Big Data and Computing Visions

www.bidacv.com

Big. Data. Comp. Vis. Vol. 2, No. 4 (2022) 149–153.

Paper Type: Original Article

Difference between Domestic and Hostile Applications of Wireless Sensor Networks

Haoran Yu*

School of Economics and Management, China Three Gorges University, China; FaTianYuff@163.com.

Citation:

Yu, H. (2022). Difference between domestic and hostile applications of wireless sensor networks. *Big data and computing visions, 2*(4), 149-153.

Received: 26/02/2022 Reviewed: 01/04/2022 Revised: 09/04/2022 Accept: 01/05/2022

Abstract

Wireless Sensor Networks (WSNs) always have many potential applications and also unique challenges. They usually consist of hundreds or thousands of small sensor nodes such as MICA2, which operate autonomously conditions such as cost, invisible deployment and many application domains, such as lead to small size and limited resources sensors.

Keywords: Wireless sensor network, Security, Link layer, Attacks, Detection, Defensive mechanism.

1 | Introduction

In Wireless Communications (WCs) have enabled the development of low-cost and low power Wireless Sensor Networks (WSNs). Wireless sensor network have many potential applications and unique challenges [1]. They usually heterogeneous systems which contains many small devices, called sensor nodes, that monitoring different environments in cooperative [2]. I.e. sensors cooperate to each other and compose their local data to reach a global view of the environment. Sensor nodes will also operate autonomously [3]. In WSNs there are two other components, such as "aggregation points" and "base stations", which will have more powerful resources than normal sensors [4]. Aggregation points collect information from their nearby sensors, integrate them and then forward to the base stations to process gathered data, WSNs are vulnerable to many types of attacks and due to unsafe and unprotected nature of communication channel untrusted and broadcast transmission media, deployment in hostile environments [5].

Security plays a vital and complex requirement for these networks. It is very necessary to design an appropriate security mechanism for these networks, which attending to be WSNs constraints [6]. This security mechanism should cover different security dimension of WSNs, include confidentiality, integrity, availability and authenticity [7]. The main purpose of this paper is presenting an overview of different link layer attacks on WSNs and comparing them together [8]. The sensor's components are sensor unit, processing unit, storage or memory unit, power supply unit and wireless radio transceiver, these units are communicating to each other [9]. The existing components on WSN's

Corresponding Author: FaTianYuff@163.com

http://doi.org/10.22105/bdcv.2022.331569.1051

architecture are including sensor nodes (motes or field devices that are sensing data), network manager, security manager, aggregation points, base stations (access point or gateway) and user/human interface. Besides, there are two approaches in WSN's communication models containing hierarchical WSN versus distributed and homogeneous WSN versus heterogeneous [10].

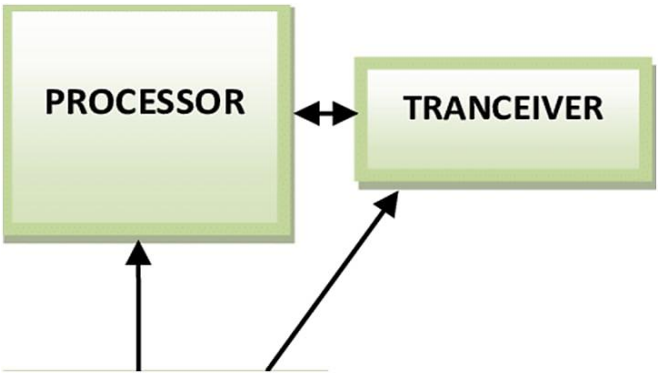

Fig. 1. Communication between processor and tranceiver.

2 | Literature Review

We can render any standard model capable of solving multiple tasks in various application domains. A literature review or narrative review is a type of review article. A literature reviews is a scholarly paper, which includes the current knowledge including substantive findings, as well as theoretical and methodological contributions to a particular topic [11].

Advantage

I. It is scalable and hence can accommodate any new nodes or devices at any time [12].
II. It is flexible and hence open to physical partitions [13].
III. All the WSN nodes can be accessed through centralized monitoring system [14].
IV. As it is wireless in nature, it does not require wires or cables [15].

3 | Working of Hostile Environment

A hostile work environment may also be created when management acts in a manner designed to make an employee quit in retaliation for some action. A hostile work environment exists when one's behaviour within a workplace creates an environment that is difficult for another person to work in small issues, annoyances, and isolated incidents typically are not considered to be illegal [6]. To be unlawful, the conduct must create a work environment that would be intimidating, hostile, or offensive to a reasonable person. An employer can be held liable for failing to prevent these workplace conditions, unless it can prove that it attempted to prevent the harassment and that the employee failed to take advantage of existing harassment counter-measures or tools provided by the employer [17].

For example, if an employee reported safety violations at work, was injured, attempted to join a union, or reported regulatory violations by management, and management's response was to harass and pressure the employee to quit [18]. Employers have tried to force employees to quit by imposing unwarranted discipline, reducing hours, cutting wages, or transferring the complaining employee to a distant work location [19]. Thus, federal law does not prohibit simple teasing, offhand comments, or isolated incidents that are not extremely serious [20]. Rather, the conduct must be so objectively offensive as to alter the conditions of the individual's employment. The conditions of employment are altered only if the harassment culminates in a tangible employment action or is sufficiently severe or pervasive [21].

Yu| Big. Data. Comp. Vis. 2(4) (2022) 149-153

4 | Domestic Environment

The term 'domestic environmental experience' was defined as users' experiences of cognitive perceptions and physical responses to their domestic built environments [22]. Domestic environments can be enriched through the implementation of Environmental Experience Design (EXD) by combining users' environmental, spatial and contextual factors that may accommodate occupants' needs and demands as well as their health and wellbeing [23]. Here, an EXD theoretical concept has been developed based on the 'User-Centred Design' thematically framework [15].

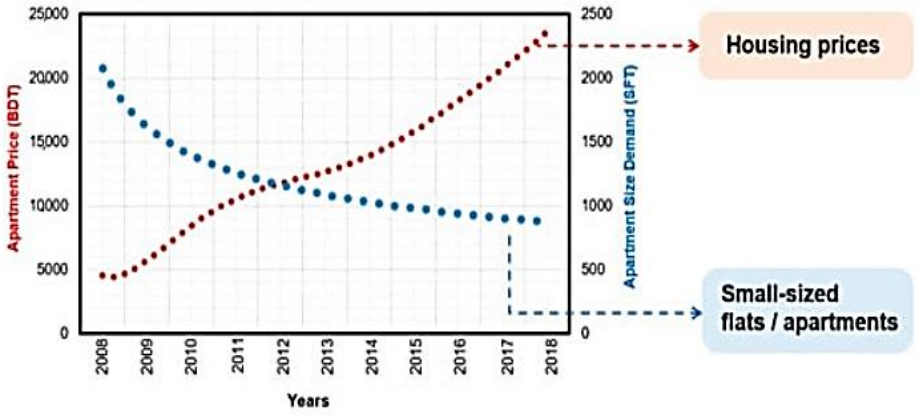

Fig. 2. Domestic environment.

5 | Detailing with Hostile Environment

The first step is to address the conduct with the proper authorities at your job. If this is not possible, or if you have tried it and the situation did not change, the next option may be litigation. An employment attorney in your area can help you fight to stop the behavior and receive compensation. If your workplace has become discriminatory and hostile, you do not have to suffer alone [16]. Technically, a hostile work environment is a workplace in which the conduct of supervisors or co-workers has created a discriminatory environment that a reasonable person would find so abusive or intimidating that it impacts the ability to work. If you are wondering whether your current work conditions could be considered a hostile work environment, continue reading for a list of requirements and examples [17]. Sometimes, people use the term "hostile work environment" in reference to nearly any unpleasant work situation: A rude boss, obnoxious co-workers, an unpleasant office or lack of benefits. It's true that these issues can make a work environment very undesirable, but they do not necessarily meet the legal definition of a hostile environment [18].

Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signals are converted into electrical signals. It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source. It receives the data which is sent by the Radio nodes wirelessly, generally through the internet. The data received by the WLAN Access Point is processed by software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

WSNs have grown substantially over the years and have a momentous potential in diverse applications in areas of environmental science, medical sciences, telecommunications, education services, agriculture, surveillance, military services, etc it has been reported that notwithstanding the influential capabilities of WSNs, their effective development is still somehow stimulating and challenging. Presently, in deploying WSNs, some programming procedures have been anticipated, which emphasis mostly on issues of Low-Level-Based (LLB) systems. some of the primary applications and values, structures in WSNs project, developments and challenges drawn from some evidence and meta-data-based survey and assessments,

which is anticipated to serve as an introduction on the applications and challenges of WSNs for persons interested in WSNs.

Fig. 3. A survey of wireless sensor networks.

This is a WSN or Wireless Computer Network (WCN) that links or connects two or more devices by means of WC to form a LAN within a restricted location such as a computer research laboratory, household, institution, or workplace. This gives users the capability to move from place to place within the said location and remain connected or linked to the WN. Wireless LAN could also offer a connection to the wider cyberspace (internet) through a gateway. Most contemporary wireless LANs are based on the standards of IEEE 802.11 and are marketed under the Wi-Fi product designation. Wireless LANs have become prevalent for use in the several households, as a result of their ease of installation and use. They are also prevalent in commercial physiognomies that offer wireless access to their workforces and clients.

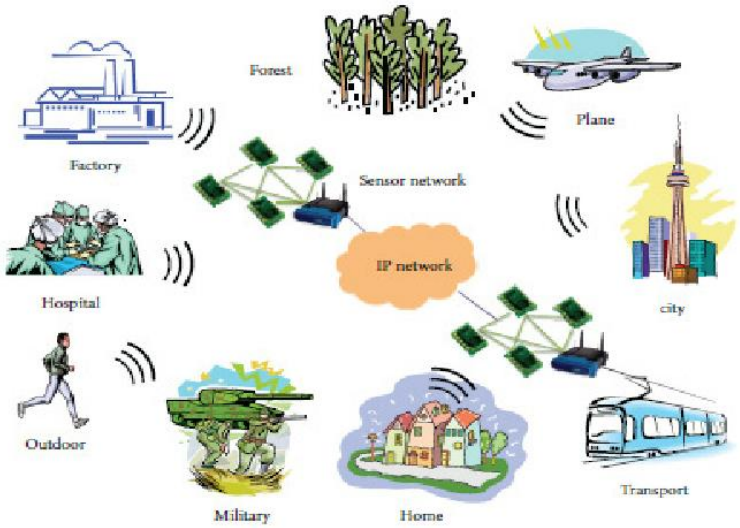

Fig. 4. Application area of wireless network sensors.

6 | Conclusion

My conclusion is that, these networks always works on a small batteries for days, months, and even years depending on the requirements of monitored applications. These networks experience threats at various layers and, as such, are vulnerable to a wide range of attacks. The proposed scheme, also known as payload-based mutual authentication for WSNs, operates in 2 steps. First, an optimal percentage of cluster heads is elected, authenticated, and allowed to communicate with neighbouring nodes. Second, each cluster head, in a role of server, authenticates the nearby nodes for cluster formation.

References

[1] Mohapatra, H., & Rath, A. K. (2020). Fault-tolerant mechanism for wireless sensor network. *IET wireless sensor systems*, *10*(1), 23-30.

[2] Mohapatra, H., & Rath, A. K. (2019). Fault tolerance in WSN through PE-LEACH protocol. *IET wireless sensor systems*, *9*(6), 358-365.

[3] Mohapatra, H., & Rath, A. K. (2019). Detection and avoidance of water loss through municipality taps in India by using smart taps and ICT. *IET wireless sensor systems*, *9*(6), 447-457.

[4] Mohapatra, H., & Rath, A. K. (2020). Survey on fault tolerance-based clustering evolution in WSN. *IET networks*, *9*(4), 145-155.

[5] Mohapatra, H., & Rath, A. K. (2021). Fault tolerance in WSN through uniform load distribution function. *International journal of sensors wireless communications and control*, *11*(4), 385-394.

[6] Mohapatra, H., & Rath, A. K. (2020, October). Nub less sensor based smart water tap for preventing water loss at public stand posts. *2020 IEEE microwave theory and techniques in wireless communications (MTTW)* (Vol. 1, pp. 145-150). IEEE.

[7] Mohapatra, H., & Rath, A. K. (2022). IoE based framework for smart agriculture. *Journal of ambient intelligence and humanized computing*, *13*(1), 407-424.

[8] Mohapatra, H., & Rath, A. K. (2021). A fault tolerant routing scheme for advanced metering infrastructure: an approach towards smart grid. *Cluster computing*, *24*(3), 2193-2211.

[9] Mohapatra, H., & Rath, A. K. (2021). An IoT based efficient multi-objective real-time smart parking system. *International journal of sensor networks*, *37*(4), 219-232.

[10] Mohapatra, H., & Rath, A. K. (2019). Fault tolerance through energy balanced cluster formation (EBCF) in WSN. In *Smart innovations in communication and computational sciences* (pp. 313-321). Springer, Singapore.

[11] Panda, H., Mohapatra, H., & Rath, A. K. (2020). WSN-based water channelization: an approach of smart water. In *Smart cities—opportunities and challenges* (pp. 157-166). Springer, Singapore.

[12] Mohapatra, Hitesh; Rath, Amiya Kumar: 'IoT-based smart water' [Control, Robotics & Sensors, 2020], 'IoT Technologies in Smart Cities: From sensors to big data, security and trust', Chap. 3, pp. 63-82, DOI: 0.1049/PBCE128E_ch3, IET Digital Library.

[13] Mohapatra, H. (2021, September). Socio-technical challenges in the implementation of smart city. *2021 international conference on innovation and intelligence for informatics, computing, and technologies (3ICT)* (pp. 57-62). IEEE.

[14] Mohapatra, H. (2020). Offline drone instrumentalized ambulance for emergency situations. *IAES international journal of robotics and automation*, *9*(4), 251-255.

[15] Mohapatra, H., & Rath, A. K. (2020). *Fundamentals of software engineering: designed to provide an insight into the software engineering concepts*. BPB Publications.

[16] Mohapatra, H. (2021). *Designing of fault tolerant models for wireless sensor network* (Doctoral Dissertation, Ph. D Dissertation, Veer Surendra Sai University of Technology). Retrieved from http://hdl.handle.net/10603/333160

[17] Mohapatra, H., & Rath, A. K. (2020). Social distancing alarming through proximity sensors for COVID-19. *Easy chair*, *18*. https://wvvw.easychair.org/publications/preprint_download/dMGk

[18] Mohapatra. H. (2021). Smart city with wireless sensor network, ISBN-13: 979-8791261380, KDP, 2021.

[19] Mohapatra, H. (2018). *C Programming: practice.cpp*. Independently Publisher.

[20] Mohapatra, Hitesh; Rath, Amiya Kumar, 'Smart Bike Wheel Lock for Public Parking', Application Number: 336834-001.

[21] Mohapatra, H., & Rath, A. K. (2020). Advancing generation Z employability through new forms of learning: quality assurance and recognition of alternative credentials. DOI: 10.13140/RG.2.2.33463.06560

[22] Mohapatra, H. (2009). *HCR using neural network* (PhD's Desertion, Biju Patnaik University of Technology). Retrieved from https://www.academia.edu/29846341/HCR_English_using_Neural_Network

[23] Mohapatra, H. (2019). *Ground level survey on sambalpur in the perspective of smart water* (No. 1918). Retrieved from https://easychair.org/publications/preprint/CWpb