CHAPTER-04

IMPACT ON DATA SECURITY IN WIRELESS SENSOR NETWORK TECHNOLOGY

[1]BABITA CHAUDHARY
[1]HLM Group of Institutions

Chapter ID: NSP/ICAAR-2023/A-04

ABSTRACT

In recent few years, IoT has been adopted in most fields of life around the world. For data on IoT a wireless sensor network system is required. It is critical that the Sensor network technologies become ample mature and robust against Malicious attack to be trustworthy. The inclusion of wireless communication technology also runs various types of security threats. This paper is presented the security related issues, the challenges and to propose some solutions to secure the WSN against these security threats while the set of challenges in sensor networks are diverse. This paper begins by introducing the concept of Wireless Sensor Network (WSN). The introductory section gives brief information on the WSN components and its architecture. This paper also proposes some of the security goals for Wireless Sensor Network.

Keywords: *Wireless Sensor Network (WSN), Internet of Things (IoT), Network Security, Data Security*

INTRODUCTION

A sensor network is a collection of small sensor nodes with different sensing capabilities that take down data at various environments and dispatch it to a base station. Depending on the deployment location and application, sensor networks can be wired or wireless. In a wired sensor network, sensor nodes are affixed by Ethernet cables; in Variance, a wireless sensor network employs Bluetooth, WiFi, cellular, Near-Field-Communication (NFC), Narrowband Internet of Things (NB-IoT), and Long-Range (LoRa) technologies. Due to the distributed nature of the sensor deployment, wireless sensor networks have acquired much more attention than wired sensor networks. Sensors are mainly classified based on their purpose, i.e., the types of physical conditions monitored by the specific sensors. The general conditions scanned by the sensors are sound, distance, heat, light, or any measurable changes. Sensor outputs are attached to an IoT network through devices, thus building a management network where security is crucial to forbid data breaches and unwanted exposure.

A wireless sensor network (WSN) is a distributive network which is made up of tiny sensors capable of accumulating the data like temperature, humidity, pressure, voice, etc. [1]. These remote sensors have a limited energy source, storage, and short radio range. The sensors associate together to form an ad-hoc network that describes the activities on the web, and finally, the data collected reach the sink. WSNs find applications in health monitoring, disaster management, target tracking, habitat monitoring, and many more. Sensor networks comprise tiny sensor nodes with many resource constraints like inadequacy of power and data storage.

WSN Architecture: There are 2 types of architecture used in WSN: Layered Network Architecture, and Clustered Architecture. These are explained as following below.

Layered Network Architecture:

Layered Network Architecture makes use of a few hundred sensor nodes and a single powerful base station. Network nodes are organized into concentric Layers.
It consists of 5 layers and three cross layers.

The 5 layers are:

1. Application Layer
2. Transport Layer
3. Network Layer
4. Data Link Layer
5. Physical Layer

Application Layer	→	Intersection with end user and Data aggregation
Transport Layer	→	Safe Transport of Data
Network Layer	→	Managing the Routing, Networking and topology
Data link Layer	→	Error Detection
Physical Layer	→	Modulation, Signal Processing

Fig.2.1 WSN Layered structure

Clustered Network Architecture: In Clustered Network Architecture, Sensor Nodes autonomously clubs into groups called clusters. It is based on the *Leach Protocol* which makes use of clusters. Leach Protocol stands for Low Energy Adaptive Clustering Hierarchy.

Properties of Leach Protocol

- It is a 2-tier hierarchy clustering architecture.
- It is a distributed algorithm for organizing the sensor nodes into groups called clusters.
- The cluster head nodes in each of the autonomously formed clusters create the Time-division multiple access (TDMA) schedules.
- It makes use of the concept called *Data Fusion* which makes it energy efficient.

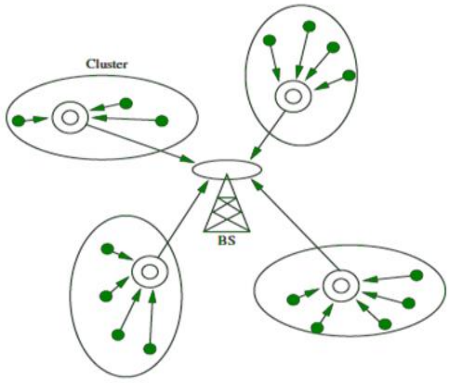

Fig 2.2 WSN Clustered Structure

CLASSIFICATION OF THREATS IN WSN SYSTEMS

WSN is a main part of the Internet of Things (IoT) [1], [2]. Almost all the Government Facilities and corporate Sectors such as Banking, hospitals, education, emergency services, and military have all

become increasingly reliant on cyber-space that can affect the level of complexity. IoT assaults (attacks/threats) are used to publicize false information, disable desirable services, get access to sensitive information, conduct espionage, steal data, and cause financial damage. Over time, the nature, complexity, and severity of these attacks are developed in which their complexity is increased as well. Many organizations and countries can be attacked because of the weakness of security system in understanding the work mechanism of these attacks. Developing effective security measures necessitates a full understanding of such assaults and their classification, which is established on the following criteria: Purpose Legal Classification, severity of Involvement, Scope and on Wireless Sensor Network (WSN)

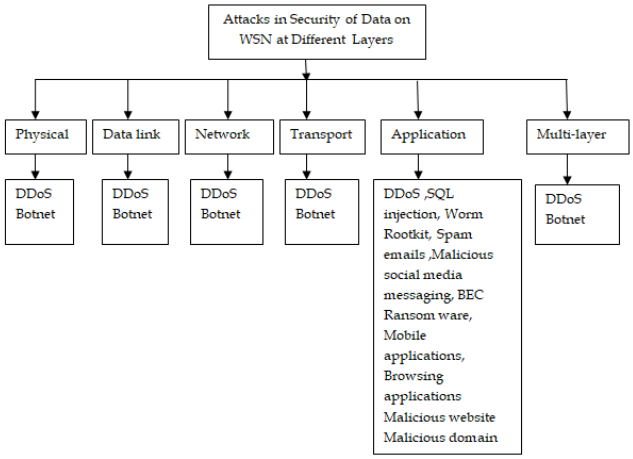

Fig 3.1 Attacks in WSN at different layers

DDoS Attack:

DDoS (Distributed Denial of Service) is a network attack that disorders and hinders legitimate user requests by flooding the host server with a large number of requests via geographically distributed internet connections employing a collection of zombie computers. DDoS degrades service by causing network congestion and preventing network components from performing their regular activities, which is significantly more disruptive for IoT [9]. The difference between DoS and DDoS is that DDoS uses more than just connecting to the internet to attack the victim, making it difficult to detect and execute through botnets or devices under the attacker's control. botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks. Assembly of a botnet is usually the infiltration stage of a multi-layer scheme. The bots serve as a tool to automate mass attacks, such as data theft, server crashing, and malware distribution.

Botnets use your devices to scam other people or cause disruptions — all without your consent. Whereas DoS is carried out using a script or a DoS tool [10]. DDoS has an impact on all layers of the Open Systems Interconnection (OSI) model, including Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol (FTP), Secure Sockets Layer (SSL), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Code-division multiple access (CDMA), coding, modulation, and transmission medium [5], [11], and [12]. The WSN Dataset (WSN-DS) is usually

used in WS for DoS attack detection and classification. WSN-DS allows numerous intelligence and data mining methodologies to be used for better detection and classification of DoS assaults [13].

Malicious domain:

Malicious domains are considered as the most important resources that adversaries need to carry out operations on the Internet. The Domain Name System (DNS) protocol is a critical component of the Internet. It converts difficult-to-remember Internet Protocol (IP) addresses into simple domain names. When it is compared to other methods, detecting malicious domains through DNS data analysis has a number of advantages. For starters, DNS data makes up a modest portion of overall network traffic, making it appropriate for studying large or small networks that cover different areas. Moreover, it normally helps in reduction of the amount of data to be evaluated, in which the researchers are allowed to investigate DNS traffic to Top Level Domains (TLD). Furthermore, there are useful characteristics in the DNS traffic for specific threat behavior like domain owner, and Autonomous System (AS) number, for this reason traffic if DNS became important to testing the artificial intelligent algorithms to detect the disaster before happening [14].

Malware:

Malware is just malicious code that disguises itself as a helpful piece of software/message/document/data and exploits any and all system weaknesses. Some dangerous programs, such as Trojan horses, spyware, viruses, and rootkits, require the usage of a host application to mask their tracks, whilst others, such as Worms, Automated Viruses, and Zombies (Botnets), live and spread independently. A common malware package now includes a Trojan, Rootkit, Virus, Worm, and Botnet, all packaged together for survival and dissemination, as well as command and control [8], [12].

DISCUSSION

As explained previously, cyber-attacks are performed in different behaviors and can affect the focused target in numerous ways, such as workflow, structure, datasets, and so on. In addition, these attacks work on specific layer of network OSI structure to disturb the performance of such network to produce a fault results. The classification of the most popular attack types is shown in Fig. 2.1, which explains the real effect of such attacks on the whole layer including the adopted protocols. Most of them are acting on the application layer as it is related to data processing and information and provides the users with the final results. The DDoS attacks are different as they are working cross different layers, in which they are nominated to be the most danger cyber-attacks. When the explanation of these attacks is read, a clear idea on each attack behavior is obtained. This leads to build a strong cyber-security system that can detect and predict the attacks in early stages. In addition, numerous solutions can be provided to overcome the losses in the data and information, particularly the real-time systems that have a critical data.

CONCLUSION

An efficient classification to Impact on data in WSN was presented. This classification was performed based on the effects of attacks on layers and related protocols. This study opened the research door for producing active Data security systems that can solve the risky problems of such attacks on the information systems. In addition, detailed information for the most popular attacks was included to give a wide vision for researchers to understand the work steps of them, thoroughly. At the other hand, a discussion was provided to look out on the main points of the included cyber attacks.

REFERENCES

1. *W. Dargie, C. Poellabauer, Fundamentals Of Wireless Sensor Networks: Theory and Practice, WILY, 2010.*
2. *A. Johana, S. Johan, M.T. Portocarrero, "Contrasting Internet of Things and Wireless Sensor Network from a conceptual overview", IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), December 2016, p.p 252-257*
3. *F. Yavuz, "Deep Learning in Cyber Security for Internet of Things", M.Sc. Thesis, Istanbul shehir University, 2018.*
4. *J. Graham, R. Howard, R. Olson, Cyber Security Essentials, Taylor and Francis Group, 2011.*
5. *M. Uma, G. Padmavathi, "A Survey on Various Cyber Attacks and Their Classification", International Journal of Network Security, Vol.15, No.5,September 2013, PP.390-396.*
6. *U. Jain, M. Hussain, " Wireless Sensor Networks: Attacks and Countermeasures", 3rd International Conference on Advances in Internet of Things and Connected Technologies, 2018.*
7. *D. Reed, " Applying the OSI Seven Layer Network Model To Information Security", SANS Institute Information Security Reading Room, November 21, 2003.*
8. *M. Ahemd, M. Shah, Abdul Wahid, " IoT Security: A Layered Approach for Attacks & Defenses", International Conference on Communication Technologies, April 2017, p.p 104 -110.*
9. *C. Zhang, R. Green, " Communication Security in Internet of Thing: Preventive Measure and Avoid DDoS Attack Over IoT Network", SpringSim, January 2015.*
10. *R. Rizal, I. Riadi, Y. Prayudi, " Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) ", International Journal of Cyber-Security and Digital Forensics, September 2018, p.p 382 – 390.*
11. *H. Obaid, E. Abeed, " DoS and DDoS Attacks at OSI Layers", International Journal of Multidisciplinary Research and Publications, Volume 2, Issue 8, 2020, pp. 1-9.*
12. *P. Sinha, A. Rai, V. K. Jha, B. Bhushan, " Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A Survey", International Conference on Signal Processing and Communication, July 2017, p.p 288 – 293.*
13. *T. Huong Le, T. Park, D. Cho, H. Kim, "An Effective Classification for DoS Attacks in Wireless Sensor Networks", IEEE, Tenth International Conference on Ubiquitous and Future Networks (ICUFN), August 2018, p.p 689 – 692.*
14. *Y. Zhauniarovich, I. Khail, T. Yu, "A Survey on Malicious Domains Detection through DNS Data Analysis", Qatar Computing Research Institute, Vol. 51, No. 4, Article 67. July 2018.*
15. *Basagni, S., Conti, M. Giordano, S. Stojmenovic, I. Mobile ad Hoc Networking; John Wiley & Sons: Hoboken, NJ, USA, 2004*