International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

A comprehensive review of attacks on Wireless Sensor Networks

Sravanthi Latha Mangalarapu
Robotic Process Automation (RPA) Developer, Wipro Technologies Ltd,
Gachibowli, India

Abstract

Progresses in sensor time and PC networks have empowered assigned sensor organizations (DSNs) to Advance from little clusters of massive sensors to enormous multitudes of miniature sensors, from steady sensor nodes to mobile nodes, from worried communications to wireless communications, from static local area topology to progressively changing over topology. Each sensor has wireless correspondence ability and some degree of insight for signal handling and systems administration of the information, which persistently gathers the data from the environmental elements and, after some handling, sends them to the base station. The PCs in the base station then, at that point, decipher the information and proposes the ideal activity. Sensor nodes in WSN have their working framework in a Small operating system. Wireless sensor networks are utilized in various applications in various fields.

Keywords: Wireless sensor networks, Distributed sensor networks (DSNs)

I. Introduction

Wireless sensor networks have, as of late, become a force to be reckoned with because they hold the possibility to change many fragments of our economy and life, from natural observing and protection to assembling and business resource the executives to computerization in the transportation and medical services industries[1]. A local sensor area is characterized as a synthesis of a significant assortment of minimal expense, low power multi-deliberate sensor nodes which are enormously distributed either inside the device or exceptionally near it. Nodes can be tiny in size, detecting, records handling, and talking parts. The job of those minuscule nodes need not be outright; this not best offers irregular situations anyway additionally strategy that conventions for sensor organizations and its calculations should have self-coordinating skills in challenging regions. Distributed sensor networks (DSNs) have recently arisen as an entire study area [2]. These commitments, across an immense range of non-military personnel, what's naval force applications, incorporate environmental factors following, scene reconstruction, development following, movement location, front-line reconnaissance, remote detecting, global acknowledgment, and so forth. They're regularly time-basic, cover an immense geological area, and require dependable delivery of exact measurements for their last touch. The final motivation behind DSNs is to decide or benefit information based on the insights melded from appropriate sensor inputs[3]. At the most reduced stage, the man or lady sensor node gathers insights from extraordinary detecting modalities locally available. On the other hand, sensors regularly talk using Wi-Fi networks wherein the local area transfer speed is a reasonable setup decline than wired correspondence. These issues bring new difficulties to the plan of DSNs: First, information

volumes being consolidated are tons more enormous; second, the correspondence transfer speed for the wireless organization is a lot of declines; third, the energy help on every sensor is very bound; fourth, the environmental elements are more prominent untrustworthy, incurring questionable network association and developing the probability of entering information to be in flawed[4].

II. Sensor Network Architecture

DSN can likewise incorporate numerous exceptional kinds of sensors along with seismic, low testing cost attractive, visual, warm, infrared, acoustic, and radar, which may be fit for screening a broad sort of surrounding circumstances. Sensor nodes might be utilized for constant detecting, event location, recognizable proof, and close-by actuators' oversight [5]. Even though smooth for verbal trade, AC shape is expensive to uphold and difficult to increment. Of course, DHC bears the cost of various leveled shapes, otherwise called tree shapes. It most potently allows communications between nodes in abutting layers, presently not inside a similar coating.

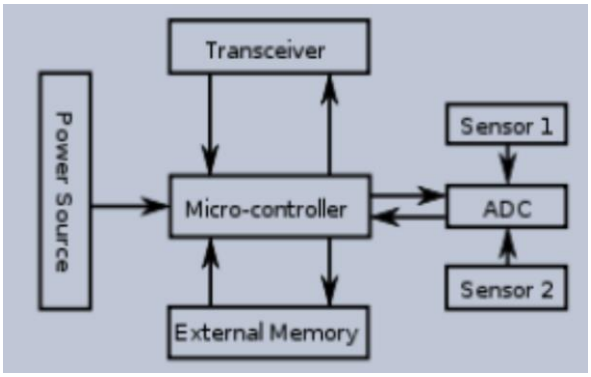

Figure 1: Basic Architecture of Wireless Sensor Node

Sensor nodes are usually designated in a sensor region. Each apportioned node can obtain data and information lower back to the sink and give up clients. Records are returned to the surrender purchaser through a multichip foundation design through the sink [6]. The convention stack consolidates power and steering consideration, incorporates information with systems administration conventions, and imparts power effectively through the wireless medium. The convention stack comprises the product, conveyance, local area, information hyperlink, even layer, control of the board plane, the executive's airplane's portability, and the executive's aircraft. Contingent upon the detecting project, elite kinds of utilizations programming can be developed and used on the programming layer [7]. They may likewise have application-dependent extra parts, for example, tracking down a framework, a power generator, and a mobilizer. Detecting units generally have two subunits: sensors and analog-to-digital converters (ADCs). Given the noticed peculiarity, the analog signs produced by the sensors are switched over entirely to digital signals by the ADC, then taken care of in the handling unit[8]. The handling unit, which is by and large connected with a little storage unit, deals with the systems that make the sensor node cooperative with different nodes to

do the appointed detecting undertakings. A transceiver unit interfaces the node to the network [9].

III. Security Issues In Sensor Networks

Sensor nodes have a few constraints involving battery power, rechargeability, sleep patterns, working memory, transmission range, tamper protection, time synchronization, and unattended activity. A few different controls are connected with the network, for example, Adhoc networking, limited reconfigurations, data rate, packet size, channel error rate, intermittent connectivity, latency, and isolated subgroups.

1. Denial of Service

The inadvertent disappointment delivers denial of Service (DoS) of nodes or atrocity. The most direct DoS attack attempts to deplete the assets accessible to the casualty node by sending extra empty packets and consequently forestalls genuine network clients from getting to services or purchases to which they are entitled [10]. DoS attack is implied not just for the foe's endeavor to undermine, disturb, or obliterate a network yet additionally for any occasion that lessens a network's capability to offer support.

2. Sybil Attack

By and large, the sensors in a wireless sensor network could cooperate to achieve an undertaking. Consequently, they can utilize the conveyance of subtasks and overt repetitiveness of data. In such a circumstance, a node can claim to be more than one node using the characters of other authentic nodes. This kind of attack where a node manufactures the personalities of more than one node is the Sybil attack. Sybil's attack attempts to debase the trustworthiness of information, security, and asset usage that the appropriated calculation endeavors to accomplish. Sybil attack can be performed for attacking the circulated storage, steering system, information conglomeration, casting a ballot, fair asset portion, and misconduct identification. Any peer-to-peer network (particularly wireless Adhoc networks) is helpless against Sybil's attack.

3. Black hole/Sinkhole Attack

In this attack, a malignant node becomes a black hole to draw in all the rush hour gridlock in the sensor network. Particularly in a flooding-based protocol, the attacker pays attention to demands for courses and then, at that point, answers to the objective nodes that contain the terrific or most limited way to the base station [11]. When the vicious gadget has had the option to embed itself between the imparting nodes (for instance, sink and sensor node), it can do anything with the packets passing between them. The protected steering system guarantees a solid node to the base station and the other way around correspondence. They have introduced a triple-key administration plot given two network pre-sent keys, and one group conveyed key. Triple keys moderate the classification and confirmation-related attacks.

IV. Application

1. Home Applications:

Homegrown automation; as age progresses, intelligent sensor nodes and actuators can be covered apparatuses, comprehensive of vacuum cleaners, microwaves, ice chests, and VCRs. Those sensor nodes in the homegrown gadgets can collaborate with an external local area through the net or satellite television for pc[12]. They grant end customers the to oversee homegrown devices locally and somewhat extra without any problem.

2. Fitness Application:

A portion of the projects offer connection points for the disabled; including the patient following; diagnostics; drug the executives in the facility; following the moves and inside the technique for bugs or different little creatures; tele monitoring of human physiological data; and following and monitoring docs and patients internal a wellbeing office[13].

3. Military Applications: Wireless sensor networks might be an essential piece of military order, control, correspondence, registering, knowledge, surveillance, and focused on (C4ISRT) frameworks.

4. Natural applications:

A few natural projects of sensor local area include following the movement of birds, little animals, and bugs; monitoring ecological circumstances that influence yields and livestock; water system; full-scale units for gigantic scope earth monitoring and planetary. Accuracy farming; organic, Earth, and environmental monitoring in marine, soil, and barometrical settings; lush region fire recognition and meteorological and geo substantial examination; flood identification; bio intricacy planning of the environmental factors; contamination study.

V. Conclusion

The primary elements of the wireless sensor network, network protocols, and security parts of WSN. To overcome the disadvantages of AC and DHC, we concentrated on the Level tree wherein nodes of the network are coordinated as many complete paired trees, and the foundations are related. Inside the data handling worldview, we assess two models, client-server form and cell-specialist fundamentally based DSNs. Finishing up the MADNs has higher local area scalability, extensibility, and stability than the buyer server adaptation. The principal challenges in wireless sensor networks are to create proficient and energy-saving steering algorithms and security protocols.

References

1. Vijay Reddy Madireddy, (2017) “Comparative analysis on Network Architecture and Types of Attacks”, 2017 International Journal of Innovative Research in Science, Engineering and Technology” July-2017, pp 20537- 20541
2. Swathi, P. (2022). Industry Applications of Augmented Reality and Virtual Reality. *Journal of Environmental Impact and Management Policy (JEIMP) ISSN: 2799-113X*, *2*(02), 7-11.

3. Vijay Reddy Madireddy (2017), “Analysis on Threats and Security Issues in Cloud Computing”,2017 International Journal of Advanced Research in Electrical, Electronics, and Instrumentation Engineering Feb-2017,pp 1040-1044 .
4. S.Ramana, M.Pavan Kumar, N.Bhaskar, S. China Ramu, & G.R. Ramadevi. (2018). Security tool for IOT and IMAGE compression techniques. Online International Interdisciplinary Research Journal, {Bi- Monthly}, 08(02), 214–223. ISSN Number: 2249-9598.
5. Vijay Reddy Madireddy (2018), “Content-based Image Classification using Support Vector Machine Algorithm”, International Journal of Innovative Research in Computer and Communication Engineering Nov-2018,pp 9017-9020
6. Satya Nagendra Prasad Poloju. ”Relevant Technologies of Cloud Computing System”, Vol. 4, Issue 4, (Version-3, pp. 74-78,) April 2014.
7. Adithya Vuppula.” Communication and Protocols towards IOT-Based Security”, Vol. 3, Issue 10, pp: 17076- 17081October 2014
8. Vijay Reddy, Madireddy (2020), “A Review on architecture and security issues Cloud Computing Services”, Journal For Innovative Development in Pharmaceutical and Technical Science (JIDPTS) Oct-2020,pp 1-4
9. S. Ramana, S. C. Ramu, N. Bhaskar, M. V. R. Murthy and C. R. K. Reddy, "A Three-Level Gateway protocol for secure M-Commerce Transactions using Encrypted OTP," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2022, pp. 1408-1416, doi: 10.1109/ICAAIC53929.2022.9792908.
10. N.Bhaskar, S.Ramana, & M.V.Ramana Murthy. (2017). Security Tool for Mining Sensor Networks. International Journal of Advanced Research in Science and Engineering, BVC NS CS 2017, 06(01), 16–19. ISSN Number: 2319- 8346
11. Karunakar Pothuganti, (2018) ‘A comparative study on position based routing over topology based routing concerning the position of vehicles in VANET’, AIRO International Research Journal Volume XV, ISSN: 2320-3714 April, 2018 UGC Approval Number 63012.
12. Swathi, P. (2019) “A Review on Skin Malanocyte Biology and Development” International Journal of Research in Engineering, Science and Management, Volume-2, Issue-10, October-2019, ISSN (Online): 2581-5792
13. K. Pothuganti, B. Sridevi and P. Seshabattar, "IoT and Deep Learning based Smart Greenhouse Disease Prediction," 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), 2021, pp. 793-799, doi: 10.1109/RTEICT52294.2021.9573794.
14. I. Ahmad and K. Pothuganti, "Smart Field Monitoring using ToxTrac: A Cyber-Physical System Approach in Agriculture," 2020 International Conference on Smart Electronics and Communication (ICOSEC), 2020, pp. 723-727, doi: 10.1109/ICOSEC49089.2020.9215282.
15. Swathi, P. (2022). Implications For Research In Artificial Intelligence. *Journal of Electronics, Computer Networking and Applied Mathematics (JECNAM) ISSN: 2799-1156*, *2*(02), 25-28.
16. Adithya Vuppula. “OPTIMIZATION OF DATA MINING AND THE ROLE OF BIG DATA ANALYTICS IN SDN AND INTRADATA CENTER NETWORKS”, Volume 1, Issue 4,pp: 389-393, April 2016.
17. Satya Nagendra Prasad Poloju.”Privacy-Preserving Classification of Big Data”, Vol.2, Issue 4, page no: 643- 646, April 2013