols, is rising. Also, besides authentication, we believe that in most cases the reviewed attacks that are related to compromising data integrity and system availability have a bigger impact than the attacks that are related to breaching IoT data confidentiality.

8. REFERENCES

[1] Karim Lounis and Mohammed Zulkernine “Attacks and Defenses in Short-Range Wireless Technologies For IOT” May 2020

[2] M. N. K. Boulos and N. M. Al-Shorbaji, ‘‘On the Internet of Things, smart cities and the WHO healthy cities,’’ Int. J. Health Geogr., vol. 13, no. 1, p. 10, 2014.

[3] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O’Flynn, ‘‘IoT goes nuclear: Creating a zigbee chain reaction,’’ IEEE Secur. Privacy, vol. 16, no. 1, pp. 54–62, Jan. 2018.

[4] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, ‘‘A survey on security and privacy issues in Internetof-Things,’’ IEEE Internet Things J., vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[5] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, ‘‘Internet of Things security: A top-down survey,’’ Comput. Netw., vol. 141, pp. 199–221, Aug. 2018

[6] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, ‘‘Internet of Things security and forensics: Challenges and opportunities,’’ Future Gener. Comput. Syst., vol. 78, pp. 544–546, Jan. 2018.