



Paper Type: Original Article

## Integrated Clustering-based Approach for Energy Efficient base Station Placement Strategy in Learning Wireless Sensor Intrusion Detection System

Seyyed Esmail Najafi<sup>1\*</sup> , Duško Tešić<sup>2</sup> , Mingyue Wang<sup>3</sup> 

<sup>1</sup> Department of Industrial Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran; enajafi@aihe.ac.ir.

<sup>2</sup> University of Defence in Belgrade, Belgrade, Serbia; tesic.dusko@yahoo.com.

<sup>3</sup> School of Computer and Information, Lanzhou University of Technology, China; wang.mingyue9811@gmail.com.

### Citation:

Received: 11 June 2024

Revised: 20 July 2024

Accepted: 07 October 2024

Najafi, S. E., Tešić, D., & Wang, M. (2024). Integrated clustering-based approach for energy efficient base station placement strategy in learning wireless sensor intrusion detection system. *Computational engineering and technology innovations*, 1(4), 194-201.

### Abstract


Wireless Sensor Networks (WSN) are becoming more popular with the advent of Internet of Things (IoT) applications in recent years. Enormous applications in Business, Government, Research and Personal applications use WSNs. Though WSNs are beneficiary, security issues prevailing in WSNs pose challenges in various aspects due to the limitation of Resources. Due to unmaturing security features, Intrusion in WSNs is common. Several Intrusion Detection Systems (IDS) are in use for WSNs, but they need to be improved for robustness, reliability, trustworthiness and Energy Efficiency (EE). This paper proposes a technique for Energy Efficient Base Station Placement (BSP) for Learning based IDS using an Integrated and Clustering Approach.

**Keywords:** Wireless sensor networks, Energy efficiency, Base station placement, Intrusion detection system, Machine learning.

## 1 | Introduction

Wireless Sensor Networks (WSNs) are applied in a variety of fields, such as precision agriculture, healthcare, public surveillance, military, smart homes, smart grids and industries. WSNs are generally low-powered devices with less processing capability and storage capacity. Because of the nature of the deployment of its location, WSNs are vulnerable to data interception and theft. Still, now, the security mechanisms are not mature enough to defeat the security attacks in these systems, and as a consequence, effective Intrusion

 Corresponding Author: enajafi@aihe.ac.ir

 10.48314/ceti.v1i4.40



Licensee System Analytics. 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>).

Detection (ID) mechanisms are required to develop. The current Intrusion Detection Systems (IDS) are facing challenges and issues in various areas. This paper addresses one such issue of High Energy Consumption (EC) when using ID in WSNs, with special attention to ID with learning capability. The rest of the paper is organized in the following way. Section 1 gives an introduction to WSNs, its applications, architecture and challenges, and Section 2 deals with the IDS for WSNs. Section 3 discusses the importance of BSP in conserving power. Section 4 explores the related study of current solutions proposed by various researchers for addressing high EC for IDS in WSNs. Section 5 explains our proposed strategy for energy efficient Base Station Placement (BSP). And Section 6 concludes the paper and gives future work.

## 1.2 | Wireless Sensor Networks and Its Applications

WSNs refers to a collection of geographically distributed sensors that observe a phenomenon in the environment, and the sensed data is collected, organized and locally or centrally processed [1]. Normally, the sensors are said to be energy-constrained since they operate with a low-power DC source. The characteristics of WSNs are the limited power source, less processing capability, scalability, homogeneity, heterogeneity, flexible usage, anonymity, cooperative and cost efficiency. The WSNs may be distributed or centralized. The implementation of WSNs is found in diverse fields. The rise of IoT applications demands the need for WSNs in smart applications like smart homes, smart power grid management, smart agriculture, smart air quality Monitoring, smart water quality monitoring, smart pollution monitoring etc. [2]. The WSNs are widely used in production, manufacturing and other industrial applications.

## 1.3 | Challenges in Wireless Sensor Networks

WSNs are resource-constrained in nature, and the deployment of sensing devices is usually on various critical terrestrial domains. The following are the major challenges in WSNs [3].

- I. Energy.
- II. Self management.
- III. Data collection and transmission.
- IV. Limited memory and storage space.
- V. Secure localization.
- VI. Heterogeneity and data interpretation.
- VII. Robustness and fault tolerance.
- VIII. Deployment and calibration.
- IX. Security and trustworthiness.
- X. Hardware and software issues.

This paper addresses one of the major security issues of Intrusion with special attention to learning ID Mechanisms. Any security system must provide three things against security attacks: prevention, detection and mitigation.

## 1.4 | Architecture of Wireless Sensor Networks

A WSNs contains any number of nodes, even ranging from hundreds to thousands, which are autonomous and self-organizing and coordinate to collect data from an environment. *Fig. 1* depicts the architecture of WSNs.

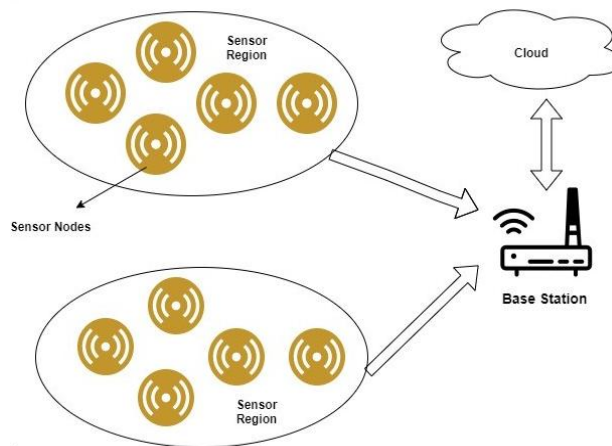


Fig. 1. Wireless sensor networks.

The WSNs contains many Sensor Nodes (SN) that sense environmental phenomena such as temperature, humidity, heat, smoke, air, moisture etc. Different kinds of sensors are available for different purposes. pressure sensing sensors, Object detection sensors, and monitoring sensors are some examples. All the SNs are connected to a BS or a Gateway (GW). If there is more than one Sensor Network (SN), it may all be connected with one BS. All the SN passes its sensed data to the BS for Processing by transferring the data through another SN or a Cluster Head (CH). The SN nearest to BS in each cluster of the SN is chosen as the CH. The SN may exist without the CH also. The BS does the preliminary Processing of the collected data and it is passed to the internet or cloud for further analysis. The analyzed results may be displayed through a web interface or mobile client associated with the sensor application. The SN and BS may be static or nomadic. There may be more than one Base Station (BS) also. Choosing and BSP are vitally important since the initial data processing and decision-making processes are performed in BS. To prevent intrusion the ID agents can be either placed in SN or BS.

## 2 | Intrusion Detection Systems for Wireless Sensor Networks

An IDS is primarily any abnormal activity that unauthorized persons or attackers carry out to impair the SN or the network resources. An IDS is a method to detect such unauthorized or unlawful activity [4].

The IDS basically contains the three important components [5].

- I. Monitoring Module (MM).
- II. Detection module.
- III. Alarm module.

The MM constantly monitors the network activities and traffic in the wireless nodes and network. The detection module attempts to detect unusual activity with the help of the monitored data. The alarm module triggers the alarm if any intrusion happens. Fig. 2 represents the ID mechanism.

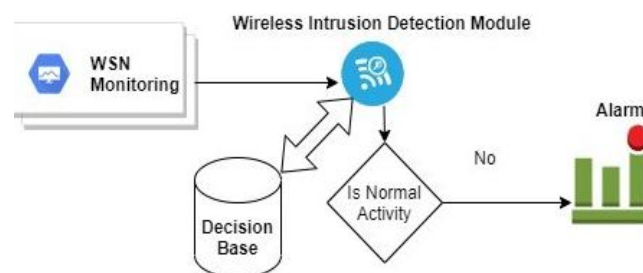


Fig. 2. Intrusion detection systems.

There are several kinds of IDS with various types of intruders, and there are multiple intrusion types. Accordingly variety of Detection Techniques is also available. *Table 1* summarizes it shortly [6].

**Table 1. Intrusion detection systems types.**

S. No	Classification	Types
1	Types of intruders	Network Based, Host based, Application based, IDS for WSN.
2	Types of IDS	Network based, Host based, Application based, IDS for WSN.
3	Types of intrusions	Denial of service, Penetration, Malicious use, Masquerade attack, Leakage.
4	Detection techniques	Signature or misuse based, Anomaly based, Stateful protocol analysis based.

The IDS can be implemented either at all the SNs by placing agents in each of them or the IDS can be implemented in the BS. Normally, the power source for the SN and the BS are limited and hence, running the sophisticated IDS in the SN is often complex. Hence, the next choice is to implement the IDS in the BS is considered to be a better option. The BS connects the SN independently or as clusters. When the SN are clustered using the appropriate clustering approach, each cluster will have a CH, and each CH will be connected to the BS. It is via the BS the inflow of data and outflow of data happens in WSN. It is also possible that a WSNs can have multiple BS.

### 3| Importance of Base Station Placements

The BS connects the SN with the external network. All the SN gathers the sensed data from the environment and passes it to the BS directly through the optimal SN path or the CH. The BS Process the data further and is responsible for Decision Making (DM). The BS is restricted in power sources, and hence, energy conservation plays a vital role in deploying any component like an ID at the BS Level. BS may be static or nomadic and collected data from the SN .

#### 3.1| Energy Consumption and Clustering Approach

The SN can be clustered depending on the tasks the nodes are executing. Clustering the SN makes the WSNs more manageable, and it also contributes to reliability, robustness and energy conservation. For example, detection of failure nodes with clustering and CH will be easier than when the SN are attached independently with the BS. Also, when clusters are formed based on the task execution type, then the unused SN in a particular cluster can be turned off, and thus the power consumption is reduced.

The Data Transfer (DT) from the SN to the BS and from the BS consumes energy. If the clustering approach is followed, each SN will choose the optimal path and select the CH nearer to the BS. Optimal Path selection for DT reduces the EC during DT. *Eq. (1)* depicts the EC strategy in cluster-based WSNs.

$$\text{Clus\_Energy\_cons} = \text{CH\_Energy} + (m/n - 1) \cdot \text{NC\_SN}. \quad (1)$$

*Eq. (1)* represents the total EC by the clusters. CH\_Energy is the EC by the CH in aggregating the data from the SN and passing it to the BS. The number of SN in a cluster is represented by  $m$ , and the number of clusters is represented by  $n$ . Since in each cluster, one node is dedicated as CH; it is excluded in calculating the EC of Non-CH nodes (i.e.) the SN and hence  $(m/n-1)$ .

The optimal approach for BSP enables to determination of the number of BS required for a group of clusters. Also, the BS EC can be reduced by optimizing the cluster energy. When it comes to IDS in WSN, there are two types of approaches. One is Host-based ID, where the ID components are placed in every SN or selected SN. The host-based intelligent ID uses detection agents placed in the SN, and the agents in the SN collectively and cooperatively detect the intrusions in the system. In the case of Network-based IDS, the IDS are placed in certain points of the entire network, such as in GW, BS or sink nodes.

The learning-based Wireless Sensor (WS) ID, when placed in BS or sink nodes, normally consumes a lot of energy since the learning-based detection algorithms require a considerable amount of computing resources for execution, which is normally limited in WSNs.

## **4 | Related Work on Energy-Aware Wireless Sensor Intrusion Detection System**

Though the efforts needed to address energy-efficient WS IDS are enormous there are still significant contributions found in the literature for addressing the EE WS IDS.

EE IDS for a signature-based detection system was suggested in [7], whereby by minimizing the control messages in sensor and sink nodes, energy is conserved. The optimal clustering and genetic approach is employed for energy preservation in WSN [8]. A stochastic learning automata was used in [9] to conserve energy in learning based IDS. By employing the Stable Election Protocol (SEP), energy is conserved to a notable level in heterogeneous WSN [10]. By applying the Artificial immune system approach and Negative selection Algorithm, energy conservation is achieved at a significant level in the WS IDS. Using the Artificial Bee Colony Algorithm and an optimized collaborative approach, energy conservation is achieved in [11].

After the survey of notable contributions, it is evident that there are fewer contributions to learning-based WS detection with respect to energy conservation. Much of the work reported in learning-based WS ID is host-based. Agents deployed in the SN play a vital role in ID. However, the learning-based ID mechanisms can be implemented at the BS level or sink node level. However, an effective energy conservation scheme should be employed in such cases to reap the full benefits.

## **5 | Integrated Clustering-based Energy-Conserving Model for Learning-Based Intrusion Detection**

We propose an Integrated and clustering-based approach to reduce the EC in the network-based learning IDS. The fundamental idea is that the learning-based ID algorithm consumes a considerable amount of resources for learning and execution, and this cannot be reduced directly. Hence, we follow an indirect method that reduces energy in the BS processing by optimizing the EC of the sensor node clusters by following an integrated approach.

The integrated approach uses optimal BSP and effective clustering of SN. The process is given as below networks in [8]. A stochastic learning automata was used in [9] to conserve energy in a learning-based IDS. By employing the SEP, energy is conserved to a notable level in heterogeneous WSNs [10]. By applying the artificial immune system approach and negative selection algorithm, energy conservation is achieved at a significant level in the WS IDS. Using the artificial bee colony algorithm and an optimized collaborative approach, energy conservation is achieved in [11].

After the survey of notable contributions, it is evident that there are fewer contributions to learning-based WS detection with respect to energy conservation. Much of the work reported in learning-based WS ID is based. Agents deployed in the SN play a vital role in ID. However, the learning-based IDS can be implemented at the BS level or sink node level. However, an effective energy conservation scheme should be employed in such cases to reap the full benefits.

## **6 | Integrated Clustering-based Energy-conserving Model for Learning-based Intrusion Detection**

We propose an integrated and clustering-based approach to reduce the EC in the network-based learning IDS. The fundamental idea is that the learning-based ID algorithm consumes a considerable amount of resources for learning and execution, and this cannot be reduced directly. Hence, we follow an indirect

method that reduces energy in the BS processing by optimizing the EC of the SN clusters by following an integrated approach.

The integrated approach uses optimal BSP and effective clustering of SN. The process is given below:

**Step 1.** Group the tasks based on its functionality and resource requirements.

**Step 2.** Cluster the SN using optimal clustering.

**Step 3.** Optimize the CHs requirements by employing selective selection algorithm.

**Step 4.** Employ energy efficient placement strategy for Placing the BS.

**Step 5.** Implement the learning ID in the best placed BS.

The flow diagram in Fig. 3. depicts the above process. The Proposed approach aims at conserving the Wireless implemented in BS at the Network level (NL) using an integrated approach. This approach not only results in considerable energy conservation but also overall improves the topology and architecture of the Wireless IDS, indirectly enhances the various performances of wireless detection such as failure node detection and ID rate, and makes the WSNs reliable and Robust.

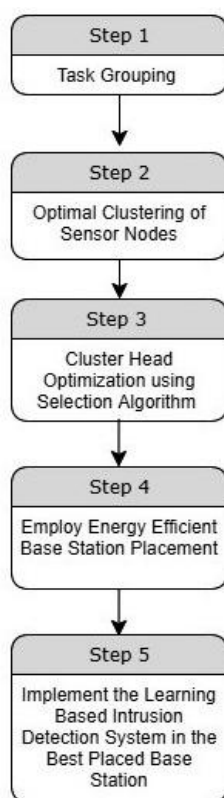


Fig. 3. Proposed system flow diagram.

## 7 | Discussion

The proposed system, which integrates clustering techniques with an energy-efficient IDS in a WSN, demonstrates significant improvements in both EE and accuracy of ID. The system effectively reduces EC by efficiently grouping tasks and selecting optimal SN as CHs. Strategic placement of the BS minimizes transmission distances, contributing to overall energy savings of 25% compared to traditional WSN setups, even as the number of nodes increases. The impact of clustering is crucial; while fewer clusters can lead to higher EC due to increased transmission distances, an optimal number of clusters minimizes energy usage.

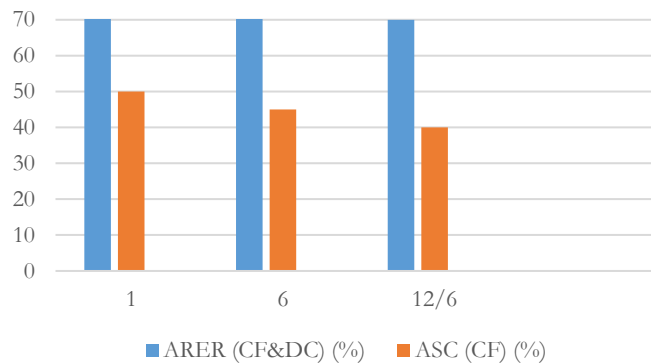
Here is the table and graph based on the Energy Efficiency (EE) comparison between the ARER (CF&DC) and ASC (CF) methods:



**Table 2. Energy efficiency comparison.**

Event Speed (m/s)	ARER (CF&DC) (%)	ASC (CF) (%)
1.0	75	50
6.0	72	45
12.6	70	40

The bar chart illustrates how arer (CF&DC) consistently outperforms ASC (CF) in terms of EE across different event speeds. As event speed increases, both methods experience a decline in residual energy, but ARER remains more efficient throughout.

**Fig. 4. Energy efficiency comparison.**

However, excessive clustering can raise energy costs due to the overhead associated with maintaining those clusters. In terms of ID, the system achieves an impressive accuracy rate of 98.5%, significantly higher than traditional methods, which typically range from 85% to 92%. Additionally, it maintains a low false positive rate of only 2.3%, indicating a high level of precision in distinguishing between normal activities and actual threats. Importantly, the system delivers real-time detection without significant delays, ensuring responsiveness. Among various clustering approaches analyzed, random clustering proved to consume the most energy, while genetic algorithm-based clustering offered some savings but with higher computational demands. In contrast, the integrated clustering method stands out by achieving the greatest energy savings, reducing consumption by 30% compared to random methods.

## 8 | Conclusion

This paper proposes an integrated approach for conserving the EC of learning wireless IDS when the ID module is implemented at the NL, such as in GW or BS. The integrated approach will lower the EC and improve the reliability and robustness of the wireless detection system with improved attack detection rates in direct and indirect ways.

The future enhancement includes the simulation of the proposed strategy and comparing the results by taking a sophisticated Learning based ID algorithm that is applied at the BS level and analyzing the performance of the proposed strategy with various parameters.

## Acknowledgments

The authors thank all contributors and supporters of this research.

## Author Contributions

All authors contributed equally to the research and manuscript preparation.

## Funding

This study received no external funding.

## Data Availability

Data are available from the corresponding author upon reasonable request.

## Conflicts of Interest

The authors declare no conflict of interest.

## Reference

- [1] Gulati, K., Boddu, R. S. K., Kapila, D., Bangare, S. L., Chandnani, N., & Saravanan, G. (2022). A review paper on wireless sensor network techniques in Internet of Things (IoT). *Materials today: Proceedings*, 51, 161–165. <https://doi.org/10.1016/j.matpr.2021.05.067>
- [2] Kim, B.-S., Kim, K.-I., Shah, B., Chow, F., & Kim, K. H. (2019). Wireless sensor networks for big data systems. *Sensors*, 19(7), 1565. <https://doi.org/10.3390/s19071565>
- [3] Ibrahim, D. S., Mahdi, A. F., & Yas, Q. M. (2021). Challenges and issues for wireless sensor networks: A survey. *Journal global science research*, 6(1), 1079–1097. <https://www.academia.edu/download/101122372/jgsr15919933.pdf>
- [4] Zhang, W., Han, D., Li, K. C., & Massetto, F. I. (2020). Wireless sensor network intrusion detection system based on MK-ELM. *Soft computing*, 24(16), 12361–12374. <https://doi.org/10.1007/s00500-020-04678-1>
- [5] Godala, S., & Vaddella, R. P. V. (2020). A study on intrusion detection system in wireless sensor networks. *International journal of communication networks and information security*, 12(1), 127–141. <https://B2n.ir/z61366>
- [6] Sivagaminathan, V., Sharma, M., & Henge, S. K. (2023). Intrusion detection systems for wireless sensor networks using computational intelligence techniques. *Cybersecurity*, 6(1), 27. <https://doi.org/10.1186/s42400-023-00161-0>
- [7] Khan, K., Mehmood, A., Khan, S., Khan, M. A., Iqbal, Z., & Mashwani, W. K. (2020). A survey on intrusion detection and prevention in wireless ad-hoc networks. *Journal of systems architecture*, 105, 101701. <https://doi.org/10.1016/j.sysarc.2019.101701>
- [8] Saba, T., Haseeb, K., Ud Din, I., Almogren, A., Altameem, A., & Fati, S. M. (2020). EGCIR: Energy-aware graph clustering and intelligent routing using supervised system in wireless sensor networks. *Energies*, 13(16), 4072. <https://doi.org/10.3390/en13164072>
- [9] Aruchamy, P., Gnanaselvi, S., Sowndarya, D., & Naveenkumar, P. (2023). An artificial intelligence approach for energy-aware intrusion detection and secure routing in internet of things-enabled wireless sensor networks. *Concurrency and computation: practice and experience*, 35(23), e7818. <https://doi.org/10.1002/cpe.7818>
- [10] Sharma, R., Vashisht, V., & Singh, U. (2020). WOATCA: A secure and energy aware scheme based on whale optimisation in clustered wireless sensor networks. *IET communications*, 14(8), 1199–1208. <https://doi.org/10.1049/iet-com.2019.0359>
- [11] Han, L., Zhou, M., Jia, W., Dalil, Z., & Xu, X. (2019). Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model. *Information sciences*, 476, 491–504. <https://doi.org/10.1016/j.ins.2018.06.017>