Concept Paper

Not peer-reviewed version

Smart Presence Detection: Harnessing Wi-Fi Signals and Machine Learning with ESP8266

Rehan Khan * and Danish Khan

Posted Date: 19 June 2024

doi: 10.20944/preprints202406.1346.v1

Keywords: Presence Detection; Wi-Fi Signals; ESP8266; Signal Interference; Smart home automation

doi:10.20944/preprints202406.1346.v1

Concept Paper

Smart Presence Detection: Harnessing Wi-Fi Signals and Machine Learning with ESP8266

Rehan Khan * and Danish Khan

Oriental Institute of Science and Technology, Bhopal; khandanish040196@gmail.com
* Correspondence: dayel.rehan@gmail.com

Abstract: Presence detection is essential in many applications, including smart homes, office automation, and public space management. Traditional technologies like infrared sensors and cameras frequently encounter obstacles due to privacy concerns, high costs, and complexity. The study provides a novel way to detect presence based on Wi-Fi signals and machine learning algorithms, utilizing the ESP8266 microcontroller. The suggested system attempts to reliably detect the presence of people in a given place by evaluating fluctuations in Wi-Fi signal strength and patterns. The theoretical basis of this strategy is investigated, including the ESP8266's capabilities for Wi-Fi data gathering and the use of machine learning methods for data analysis. The methodology includes data collecting with the ESP8266, preprocessing, feature extraction, and training and evaluating machine learning models. This system's potential uses include smart home automation, office occupancy tracking, and crowd management in public settings. The paper also discusses potential issues such as signal interference, data privacy concerns, and the limitations of Wi-Fi detection. Future work is also mentioned, including the suggested system's installation and testing and enhancement proposals to improve accuracy and scalability. This research aims to provide a cost-effective, non-intrusive, and scalable presence detection system by harnessing the power of Wi-Fi signals and machine learning, enhancing intelligent environments.

Keywords: presence detection; Wi-Fi signals; ESP8266; signal interference; smart home automation

---

1. Introduction

Presence detection systems play a crucial role in modern smart environments, enabling applications in home automation, office space management, and public area optimization. These systems enhance security, optimize energy usage, and improve user convenience by detecting human presence and responding accordingly. Traditional methods, such as infrared sensors, cameras, and RFID systems, have limitations, including privacy concerns, high costs, and deployment complexities.

Infrared sensors detect body heat, making them suitable for motion detection but restricted by obstructions and limited range. Cameras offer comprehensive monitoring but raise privacy issues and require sophisticated image processing. RFID systems provide accurate detection and tracking but involve high costs and logistical challenges, requiring users to carry tags. [1]

Despite advancements, there is a need for a cost-effective, non-intrusive, and easily deployable presence detection system. This necessity drives the exploration of alternative approaches leveraging ubiquitous technologies already present in most environments, such as Wi-Fi.

This paper proposes a novel presence detection system that utilizes Wi-Fi signals and machine learning, leveraging the ESP8266 microcontroller. Ubiquitous in modern environments, Wi-Fi signals provide a rich data source for analyzing variations in signal strength and patterns to detect human presence without additional hardware beyond existing Wi-Fi infrastructure.

The primary objective is theoretically exploring the feasibility and potential of Wi-Fi-based presence detection using the ESP8266 and machine learning algorithms. We will discuss the ESP8266's data collection capabilities, data preprocessing and feature extraction methodologies, and the application of various machine learning models for data analysis. Additionally, we will examine potential applications, challenges, and limitations and propose future research directions.

 doi:10.20944/preprints202406.1346.v1

2. Literature Review

The utilization of Wi-Fi signals for presence detection has garnered significant interest in recent years. Various studies have demonstrated the feasibility of using Wi-Fi channel state information (CSI) and received signal strength indicator (RSSI) to detect motion and presence. Recent research has shown the potential of Wi-Fi signals for presence detection. Liu (2020, 2022) [2] and Zubow [3] have all explored the use of Wi-Fi signals, mainly channel state information (CSI), for this purpose. Liu's work focuses on deep learning, while Zubow's approach utilizes a One-Class Support Vector Machine (OC-SVM). Both studies have achieved high accuracy in presence detection. Juki'c et al., [4] have advanced this field by using Wi-Fi signals to detect the presence and accurately count the number of people in a given area. These studies collectively highlight the promising potential of Wi-Fi signals for presence detection and the various methods that can be employed to achieve this.

J. Soto's paper [5] introduces a novel device-free presence detection method utilizing Wi-Fi Channel State Information (CSI) combined with the Dynamic Time Warping (DTW) algorithm. This approach leverages the variations in Wi-Fi signals caused by human movement to detect presence without requiring individuals to carry any device. The DTW algorithm effectively identifies temporal patterns associated with human activity by analyzing the CSI data, enabling accurate presence detection. Soto's method demonstrates competitive accuracy compared to existing technologies, highlighting its potential as a non-intrusive and efficient alternative. This technique capitalizes on the ubiquitous nature of Wi-Fi infrastructure, offering a cost-effective solution for presence detection in innovative environments without additional hardware.

The ESP8266 microcontroller has emerged as a popular choice in the Internet of Things (IoT) domain due to its low cost, power efficiency, and integrated Wi-Fi capabilities. Numerous IoT applications have employed the ESP8266 for data collection and transmission, from environmental monitoring to home automation, demonstrating its versatility and reliability. The microcontroller's ability to interface with various sensors and its programmable nature make it a suitable candidate for developing a Wi-Fi-based presence detection system.

Recent advances in deep learning have shown significant promise in enhancing passive RF sensing using Wi-Fi signals for human presence detection. Yang Liu et al., [6] demonstrated that deep learning-based approaches could achieve near-perfect accuracy in detecting human presence by leveraging the detailed information in Wi-Fi Channel State Information (CSI). Unlike traditional methods that often rely on dedicated hardware such as cameras or infrared sensors, deep learning models can exploit the ubiquitous nature of Wi-Fi signals to perform non-intrusive presence detection. These models can learn complex patterns and features from the RF signals corresponding to human movement and presence, offering superior performance even in challenging environments with significant signal interference and multipath effects. By training neural networks on large datasets of Wi-Fi CSI, these systems can accurately differentiate between occupied and unoccupied states, making them a viable and promising alternative to existing detection methods. This approach reduces the need for additional sensors and preserves privacy, as it does not require visual or audio data. The work by Liu et al. thus underscores the potential of deep learning to transform passive RF sensing into a highly reliable and efficient technology for smart environments.

Carlos M. et al., [7] propose a non-intrusive human presence detection methodology leveraging Channel State Information (CSI) from 802.11n wireless networks, achieving an impressive average accuracy of over 90%. This technique utilizes the detailed signal characteristics provided by CSI to detect human presence without additional sensors or devices, making it a cost-effective and efficient solution for smart environments. In a related study, Wenda Li et al., [8] compare the effectiveness of passive Wi-Fi radar (PWR) and CSI-based wireless sensing (SENS) systems in detecting human activity. The findings indicate that SENS systems offer superior performance in line-of-sight (LOS) conditions due to their ability to capture fine-grained signal variations. In contrast, PWR systems excel in non-line-of-sight (NLOS) environments where direct signal paths are obstructed. These insights

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 19 June 2024 doi:10.20944/preprints202406.1346.v1

underscore the versatility and potential of CSI-based approaches in various deployment scenarios, highlighting their applicability in residential and commercial settings.

While existing research provides valuable insights, several gaps remain. Most studies focus on controlled environments, with limited exploration of real-world scenarios where signal interference and environmental variability can impact performance. Additionally, the integration of machine learning algorithms with low-cost microcontrollers like the ESP8266 remains underexplored. Comprehensive studies are needed to address the challenges of deploying such systems in diverse environments and evaluate their scalability and robustness.

This research proposal aims to bridge these gaps by developing a theoretical framework for a Wi-Fi-based presence detection system using the ESP8266 and machine learning techniques. The proposed approach will investigate the integration of signal processing and machine learning algorithms on the ESP8266 platform, exploring supervised and unsupervised learning methods. The research will address real-world deployment challenges, including signal interference, environmental variability, and scalability considerations.

3. Background

3.0.1. Wi-Fi Fundamentals

Wi-Fi, an acronym for Wireless Fidelity, is a technology that facilitates wireless connectivity and communication among devices. It allows electronic gadgets to access the internet or exchange data with one another without the need for physical wired connections. Wi-Fi functions within the unlicensed radio frequency (RF) bands, commonly operating in the 2.4 and 5 GHz ranges. It facilitates data communication by leveraging radio waves to transmit and receive information. Wi-Fi employs Orthogonal Frequency-Division Multiplexing (OFDM), which involves splitting the available bandwidth into multiple subcarriers. This approach enables parallel data transmission across these subcarriers, enhancing achievable data rates compared to traditional single-carrier transmission methods. Wi-Fi signals, generated by routers and smartphones, propagate through space and interact with the environment, resulting in signal strength and quality variations. The Received Signal Strength Indicator (RSSI) and Channel State Information (CSI) are two critical properties of Wi-Fi signals relevant to presence detection. RSSI is a simple measurement that reflects the overall power level of the received Wi-Fi signal, reported in decibel-milliwatts (dBm). It indicates the signal strength a device receives from a Wi-Fi access point (router). Conversely, CSI provides detailed information about the characteristics of the communication channel between a transmitter and receiver. It captures the signal strength, phase shift, and fading experienced on each subcarrier, making it more sensitive to environmental changes than RSSI. This sensitivity allows for finer-grained analysis of movement and presence detection. Every Wi-Fi connection experiences changes in the signal as it travels from the transmitter to the receiver, influenced by factors like distance, obstacles, and objects in the environment. CSI measurements capture these changes, enabling more accurate detection of environmental variations and presence monitoring compared to RSSI alone.

3.1. Impact of Human Presence on CSI and RSSI

When an individual enters a Wi-Fi zone, their presence disrupts the typical signal propagation. The human body is a substantial obstacle, causing the Wi-Fi signal to reflect and scatter in various directions.[9] This alteration in the signal path from the router to the receiver is captured by the Channel State Information (CSI). CSI provides detailed information on how the signal strength (amplitude) and timing (phase) change on different subcarriers due to reflections and scattering caused by the person's presence. These changes create a unique "fingerprint" in the CSI data, distinguishable from an empty room. [10] On the other hand, the Received Signal Strength Indicator (RSSI) offers a more straightforward representation. It merely indicates the overall strength of the received signal. If the person obstructs the direct path, the signal weakens, resulting in a lower RSSI value. However, RSSI is less sensitive to presence detection because factors such as furniture or electronic devices can also attenuate the signal strength.

Table 1 compares two different signal measurement techniques, Channel State Information (CSI) and Received Signal Strength Indicator (RSSI), regarding their impact on various features related to wireless signal analysis and device presence detection.

Table 1. CSI vs RSSI.

Feature	**Impact on CSI**	**Impact on RSSI**
Mechanism	Reflection and scattering of signal	Signal blockage
Information Captured	Detailed changes in amplitude & phase on each subcarrier	Overall received signal strength
Sensitivity to Presence	More sensitive, specific patterns emerge	Less sensitive, influenced by other factors
Reliability for Presence Detection	More reliable for accurate detection	Less reliable due to susceptibility to noise

3.2. ESP8266 Capabilities

The ESP8266 is a highly integrated Wi-Fi System on Chip (SoC) designed for Internet of Things (IoT) applications. It offers a complete and self-contained Wi-Fi networking solution capable of hosting applications or offloading Wi-Fi functions to another processor. Compliant with IEEE 802.11 b/g/n standards, the ESP8266 provides robust and reliable Wi-Fi connectivity. It can operate as a station, soft access point, or both, making it versatile for various IoT use cases. Featuring a 32-bit RISC CPU running at up to 160 MHz, the ESP8266 has sufficient processing power for primary signal processing tasks and lightweight machine learning models. One of its key capabilities is monitoring the Received Signal Strength Indicator (RSSI) of a Wi-Fi signal from a nearby router. A significant drop in RSSI may occur if a person obstructs the direct path between the router and the ESP8266. The proposed system's ESP8266 bridges the Wi-Fi environment and machine learning processing unit. It captures the Wi-Fi signal strength data and transmits it to the machine learning model for presence detection. The proposed method takes advantage of the ESP8266's wireless communication features and computational capabilities to provide an economical and discreet solution for detecting the presence of individuals or objects. This approach finds applications within the Internet of Things (IoT) realm in diverse scenarios. [11]

3.3. Machine Learning

Channel State Information (CSI) provides granular data on channel properties, including the amplitude and phase of individual subcarriers. In contrast, the Received Signal Strength Indicator (RSSI) represents the overall signal strength. Machine learning algorithms analyze the collected CSI and RSSI data to identify patterns and signatures indicating individuals' presence or absence. [12] These algorithms learn from labelled training data consisting of CSI and RSSI samples gathered in scenarios with and without people present. During the training process, the algorithms discover subtle changes in signal characteristics caused by human presence or motion. After training, the machine learning model can be deployed on devices like the ESP8266 to continuously monitor wireless signals and make real-time predictions about the presence or absence of individuals. The proposed system can detect human presence without needing dedicated sensors by leveraging CSI and RSSI data and machine learning techniques.

4. Proposed System

The proposed system design for Wi-Fi-based presence detection combines the ESP8266 microcontroller and machine learning techniques to create an efficient and scalable solution. The ESP8266, a low-cost and low-power Wi-Fi-enabled microcontroller, is the primary hardware component, cap-

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 19 June 2024 doi:10.20944/preprints202406.1346.v1

turing Wi-Fi signal variations that indicate the presence or absence of individuals in a given space. To collect the necessary data, the ESP8266 is configured to extract Channel State Information (CSI), which provides detailed insights into the Wi-Fi channel characteristics. This process involves using customized firmware to enable CSI extraction and continuously monitoring and recording CSI data. The raw data is then preprocessed to remove noise and normalized for consistency. The final trained model can be deployed on the ESP8266 or a central server for real-time presence detection. It is a practical solution for various applications, including smart homes, offices, and public spaces. A visual representation of the proposed system is shown in Figure 1.

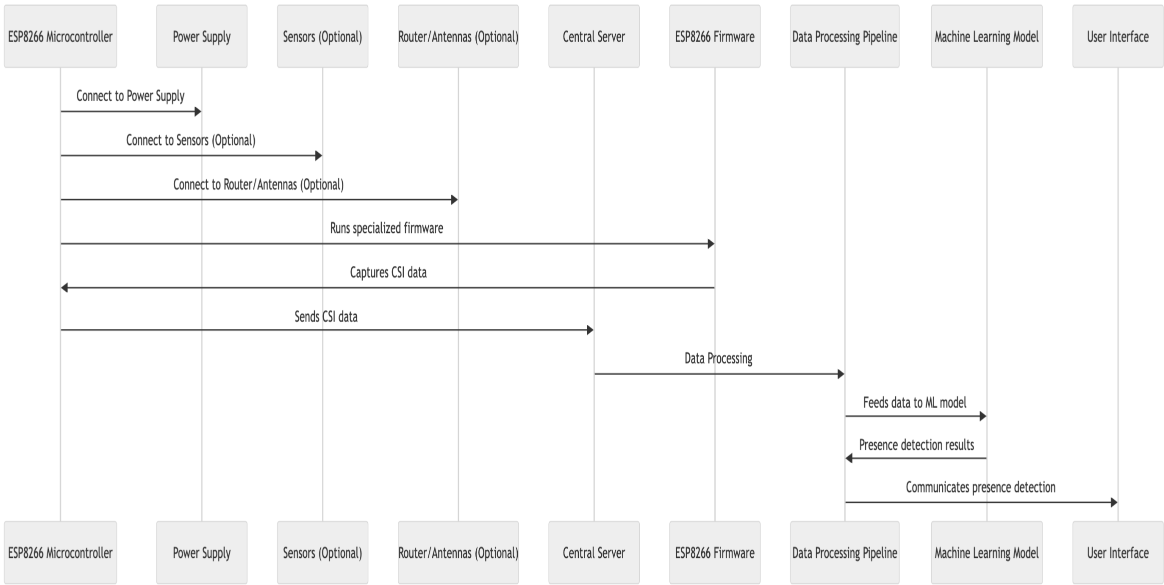

Figure 1. Architecture of Proposed System.

4.1. Capturing CSI and RSSI Data with ESP8266

Capturing Channel State Information (CSI) data using the ESP8266 involves configuring the microcontroller with specialized firmware like Espressif's ESP8266_NONOS_SDK [13]. This firmware enables the ESP8266 to extract detailed Wi-Fi signal characteristics. Once configured, the ESP8266 continuously monitors the Wi-Fi channel, recording CSI data from incoming packets. CSI data provides insights into the signal's amplitude and phase across different subcarriers, reflecting its interaction with the environment. The captured CSI data can be stored locally on the ESP8266 or transmitted to a central server for analysis, leveraging the ESP8266's efficient Wi-Fi capabilities for reliable data transfer.

4.2. Feature Extraction from Collected Data

Feature extraction is critical in converting raw CSI data into meaningful inputs for machine learning models. This process begins with preprocessing, where noise reduction techniques, such as moving average filtering, are applied to smooth out the data, and normalization scales the CSI values to a standard range. Statistical features, such as mean, variance, skewness, and kurtosis, are then extracted to summarize the distribution of the CSI data. Additionally, time-domain features capture temporal patterns, including the rate of change, autocorrelation, and cross-correlation of the data. Frequency-domain features are derived by performing Fourier Transform, identifying dominant frequencies and power spectral density. To reduce dimensionality and retain the most significant components, Principal Component Analysis (PCA) is applied, making the data more manageable and highlighting key patterns related to presence detection.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 19 June 2024 doi:10.20944/preprints202406.1346.v1

4.3. Machine Learning Algorithms for Presence Detection

Several machine learning algorithms are suitable for analyzing the extracted features to detect presence. Support Vector Machines (SVMs) are effective for binary classification tasks, finding the optimal hyperplane that separates presence and absence states. K-Nearest Neighbors (KNN) classifies data points based on their proximity to labelled examples, offering simplicity and robustness, especially when the decision boundary is non-linear. Decision Trees and Random Forests create tree-like models that make decisions based on feature values. Random Forests improve accuracy through ensemble learning. Neural Networks, intense learning models, excel at capturing complex relationships in large and high-dimensional datasets like Channel State Information (CSI) data, providing powerful tools for presence detection. The suitability of machine learning algorithms varies based on several factors. The intricacy of the data, the computational resources, and the desired balance between precision and interpretability play crucial roles in determining the appropriate algorithm. Some algorithms excel in handling complex data but may require substantial computational power, while others prioritize interpretability over accuracy. A thorough assessment and comparative analysis of different algorithmic approaches is essential to identify the most fitting solution for the problem.

4.4. Training the Machine Learning Model

The machine learning model training begins with collecting labelled Channel State Information (CSI) data corresponding to known presence and absence states. This involves setting up controlled environments where human presence is systematically recorded alongside CSI data. The dataset is then split into training, validation, and test sets to ensure the model's generalizability and prevent overfitting. Relevant features are extracted from the labelled CSI data and used to train the selected machine learning algorithm. The model's parameters are optimized to minimize prediction errors. Validation is performed using the validation set to fine-tune hyperparameters and enhance performance. Cross-validation techniques are employed to ensure the model's robustness. The model's performance is evaluated on the test set using metrics such as accuracy, precision, recall, and F1 score. Once validated, the trained model can be deployed on the ESP8266 or a central server, enabling real-time presence detection based on CSI data analysis.

5. Challenges and Limitations

5.1. Signal Interference

Wi-Fi-based presence detection systems face a significant challenge due to signal interference. Wi-Fi signals are susceptible to various forms of interference, including other wireless devices, physical obstructions, and environmental factors like temperature and humidity. Signal quality can degrade significantly in high-density Wi-Fi environments, leading to inaccurate presence detection. Additionally, physical obstacles such as walls, furniture, and human bodies cause multipath effects, where the signal takes multiple paths to reach the receiver, complicating the analysis. Effectively managing and mitigating these interferences is crucial for ensuring reliable performance of the presence detection system.[14]

5.2. Data Privacy Concerns

Leveraging Wi-Fi signals for presence detection introduces significant privacy implications. As these signals can be captured and analyzed to infer human presence and movement, there exists a risk of misuse if the data is not adequately safeguarded. Ensuring compliance with privacy regulations and implementing robust encryption and anonymization techniques are crucial to protecting user privacy. Furthermore, it is essential to maintain transparency by informing users about the data collection process and obtaining their consent. This approach mitigates potential privacy breaches, and fosters trust in the system's deployment and operation.

 doi:10.20944/preprints202406.1346.v1

5.3. Limited Range and Resolution

Wi-Fi signals have a limited effective range, typically up to 100 meters in open spaces. The Wi-Fi standard being used is a key determinant of the range. [15] Newer standards like 802.11ax (Wi-Fi 6) have a longer range than older standards like 802.11b/g/n. 802.11ax can provide a range of up to 230 feet (70 meters) indoors and 820 feet (250 meters) outdoors. However, this range can be significantly reduced by obstacles, posing a challenge for presence detection systems that rely on a single ESP8266 device to monitor large or complex environments. Additionally, Wi-Fi-based detection often lacks the resolution of dedicated sensors like cameras or infrared detectors. While the system can detect presence and movement, it may struggle to distinguish between multiple individuals or detect fine-grained activities within the monitored area.

5.4. Computational Constraints

The ESP8266 microcontroller, although versatile and cost-effective, possesses limited computational resources compared to more powerful processors. Executing complex machine learning algorithms on the ESP8266 can be challenging due to its constrained processing power, memory, and storage capacity [16]. This limitation necessitates the use of lightweight algorithms and efficient data processing techniques. Offloading data processing to a central server may be required in specific scenarios, introducing additional complexities in data transmission and real-time analysis.

5.5. Environmental Variability

The performance of Wi-Fi-based presence detection systems can be influenced by environmental variability. Environmental changes, such as furniture movement or opening and closing doors and windows, can alter Wi-Fi signal characteristics, potentially leading to false positives or negatives. Regular system calibration and adaptation to account for such changes are essential to maintain accuracy. Developing robust algorithms adapting to dynamic environments remains a crucial challenge.

5.6. Energy Consumption

While the ESP8266 is designed for low power consumption, continuous monitoring and data transmission can still result in significant energy use, especially in battery-powered deployments. Optimizing the power management of the ESP8266 and implementing energy-efficient data collection and processing methods are essential to prolong the system's operational life. Strategies such as duty cycling, where the device periodically enters a low-power sleep mode, can help mitigate energy consumption issues.

5.7. Scalability

Scaling the presence detection system to cover large or multiple areas poses additional challenges. Integrating multiple ESP8266 devices and ensuring seamless data collection and processing requires careful network management and synchronization. Moreover, as the number of devices increases, so does the potential for signal interference and data congestion, which can degrade the system's performance. Developing scalable architectures and protocols that efficiently handle large deployments is critical for broader system applications.

The successful deployment and operation of a Wi-Fi-based presence detection system using the ESP8266 and machine learning hinges on overcoming several challenges and limitations. Ongoing research and development efforts are essential to enhance the system's reliability, accuracy, and scalability. The proposed approach can be effectively implemented and optimized for real-world scenarios by addressing these issues.

6. Future Work

To further advance this technology, we identify critical areas for future research and development.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 19 June 2024 doi:10.20944/preprints202406.1346.v1

6.1. Expanding Coverage and Resolution

Future research could explore deploying a network of ESP8266 devices to overcome the range and resolution limitations to cover more significant, more complex environments. Developing seamless handoff and coordination algorithms among multiple devices could ensure continuous coverage without blind spots. Furthermore, integrating the system with high-resolution sensors like cameras or LiDAR [17] could enhance its ability to distinguish between various individuals and detect fine-grained activities. Investigating techniques like using directional antennas or beamforming could also improve spatial resolution. The system's capabilities could be significantly enhanced for real-world deployment in various scenarios by addressing these limitations.

6.2. Enhancing Computational Efficiency

Considering the computational limitations of the ESP8266, future research should focus on optimizing machine learning algorithms for resource-constrained environments. Developing lightweight models that offer high accuracy with minimal computational overhead is crucial. Techniques like model pruning, quantization, and edge computing could enhance the system's efficiency. Furthermore, exploring hybrid approaches where initial processing occurs on the ESP8266 and more complex analysis is offloaded to a central server could be beneficial. The proposed Wi-Fi-based presence detection system can be made more practical and feasible for real-world deployment by addressing these aspects.

6.3. Adapting to Dynamic Environments

Future research should prioritize enhancing the system's adaptability to dynamic environments. Developing self-learning algorithms capable of continuous adaptation to environmental changes, such as furniture rearrangement or door movements, is crucial. Reinforcement learning techniques could enable the system to learn from its surroundings and improve performance. Implementing regular calibration procedures and developing adaptive algorithms to handle real-world variability will significantly enhance the system's robustness and reliability.

6.4. Energy Optimization

Future research should prioritise energy optimisation techniques for battery-powered ESP8266 prioritize to achieve optimisation viability. Developing more efficient power management strategies like duty cycling and energy-efficient data transmission protocols could significantly extend battery life. Exploring energy harvesting technologies, like solar power, to supplement the power supply of these devices is another promising avenue. Optimizing the firmware to reduce energy consumption without compromising performance will be crucial. Researchers should focus on developing algorithms and protocols that balance energy efficiency and operational requirements, ensuring reliable and sustainable operation in resource-constrained environments.

6.5. Integration with Other Smart Systems

Future research could explore integrating Wi-Fi-based presence detection systems with other smart systems, such as heating, ventilation, air conditioning (HVAC), lighting, and security. This integration could enable comprehensive and intelligent smart environments where the presence of data optimizes energy usage, enhances security and improves user comfort. Developing standardised protocols and application programming interfaces (APIs) for interoperability with other smart devices and platforms is essential for creating cohesive and efficient intelligent environments. Addressing these areas in future research will help overcome current challenges and limitations, enhancing the capabilities and applications of Wi-Fi-based presence detection systems. Building upon this foundational work can lead to more robust, scalable, and efficient solutions that advance smart environments.

 doi:10.20944/preprints202406.1346.v1

7. Conclusion

This paper proposes a novel Wi-Fi-based presence detection system utilizing the ESP8266 microcontroller and machine learning techniques. The approach leverages Wi-Fi signals' inherent capabilities to detect individuals' presence and movement within an environment. The cost-effective and efficient ESP8266, with its robust Wi-Fi functionality and low power consumption, is an ideal platform for implementing this system.

The theoretical framework encompasses the properties of Wi-Fi signals, the capabilities of the ESP8266, and suitable machine-learning techniques for analysing data. The system accurately detects presence and movement by capturing and preprocessing data, extracting relevant features, and applying machine learning algorithms, offering a scalable solution for various smart environment applications.

However, several challenges and limitations exist, including signal interference, data privacy concerns, limited range and resolution, computational constraints, environmental variability, and energy consumption. Addressing these challenges is crucial for successful deployment and operation.

Future work will focus on enhancing signal processing, improving data privacy and security, expanding coverage and resolution, optimising computational efficiency, adapting to dynamic environments, optimising energy usage, scaling for larger deployments, and integrating with other smart systems. These efforts will help overcome current limitations and pave the way for robust, reliable, and versatile presence detection solutions.

References

1. Byunghun Song, Haksoo Choi, and Hyung Su Lee. Surveillance tracking system using passive infrared motion sensors in wireless sensor network. In *2008 International Conference on Information Networking*, pages 1–5, 2008.
2. Yang Liu, Tiexing Wang, Yuexin Jiang, and Biao Chen. Harvesting ambient rf for presence detection through deep learning. *IEEE Transactions on Neural Networks and Learning Systems*, 33(4):1571–1583, 2022.
3. Anatolij Zubow, Kim Petto, and Falko Dressler. One-class support vector machine for wifi-based device-free indoor presence detection.
4. Dario Jukić, Silvije Domazet, Ante Ivanko, David Raca, Siniša Nikolić, Marin Knežević, Filip Jović, Nenad Raca, and Hrvoje Buljan. Determining the presence and the number of people by using a wi-fi signal. (arXiv:2308.06773), August 2023. arXiv:2308.06773 [eess].
5. Julio C. H. Soto, Iandra Galdino, Brenda G. Gouveia, Egberto Caballero, Vinicius Ferreira, Débora Muchaluat-Saade, and Célio Albuquerque. Wi-fi csi-based human presence detection using dtw features and machine learning. In *2022 IEEE Latin-American Conference on Communications (LATINCOM)*, pages 1–6, 2022.
6. Yang Liu, Tiexing Wang, Yuexin Jiang, and Biao Chen. Harvesting ambient rf for presence detection through deep learning. *IEEE Transactions on Neural Networks and Learning Systems*, 33(4):1571–1583, 2022.
7. Carlos M. Mesa-Cantillo, David Sánchez-Rodríguez, Itziar Alonso-González, Miguel A. Quintana-Suárez, Carlos Ley-Bosch, and Jesús B. Alonso-Hernández. A non intrusive human presence detection methodology based on channel state information of wi-fi networks. *Sensors*, 23(11):500, January 2023.
8. Wenda Li, Mohammud Junaid Bocus, Chong Tang, Robert J. Piechocki, Karl Woodbridge, and Kevin Chetty. On csi and passive wi-fi radar for opportunistic physical activity recognition. *IEEE Transactions on Wireless Communications*, 21(1):607–620, 2022.
9. Shengjie Li, Xiang Li, Kai Niu, Hao Wang, Yue Zhang, and Daqing Zhang. Ar-alarm: An adaptive and robust intrusion detection system leveraging csi from commodity wi-fi. In Mounir Mokhtari, Bessam Abdulrazak, and Hamdi Aloulou, editors, *Enhanced Quality of Life and Smart Living*, page 211–223, Cham, 2017. Springer International Publishing.
10. Giovanni Pecoraro, Simone Di Domenico, Ernestina Cianca, and Mauro De Sanctis. Csi-based fingerprinting for indoor localization using lte signals. *EURASIP Journal on Advances in Signal Processing*, 2018(1):49, July 2018.
11. Marco Schwartz. *Internet of Things with ESP8266*. Packt Publishing Ltd, July 2016. Google-Books-ID: ROnUDQAAQBAJ.

doi:10.20944/preprints202406.1346.v1

12. Juncong Sun, Xin Bian, and Mingqi Li. Non-contact heart rate monitoring method based on wi-fi csi signal. *Sensors*, 24(77):2111, January 2024.
13. Espressif. *ESP8266 RTOS SDK Programming Guide*, 2020. Get Started - ESP8266 RTOS SDK Programming Guide documentation.
14. Fahd Saad Abuhoureyah, Yan Chiew Wong, and Ahmad Sadhiqin Bin Mohd Isira. Wifi-based human activity recognition through wall using deep learning. *Engineering Applications of Artificial Intelligence*, 127:107171, January 2024.
15. Sonali Awati. Wi-fi gun as a range extender. *International Journal for Research in Applied Science and Engineering Technology*, 7(4):569–573, April 2019.
16. Norah N. Alajlan and Dina M. Ibrahim. Tinyml: Enabling of inference deep learning models on ultra-low-power iot edge devices for ai applications. *Micromachines*, 13(66):851, June 2022.
17. Mondher Bouazizi, Alejandro Lorite Mora, Kevin Feghoul, and Tomoaki Ohtsuki. Activity detection in indoor environments using multiple 2d lidars. *Sensors*, 24(22):626, January 2024.