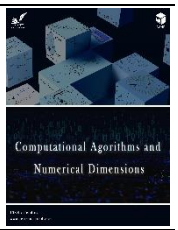
Computational Algorithms and Numerical Dimensions

www.journal-cand.com

Com. Alg. Num. Dim Vol. 1, No. 3 (2022) 104–109.



Paper Type: Original Article

Application on Wireless Sensor Networks in Domestic and Hostile Environment

Lu Fan*

Beijing Technology and Business University, China; 1150837457@qq.com.

Citation:

Fan, L. (2022). Application on wireless sensor networks indomestic and hostile environment. *Computational algorithms and numerical dimensions, 1*(3), 104-109.

Received: 26/02/2022 Reviewed: 26/03/2022 Revised: 01/04/2022 Accept: 24/04/2022

Abstract

Wireless Sensor Networks (WSNs) have many potential applications and unique challenges. They usually consist of hundreds or thousands small sensor nodes such as MICA2 which operate autonomously conditions such as cost invisible deployment and many application domains, lead to small size and limited resources sensors. WSNs are susceptible to many types of link layer attacks and most of traditional networks security techniques are unusable on WSNs due to wireless and shared nature of communication channel, untrusted transmissions, deployment in open environments, unattended nature and limited resources. So, security is a vital requirement for these networks; but we have to design a proper security mechanism that attends to WSN's constraints and requirements. In this paper, we focus on security of WSNs, divide it (the WSNs security) into four categories and will consider them, include: an overview of WSNs, security in WSNs, the threat model on WSNs, a wide variety of WSNs' link layer attacks and a comparison of them. This work enables us to identify the purpose and capabilities of the attackers; also, the goal and effects of the link layer attacks on WSNs are introduced. Also, this paper discusses known approaches of security detection and defensive mechanisms against the link layer attacks; this would enable it security managers to manage the link layer attacks of WSNs more effectively.

Keywords: Wireless sensor network, IoT, Smart home.

1 | Introduction

Advances in wireless communications have enabled the development of low-cost and low power Wireless Sensor Networks (WSNs) [1]. WSNs have many potential applications, and unique challenges. They usually are heterogeneous systems contain many small devices, called sensor nodes, that monitoring different environments in cooperative; i.e. sensors cooperate to each other and compose their local data to reach a global view of the environment; sensor nodes also can operate autonomously [2]. In WSNs there are two other components, called "aggregation points" and "base stations" which have more powerful resources than normal sensors [3]. Aggregation points collect information from their nearby sensors, integrate them and then forward to the base stations to process gathered data, as shown in *Fig. 1*.

Licensee **Computational Algorithms and Numerical Dimensions.** This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0).

Corresponding Author: 1150837457@qq.com

https://doi.org/10.22105/cand.2022.161800

Limitations such as cost, invisible deployment and variety application domains, lead to requiring small size and limited resources (like energy, storage and processing) sensors [4]. Also, 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 automated nature and limited resources, the most of security techniques of traditional networks [5].

International journal on applications of graph theory in wireless ad hoc networks and sensor networks, March 2011 36 are impossible in WSNs; therefore, security is a vital and complex requirement for these networks [6]. It is necessary to design an appropriate security mechanism for these networks [7], which attending to be WSN's constraints. This security mechanism should cover different security dimension of WSNs, include confidentiality, integrity, availability and authenticity [8]. The main purpose of this paper is presenting an overview of different link layer attacks on WSNs and comparing them together. In this paper, we focus on security of WSNs and classify it into four categories, as follows:

2 | An Overview of WSNs

Security in WSNs includes security goals, security obstacles and security requirements of WSNs [9]. The threat model on WSNs.

A wide variety of WSN's link layer attacks and comparison them to each other, include classification of WSN's link layer attacks based on threat model and compare them to each other based on their goals, results, strategies, detection and defensive mechanisms [10]. This work makes us enable to identify the purpose and capabilities of the attackers; also, the goal, final result and effects of the attacks on the WSNs [11]. We also state some available approaches of security detection and defensive mechanisms against these attacks to handle them [12].

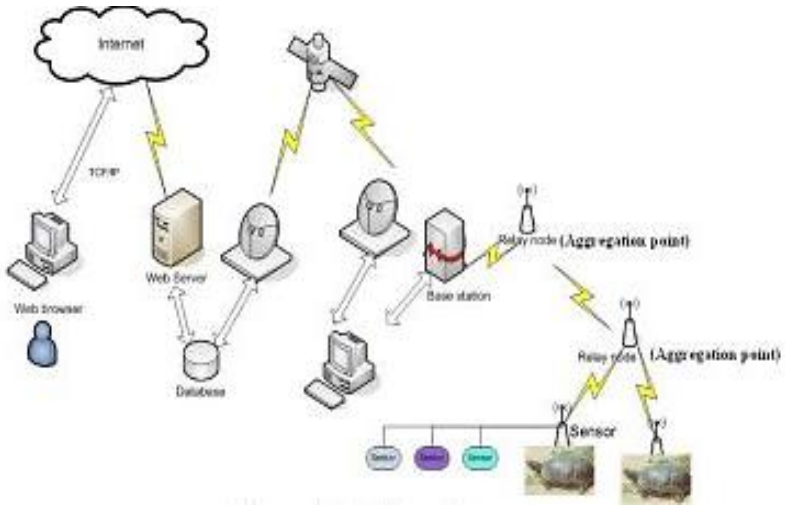


Fig. 1. WSN's architecture.

Common functions of WSNs are including broadcast and multicast, routing, forwarding and route maintenance [13]. The sensor's components are: sensor unit, processing unit, storage/memory unit, power supply unit and wireless radio transceiver; these units are communicating to each other, as shown in [14]. The existing components on WSN's 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 [15]. Besides, there are two approaches in WSN's communication models containing hierarchical WSN versus distributed and homogeneous WSN versus heterogeneous. Some of common suppositions of these networks are:

- *Insecure radio links.*
- *Packet injection and replay.*
- *Non tamper resistant.*
- *Many normal sensor nodes (high-density) and low malicious nodes.*
- *Powerful attackers (laptop-class).*

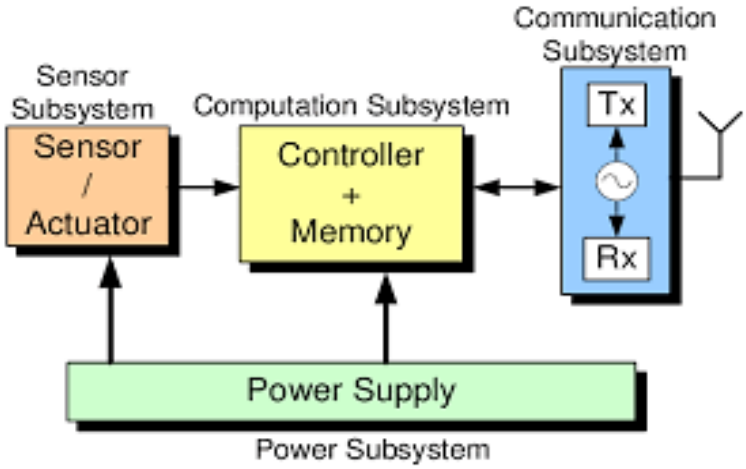


Fig. 2. WSN node architecture.

3 | Literature Survey

WSN's applications

In general, there are two kinds of applications for WSNs including, monitoring and tracking therefore, some of most common applications of these networks are: military, medical, environmental monitoring industrial, infrastructure protection disaster detection and recovery, agriculture, intelligent buildings, law enforcement, transportation and space discovery [16].

Fig. 2. WSN node applications.

Security in WSNS

Now, intrusion techniques in WSNs are growth; also there are many methods to disrupt these networks [17]. In WSNs, data accuracy and network health are necessary; because these networks usually use on confidential and sensitive environments [18]. There are three security key points on WSNs, including

Fan| Com. Alg. Num. Dim. 1(3) (2022) 104-109

system (integrity, availability), source (authentication, authorization) and data (integrity, confidentiality) [19]. Necessities of security in WSNs are:

I. Correctness of network functionality.
II. Unusable typical networks protocols.
III. Limited resources.
IV. Untrusted nodes.
V. Requiring trusted centre for key management to authenticating nodes to each other preventing from existing attacks and selfishness and extending collaboration [20].
VI. Security services: There are many security services on WSNs; but some of their commons are including encryption and data link layer authentication multi-path routing identity verification, bidirectional link verification and authenticated broadcasts [21].
VII. Security protocols: section presents the most common security protocols of WSNs, containing.
VIII. SNEP: Secure network encryption this protocol (secure channels for confidentiality, integrity by using authentication, freshness) [22].
IX. μTESLA (Micro timed, efficient, streaming, loss-tolerant authentication protocol, authentication by using asymmetric authenticated broadcast) [23].

4 | Proposed Work

Sensor Protocols for Information via Negotiation (SPIN)

The idea behind SPIN is to name the data using high-level descriptors or meta-data. Before transmission, metadata are exchanged among sensors via a data advertisement mechanism, which is the key feature of SPIN. Each node upon receiving new data, advertises it to its neighbours and interested neighbours, i.e. those who do not have the data, retrieve the data by sending a request message. There is no standard meta-data format and it is assumed to be application specific. There are three messages defined in SPIN to exchange data between nodes, include: ADV message to allow a sensor to advertise a particular meta-data, REQ message to request the specific data and DATA message that carry the actual d. Broadcasts of end-to-end encrypted packets (authentication, integrity, confidentiality, and replay).

In WSNs that consist of a large number of low-power, short-lived, unreliable sensors, one of the main design challenges is to obtain long system lifetime, as well as maintain sufficient sensing coverage and reliability. In this paper, we propose a node-scheduling scheme, which can reduce system overall energy consumption, therefore increasing system lifetime, by turning off some redundant nodes. Our coverage-based off-duty eligibility rule and back off-based node-scheduling scheme guarantees that the original sensing coverage is maintained after turning off redundant nodes. We implement our proposed scheme in NS-2 as an extension of the LEACH protocol. We compare the energy consumption of LEACH with and without the extension and analyse the effectiveness of our scheme in terms of energy saving.

In Right to be Hostile, scholar and activist Erica Meiners offers concrete examples and new insights into the "school to prison' pipeline phenomenon, showing how disciplinary regulations, pedagogy, pop culture and more not only implicitly advance, but actually normalize an expectation of incarceration for urban youth. Analyzed through a framework of an expanding incarceration nation, Meiners demonstrates how educational practices that disproportionately target youth of colour become linked directly to practices of racial profiling that are endemic in state structures. As early as preschool, such educational policies and practices disqualify increasing numbers of students of colour as they are funnelled through schools as under-educated, unemployable, 'dangerous,' and in need of surveillance and containment. By linking schools to prisons, Meiners asks researchers, activists, and educators to consider not just how our schools' physical structures resemble prisons— metal detectors or school uniforms— but the tentacles in policies, practices and informal knowledge that support, naturalize, and extend, relationships between incarceration and schools. Understanding how and why prison expansion is possible necessitates connecting schools to prisons and the criminal justice system, and redefining "what counts" as educational policy.

Proximity detection is defined as the capability of a Location-Based Service (LBS) to automatically detect when a pair of mobile targets approaches each other closer than a pre-defined proximity distance. For realizing this function the targets have to be permanently tracked. To this end they are equipped with a cellular mobile device with an integrated GPS receiver, which passes position fixes obtained by GPS to a central location server. In order to save valuable bandwidth, reduce monetary costs for bearer services and to limit the power consumption at the mobile device, the number of messages exchanged between server and device needed for keeping track of the target should be reduced as far as possible. In the paper a novel strategy for efficient proximity detection is presented, which is based on an adoption of dead reckoning. In contrast to existing work the strategy considers the movement patterns of the observed targets. The paper presents results that have been achieved in various simulations comparing the proposed strategy to known approaches with regard to the amount of messages that pass the air interface. Also, it is described how proximity detection interplays with related functions like clique and k-nearest-neighbour detection. Therefore, the layered architecture of the LBS middleware framework TraX is presented, which has a special focus on community-LBS.

We describe the design and implementation of a running system for energy-efficient surveillance. The system allows a group of cooperating sensor devices to detect and track the positions of moving vehicles in an energy-efficient and stealthy manner. We can trade off energy-awareness and surveillance performance by adaptively adjusting the sensitivity of the system. We evaluate the performance on a network of 70 MICA2 motes equipped with dual-axis magnetometers. Our results show that our surveillance strategy is adaptable and achieves a significant extension of network lifetime. Finally, we share lessons learned in building such a complete running system.

5 | Conclusion

Security is a vital requirement and complex feature to deploy and extend WSNs in different application domains. The most security link layer attacks are targeting network security dimensions such as integrity, confidentiality, authenticity and availability. In this paper, we analyse different dimensions of WSN's security, present a wide variety of WSNs' link layer attacks and classify them; our approach to classify and compare the WSN's link layer attacks based on different extracted features of WSN's link layer, attacks' and attackers' properties, such as the threat model of WSNs, link layer attacks' nature, goals and results, their strategies and effects and finally their associated detection and defensive techniques against these attacks to handle them, independently and comprehensively.

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, H., & Amiya Kumar, R. (2020). '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