


Review

Violence Detection Using Wi-Fi and 5G/6G Sensing Technologies: A Review

Aieswarya Kannan and Abbas Z. Kouzani * 

School of Engineering, Deakin University, Geelong, VIC 3216, Australia; s224237852@deakin.edu.au

* Correspondence: kouzani@deakin.edu.au

Abstract: Violence, a pervasive societal concern, demands innovative approaches for its early detection and prevention. This review paper explores the intersection of violence detection and wireless fidelity (Wi-Fi), alongside fifth-generation (5G) and sixth-generation (6G) mobile technologies. Wi-Fi sensing, initially employed for human activity detection, has also demonstrated versatility across a number of other important applications. The significance of leveraging Wi-Fi sensing for violence detection is investigated, underscoring its ability to enhance security protocols and minimise response time. Moreover, through the development and use of machine learning algorithms to analyse and interpret intricate channel state information (CSI) features, the accuracy of violence detection can be improved. Furthermore, this investigation delves into the rapidly developing domain of mobile sensing, examining its contribution to the advancement of violence detection functionalities. The potential convergence of 5G and forthcoming 6G sensing technologies increases the effectiveness of violence detection. Through an analysis of Wi-Fi and mobile sensing technologies, this review paper highlights the transformative capacity that their integration may have on approaches to violence prevention and response.

Keywords: violence detection; Wi-Fi sensing; mobile sensing; 5G sensing; 6G sensing; channel state information



Citation: Kannan, A.; Kouzani, A.Z. Violence Detection Using Wi-Fi and 5G/6G Sensing Technologies: A Review. *Electronics* **2024**, *13*, 2765. <https://doi.org/10.3390/electronics13142765>

Academic Editors: Ali Khoshkholghi, Javid Taheri and Andreas Johnsson

Received: 18 April 2024

Revised: 2 July 2024

Accepted: 11 July 2024

Published: 14 July 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Violence poses a substantial threat to the well-being of individuals and communities worldwide. In recent years, the alarming rise in violent incidents has drawn increased attention, necessitating innovative approaches to address and mitigate violence. The findings in the 2021–2022 Australian Bureau of Statistics' Personal Safety Survey indicate that about 20% of Australian adults faced physical and/or sexual family and domestic violence, starting from the age of 15 [1]. One area of concern is violence within educational institutions, affecting adolescents' mental and physical well-being globally. As societies deal with the multifaceted challenges of violence, technological advancements have become essential tools in devising effective preventive measures and interventions. For example, Kouzani [2] discusses the technological advancements for tackling domestic violence, including artificial intelligence algorithms, social media platforms, smartphones and applications, ambient and wearable sensors, virtual reality methods, and others.

Physical violence, which is a devastating form of violence, includes acts of aggression that result in bodily harm or injury. Instances of bullying, physical altercations, and other aggressive behaviours fall under this category [3]. Verbal violence, manifested through threats, harassment, or verbal abuse, can be equally detrimental, causing psychological distress and emotional trauma. Psychological violence, which may be less apparent but equally harmful, involves manipulation, coercion, and intimidation that erode an individual's mental well-being. The urgency to address and prevent violence has prompted researchers to explore innovative solutions that leverage emerging technologies.

Traditional technologies, such as surveillance cameras, have been integral tools in the realm of security and violence detection [4]. Although pre-mounted cameras consistently

gather and evaluate video frames in areas of interest, they operate exclusively within a clear line-of-sight (LOS) view and introduce inherent privacy concerns.

Vijeikis et al. [5] present an architecture for detecting violence from video surveillance cameras, made up of a U-Net-like network for extracting spatial features using the MobileNet V2 as an encoder, and a long short-term memory (LSTM) network as a feature extractor and classifier. Surveillance cameras offer a visual record of events, providing a tangible and often deterrent presence in monitored areas. However, Omarov et al. [6] stated that their effectiveness is limited by dynamic illumination variations, motion blur, non-professionally produced content, fixed viewpoints, few publicly available datasets, and computational and time-consuming cost. Moreover, the reliance on visual cues poses challenges in scenarios where the identification of subtle, non-visual indicators of violence is crucial. Privacy concerns associated with constant video monitoring and the high cost of infrastructure deployment further impede the widespread and efficient use of surveillance cameras for violence detection.

On the other hand, wearable devices, equipped with sensors such as cameras, have gained popularity for their potential in real-time data collection and personal safety monitoring. Devices, such as smartwatches, belts, and body cameras, offer mobility and the ability to capture dynamic situations where fixed cameras may fall short [7,8]. Wu et al. [9] developed a wearable device-based accident detection system. The system is capable of tracking the bodily movements of individuals, employs an efficient quaternion algorithm to identify falls from routine daily activities, and transmits an automated request for assistance to the caregivers, including the location of the patient.

Wearable technologies, however, face practical challenges related to user compliance and acceptance. Users tend to resist wearing devices consistently, especially in situations where privacy concerns are heightened, or the devices may be intentionally removed during instances of violent behaviour to evade detection. Additionally, the financial burden of deploying and maintaining a network of wearable devices, for example, in a school for an entire student population, can be substantial, limiting the feasibility of widespread adoption.

This study aims to investigate the potential applications of wireless fidelity (Wi-Fi) sensing technology, in particular channel state information (CSI) analysis, for early detection and prevention of violent behaviour. This study delves into the potential benefits of Wi-Fi sensing for enhancing security and examines the development and utilisation of CSI data to enhance the accuracy of violence detection. It also explores the quickly growing field of mobile sensing and how it can help improve various aspects of violence detection. This includes looking at how fifth-generation (5G) and sixth-generation (6G) mobile technologies may come together to make violence detection systems perform better. The paper also covers the public datasets available to advance this research field.

2. Methodology

This literature review is structured around a methodology that consists of a search strategy and selection of sources. Appropriate search terms are identified to conduct the literature search. Figure 1 shows the search terms that are adopted to find the most relevant research publications through relevant digital databases and search engines, such as Scopus and Google Scholar.

The search through the digital databases and search engines identified only a limited number of relevant publications. Due to the emerging nature of the field of violence detection with Wi-Fi and 5G/6G sensing, the available literature remains relatively small. As a newly growing area of research, Wi-Fi Sensing, 5G sensing, and 6G sensing have only recently received significant attention, resulting in a limited pool of publications.

Figure 2 presents a PRISMA flow chart for the executed literature search. Using the specified search terms, the search yielded a total of 4802 papers, with an additional 5 obtained from supplementary sources. Among the total records identified, 18% were duplicates. After the duplicate screening process, we found that nearly two-thirds of the

remaining records focused on video surveillance and computer vision-based techniques, which were outside the scope of this literature review. These techniques have gained prominence in violence detection for their efficient analysis and interpretation of visual data. However, they also face significant privacy concerns.

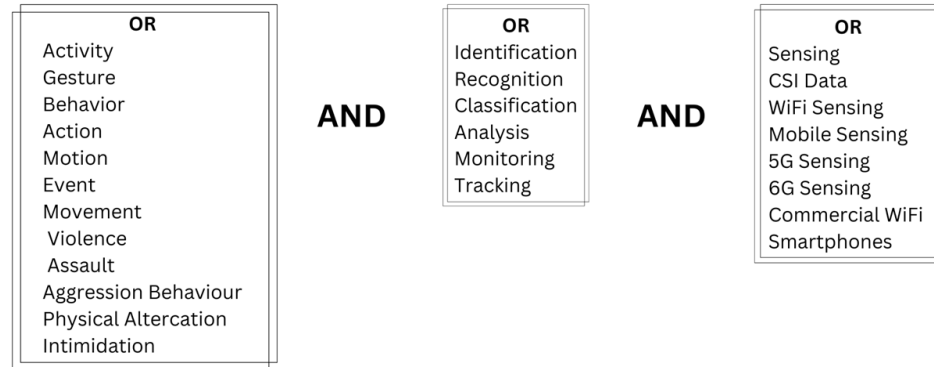


Figure 1. Search terms.

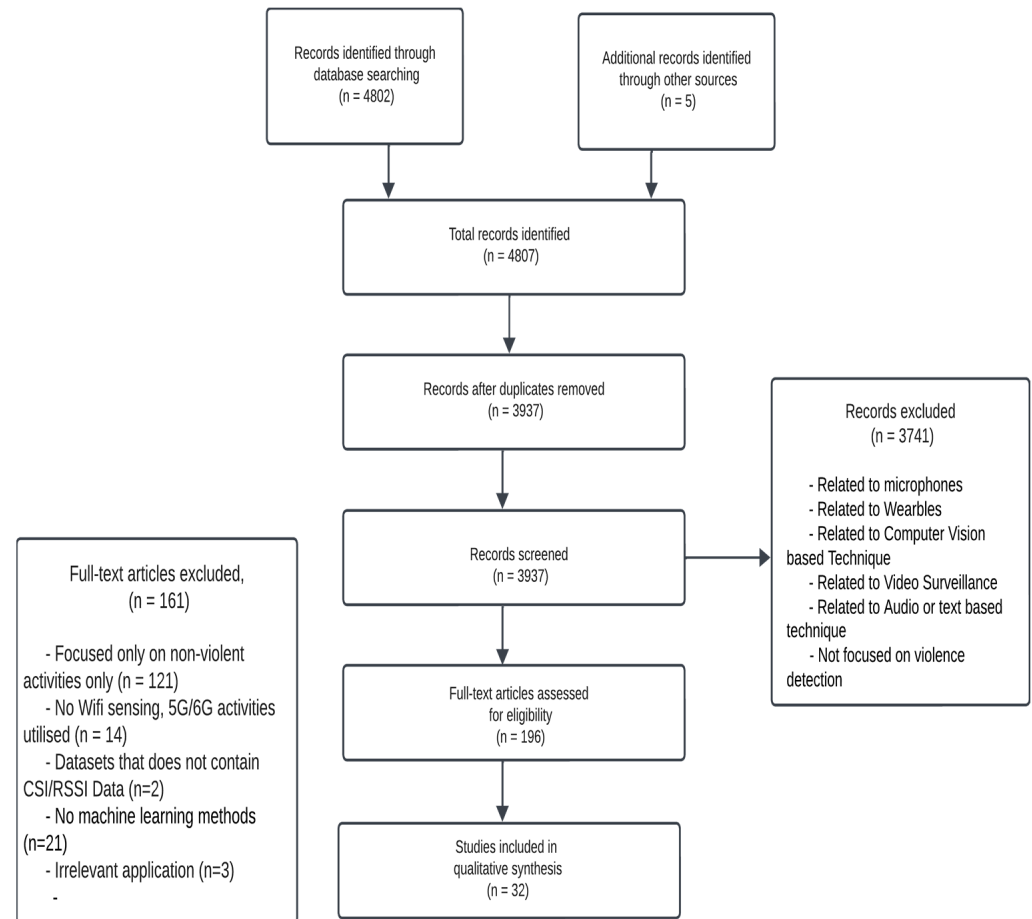


Figure 2. PRISMA flowchart.

Another 20% of the records utilised microphones and other wearable devices, which were also beyond the scope of this literature review. These technologies offer a different approach by capturing audio cues and physiological signals, which can be critical in identifying violent incidents. The remaining records were divided between those that focused on audio- or text-based violence detection and those that were not relevant to violence detection at all. Audio- and text-based methods often rely on analysing spoken words, ambient sounds, or written content to detect signs of violence.

Ultimately, about 95% of the identified records were excluded from further screening. This exclusion was necessary to refine our focus on the most relevant and high-quality studies that contribute to our understanding of violence detection techniques using only Wi-Fi/5G/6G sensing. The screening process ensures that the final selection of papers provides valuable insights and advancements in the field of violence detection using the technological approaches that are within the scope of this literature review.

From the 196 articles remaining, a total of 161 articles were excluded from the analysis for various reasons, and thus 32 were kept for this study. Of the 161 excluded articles, 75.2% were excluded because they focused only on non-violent activities like sitting, walking, etc. Additionally, 8.7% did not utilise Wi-Fi sensing or 5G/6G sensing, which were essential for our research criteria. Another 1.2% of the articles were excluded because their datasets contained videos or CCTV footage of violence activities and did not contain CSI or received signal strength indicator (RSSI) data-based violence datasets, both critical for our analysis. Furthermore, 13% of the articles did not employ machine learning methods using CSI data, which are pivotal for advancing violence detection techniques. Finally, 1.9% were excluded due to their irrelevant applications, like authentication purposes, smart appliances, etc., which did not contribute to the study's objectives.

3. Wi-Fi Sensing

The Wi-Fi sensing technology introduces a paradigm shift in violence detection. Wi-Fi sensing, an emerging technology, uses Wi-Fi signals to detect changes in surroundings, motion, and presence in a specific area. Similar to short-range passive radar systems, this innovative technique tracks locations and activities by utilising the interactions between Wi-Fi waves and movement. Employing current Wi-Fi infrastructure, Wi-Fi sensing detects and analyses disturbances caused by movement and environmental changes.

The signals are sent using typical Wi-Fi communication data frames, which are intended for use in digital communications. The access point (AP) or other network-connected devices receive the Wi-Fi signals. Wi-Fi sensing uses artificial intelligence (AI) to identify, categorise, and analyse Wi-Fi signal disruptions. Based on the collected data, the technology generates intelligent solutions [10–12].

Some of the commercial signal sensing hardware utilised for Wi-Fi-based recognition systems include commercial wireless network interface cards (NICs) (e.g., Intel 5300 NIC) and Atheros NIC system on chips (SoCs) (e.g., Espressif SoC), smartphones, and universal software radio peripheral (USRP) devices [13].

While NICs are primarily designed for networking functions, they are also extensively used for Wi-Fi-based gesture recognition. A NIC can function as a receiver when paired with other computing devices, such as personal computers (PCs), and a standard Wi-Fi router typically serves as the transmitter. The obtained CSI data undergoes various data preprocessing techniques such as denoising, signal processing, and feature extraction before it is fed into machine learning algorithms. Ali et al. [14] give a performance comparison of various algorithms used for Wi-Fi sensing applications, such as support vector machine (SVM), decision trees (DT), ensemble methods, and others. Figure 3 provides a block diagram illustrating the step-by-step process of recognising human gestures through Wi-Fi sensing.

By leveraging the existing Wi-Fi infrastructure, this approach provides a cost-effective and unobtrusive solution that operates passively, eliminating the need for user cooperation or the physical presence of additional devices. Wi-Fi sensing utilises CSI data to detect violence by capturing alterations in signal propagation caused by human actions. The amplitude is obtained by taking the square root of the sum of the squares of the imaginary part and the real part of the collected CSI data, while the phase is derived by taking the arctangent of the ratio of the imaginary part to the real part of the collected CSI data [13].

This innovative method not only addresses the limitations of traditional technologies, but also offers a unique and comprehensive perspective on violence detection, making it a promising and adaptable solution for creating safer environments. Khalili et al. [15]

presents a comprehensive assessment on the use of Wi-Fi sensing including monitoring elderly individuals, recognising gestures, classifying activities, counting people, through the wall sensing, and behind the corner sensing.

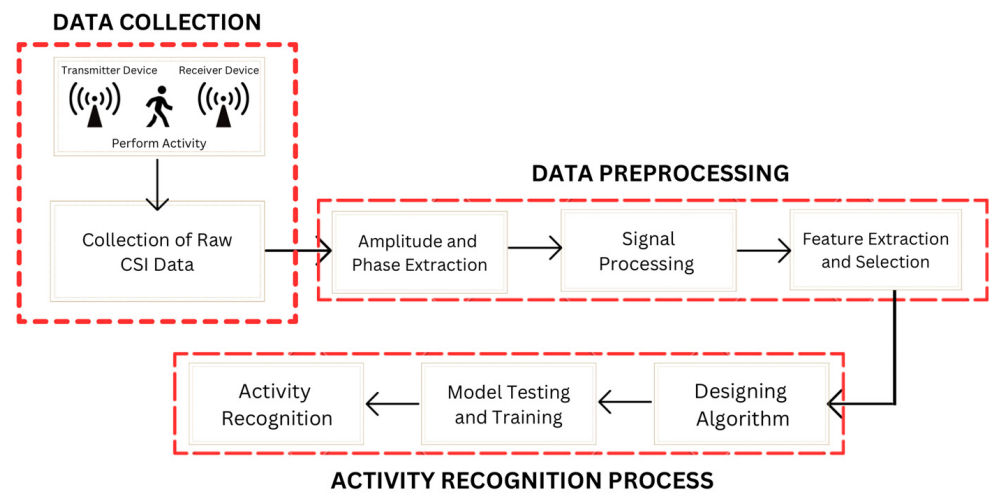


Figure 3. CSI-based activity recognition process.

3.1. Activity Recognition

Liu et al. [16] introduce a method for detecting intense human motion in enclosed surroundings based on CSI obtained from Wi-Fi signals. The study tackles the requirement for passive human detection without the need for any devices in a variety of contexts, including automated homes, geriatric care, protecting assets, and detection of intrusion. The authors propose a system that utilises the physical layer information in wireless signals, specifically the CSI, to identify strong human motion involving numerous targets. The proposed method in the paper involves several key steps to achieve device-free, passive detection of intense human propulsion by means of CSI from wireless transmissions. Initially, the system focuses on line-of-sight (LOS) and non-line-of-sight (NLOS) identification by analysing the skewness of channel impulse response (CIR) distribution. To mitigate the sensitivity of wireless signals to environmental changes, signal preprocessing techniques are applied, including the use of a band-pass filter to filter out unrelated frequency components of a signal. Subsequently, features such as standard deviation, median absolute deviation, interquartile range, and signal entropy are calculated from CSI phase and amplitude difference to effectively characterise various human motions.

For classification, the method employs a one-class support vector machine (OSVM) classifier, utilising training sets containing only one positive sample type, namely intense human motion, without incorporating other sample types. The system's performance is evaluated through experiments conducted in both enclosed and semi-closed spaces. The evaluation encompasses LOS/NLOS identification and detection of intense human motion. Furthermore, the paper explores the impact of factors such as transmitter–receiver height, sample size, and distance between the receiver and transmitter on the overall effectiveness of the proposed method. Experiments are conducted in semi-closed and confined areas, simulating real-world indoor scenarios. The collected data include various human activities in LOS and NLOS conditions, helping train and validate the proposed detection system. The paper reports promising results for LOS/NLOS identification, maximising the rate of detection while minimising the rate of false alarms. For intense human motion detection, the system exhibits notable performance, with sensitivity (true positive rate) and specificity (true negative rate) reaching satisfactory levels, especially when considering both LOS and NLOS conditions.

The proposed system presents advantages, leveraging existing Wi-Fi access points to achieve device-free, passive detection of human motion without the need for additional

equipment. Notably, privacy concerns related to camera-based methods are effectively addressed, making them well suited for deployment in private spaces. The utilisation of CSI enhances the system's capabilities by providing fine-grained information, enabling the detection of complex human motions. However, some shortcomings exist. The system's performance is influenced by the height of the transmitter–receiver pair, with optimal results obtained at specific heights. Additionally, distinguishing between intense human motion and regular activities may pose challenges, potentially leading to misclassifications.

Furthermore, the effectiveness of the system diminishes in semi-closed spaces compared to enclosed spaces, highlighting considerations for specific deployment scenarios. Potential applications for the proposed system include smart buildings, elderly support, safeguarding assets, and theft prevention, among others. Its ability to operate without additional devices makes it suitable for deployment in environments where privacy concerns or the inconvenience of wearable sensors exist. The focus on intense human motion detection positions it for applications in security monitoring and incident identification in complicated indoor scenarios. In conclusion, the paper presents a robust framework for device-free, passive detection of intense human motion using CSI from Wi-Fi signals. The experimental results demonstrate its effectiveness in real-world scenarios, highlighting its potential for applications in diverse domains.

Gu et al. [17] discuss a novel approach for recognising human activities using Wi-Fi ambient signals. The authors highlight the challenges posed by the increasing number of sensors in devices for the Internet of Things (IoT) applications, particularly in terms of volume and energy issues. They propose utilising wireless ambient signals, specifically radio frequency (RF) transceivers, as an alternative source of information for activity recognition. The authors conducted an empirical study to understand the impact of various activities on RSSI values, a key parameter in Wi-Fi communication. They explore the stability of wireless signals in indoor environments and propose a method to recover physical activities by analysing signal fluctuations caused by human movements.

The research builds upon previous works that primarily focused on the utilisation of wireless transmissions for services that use location. However, the paper introduces a novel approach by connecting pervasive wireless signals with the recognition of human activities, a concept referred to as “WiSee”. The paper acknowledges pioneering works such as WiSee and Wi-Vi but emphasises the need for solutions compatible with commodity Wi-Fi devices. The authors explore the details of two categories of solutions: CSI-based and RSSI-based. While CSI offers unique advantages, its limitations in terms of hardware and complexity lead the authors to favour RSSI as a more practical trade-off between efficiency and cost, particularly for smartphones and tablets.

The empirical investigation of Wi-Fi characteristics is delineated by the authors, who emphasise the influence of diverse activities on RSSI. The research findings indicate that activities do indeed influence the signal, with distinct activities producing unique patterns or fingerprints on Wi-Fi RSSI. The architecture of the recognition system is presented, involving three layers: access points as signal sources, smart devices for data collection, and a server for storing, analysing, and recognising activities. Real-world applications can utilise the online fingerprint-based activity recognition system without requiring adjustments at access points or mobile entities due to its adaptability and flexibility. The paper details the preprocessing module, aimed at filtering abnormal samples, and the classification module, which selects suitable features for activity recognition. The selection of recognition features involves a case study, focusing on the mean (μ) and standard deviation (σ) of RSSI values.

The authors introduce a fusion algorithm, combining k-nearest neighbours (k-NN) classification with a classification tree, to enhance recognition precision. Six distinct activities are prototyped into the system as part of the performance evaluation process. The proposed fusion algorithm outperforms other classifiers, such as k-NN, naïve Bayes, and bagging, in terms of recognition precision. The paper acknowledges the importance of carefully selecting the group size for optimal performance. Advantages of the proposed

system include its flexibility, adaptability, and the ability to work with commodity Wi-Fi devices. The fusion algorithm enhances recognition accuracy by combining features and addressing challenges related to similar footprints of different activities. The system requires no modifications at the ends of access points or mobile entities, making it suitable for real-world applications.

However, the paper acknowledges that the size of data groups during recognition is crucial, and the system's performance is impacted by the choice of this parameter. Additionally, while the proposed system shows promising results, it is essential to consider scalability and potential challenges in diverse environments. In conclusion, the paper highlights the contributions of Passive Human Activity Recognition Based on Wi-Fi Ambient Signals, including empirical results, an online fingerprint-based architecture, and extensive evaluations. The proposal establishes the system as a viable remedy for dormant activity by humans detection via Wi-Fi ambient signals, with potential applications in various real-world scenarios.

The research on Wi-Fi sensing for smart residential environments with real-time activity monitoring by Sahoo et al. [18] addresses the broad applications of human activity recognition (HAR). The study identifies traditional sensors' limitations, particularly the intrusive nature of proximity, pressure, and light sensors. Instead, it proposes harnessing RF signals, specifically Wi-Fi signals, to achieve real-time activity detection. The core concept revolves around utilising CSI derived from Wi-Fi signals. The proposed system introduces a two-layer architecture employing low-cost IoT devices, specifically the ESP32 micro-controller. The architecture consists of an IoT layer responsible for data generation and an edge layer for real-time data processing, filtering, and visualisation.

The methodology encompasses data collection using ESP32 devices, data transfer between IoT and edge layers, and processing CSI data to extract amplitude and phase information. The novel two-layer architecture focuses on edge computing technology for real-time activity detection. The IoT layer comprises physical devices, while the edge layer collects, processes, and visualises data almost in real-time. The paper concentrates on the ESP32 micro-controller for both IoT and edge layers, highlighting the flow of CSI data from IoT to edge for further analysis. The proposed system's advantages include simplicity, low cost, and real-time processing capabilities.

The ESP32 micro-controller is positioned as a superior alternative to traditional Wi-Fi sensing tools. However, the paper acknowledges a 70% accuracy in activity classification using the lightweight SVM algorithm, indicating room for improvement. Additionally, the limitations of the ESP32, such as its low processing capability, are recognised. In terms of applications, the paper suggests its relevance in smart home environments, where real-time activity detection can enhance the user experience and enable various services. The proposed system can find utility in monitoring daily activities, providing security, and facilitating personalised human-computer interactions within smart homes.

Yang et al. [19] introduce a novel approach for HAR in enclosed environments using commercial Wi-Fi devices. Traditional HAR systems face challenges related to inconvenience, environmental restrictions, and the need for special equipment. In contrast, Wi-Fi-based systems, leveraging CSI, offer a device-free solution with potential applications in smart homes, security monitoring, medical assistance, and more. The proposed system, termed WiTA, focuses on three technical challenges. Firstly, it addresses the separation of effective signals with multipath from the original CSI. An introduced method for the precise extraction of multipath signals utilises the propagation delays of different multipath signals. Secondly, the paper tackles the segmentation of effective motion fragments, avoiding the need for re-adjustment of parameters when the signal environment changes.

Thirdly, it places significant emphasis on the efficient extraction of correlation features from the initial CSI. WiTA comprises two main modules: CSI data processing and neural networks. Involved in the CSI data processing module are the extraction of features, multipath separation, noise elimination, and feature acquisition. The neural network module integrates temporal–frequency attention through the utilisation of an attention mechanism

integrated into a multi-layer LSTM network architecture. The proposed algorithm in the paper offers several advantages in the context of human activity recognition. Firstly, it effectively addresses the challenge of separating multipath signals, ensuring accurate recognition of human activities. This is a critical aspect, particularly in complex environments where signal interference is common. Additionally, the end-to-end method employed by the algorithm minimises information loss during data processing, enhancing the overall efficiency of the recognition system.

The introduction of a temporal–frequency attention mechanism in WiTA further contributes to its effectiveness. This attention mechanism improves the system’s ability to focus on relevant features, ultimately leading to enhanced recognition accuracy. However, the algorithm comes with certain shortcomings that warrant consideration. One notable challenge is the complexity of training, especially due to the interaction between four sub-networks during the training process. This complexity may necessitate a step-by-step training method to ensure optimal performance. Another limitation is the acknowledgement of the system regarding the processing capacity, particularly in the ESP32 micro-controllers utilised in the experimental setup. This recognition of processing limitations suggests that the algorithm’s practical implementation may face constraints in certain hardware environments.

Overall, while the algorithm presents significant advancements in human activity recognition, careful consideration of these advantages and shortcomings is crucial for its successful implementation. The authors present experimental results using the WiAR dataset and their own collected data, demonstrating an average recognition accuracy of 94%. In comparison to other prevalent recognition algorithms, the proposed algorithm demonstrates superior accuracy. Additionally, the effect of the quantity of training samples on recognition accuracy is assessed, indicating a positive relationship.

Feng et al. [20] explore the development of a system, named Wi-Multi, for human activity recognition based on CSI obtained from commercial wireless devices. The application areas targeted include healthcare, security, and IoT. Traditional approaches for activity recognition often involve sensors or cameras, but these methods face issues such as inconvenience for users wearing sensors and privacy concerns with camera-based systems. The proposed system leverages CSI extracted from commercial Wi-Fi devices, eliminating the need for additional equipment and addressing cost concerns. The paper’s deep learning network selects high-level characteristics independently, with no pre-processing modules required. The results of the tests indicate that the system might successfully strike a balance between efficiency and accuracy at various stages, with Wi-Multi achieving an average accuracy of 96.1%.

One key contribution is the introduction of a three-phase system tailored for various stages of system setup. When there are few samples in the profile, Phase 1 is used, based on principal component analysis (PCA), discrete wavelet transform (DWT), and distance-based classification. Using the SVM algorithm, features are extracted from the time and frequency domains and classified in the second phase. Phase 3 employs LSTM in a deep learning network when a large number of samples are available. The research highlights a new activity extraction technique that can locate an activity’s beginning and ending even in noisy settings with several subjects. The algorithm employs outlier filtering, differential algorithms, and eigenvalue comparison to achieve robust activity sample extraction.

While the paper highlights several advantages, such as the use of existing Wi-Fi devices, the autonomous feature selection of the deep learning network, and the effectiveness of the activity extraction algorithm, it does not explicitly address potential shortcomings or limitations. The experimental results demonstrate the system’s performance in terms of accuracy, efficiency, and the ability to recognise the number of subjects present in a situation. The Wi-Multi system offers a comprehensive approach to human activity recognition using CSI from Wi-Fi signals. The three-phase design caters to different stages of system deployment, showcasing adaptability and robustness in various environments. The

proposed system presents a promising direction for applications in healthcare, security, and IoT, providing a balance between accuracy and efficiency.

3.2. Violence Detection

Zhang et al. [21] introduce WiVi, a pioneering passive violent behaviour detection system utilising commercial Wi-Fi infrastructure. Addressing the escalating global concern of school violence impacting youth's physical and mental health, WiVi leverages CSI from Wi-Fi signals to recognise violent activities. The existing challenges in violence detection, including the limitations of traditional methods and privacy concerns, prompt the need for innovative solutions. WiVi leverages the widespread implementation of Wi-Fi infrastructure, in particular the CSI offered by the physical layer, to expose multipath characteristics impacted by human movements and actions. The study highlights the underuse of CSI by current techniques and suggests a unique method that combines correlated information generated from the combination of distinct CSI subcarriers' time series data. A PCA-based feature fusion technique is created to integrate both time series and correlated information adaptively in various contexts, while a Gabor filter-based feature extraction method is presented for the automatic extraction of correlated features.

The authors highlight the significance of WiVi's ability to precisely identify complex violent activities, even in changing operating environments. They address the limitations of existing methods, which often concentrate on pre-defined actions and struggle to adapt to diverse scenarios. The proposed feedback adjustment method ensures adaptability for environmental changes by readjusting model parameters and potentially retraining the model when necessary. WiVi's prototype, implemented on commercial Wi-Fi devices, demonstrates impressive performance with a 93.46% accuracy in detecting violent activities and a 6.43% false alarm rate. The paper concludes by summarising the key contributions, emphasising the combination of time series and correlated features, the Gabor-filter and PCA-based methods, and the successful implementation and evaluation of WiVi in various environments.

In conclusion, WiVi represents a significant advancement in violence detection systems, offering a reliable and adaptive solution with potential applications in ensuring the safety of educational environments. The authors provide a comprehensive overview of their methodology, results, and contributions, laying the groundwork for future research in the field.

Zhou et al. [22] introduce Wi-Dog, a non-invasive system for monitoring physical assaults in smart schools using commercial Wi-Fi devices. The research addresses the increasing concern of school violence and leverages Wi-Fi signals to detect and alert in real-time instances of physical assault. The motivation for this innovation stems from the limitations of traditional monitoring systems, such as wearable sensors and camera-based approaches, which either compromise comfort or raise privacy concerns. Wi-Dog employs Wi-Fi signals to capture distinct features in the CSI at the physical layer (PL). Unlike conventional approaches, Wi-Dog focuses on the irregular and unpredictable nature of assault events. The system overcomes three critical challenges: extracting motion data from CSI dynamics with noise, detecting abnormal transitions during human interactions, and differentiating actual attacks from acts resembling assaults.

Wi-Dog employs a multifaceted approach to non-invasive physical assault monitoring through commercial Wi-Fi devices. In relation to motion information extraction, the system leverages spatial diversity, analysing variations in CSI waveforms across different antennas for accurate and abundant motion cues. Noise reduction steps are strategically implemented to eliminate irrelevant interferences while retaining crucial motion data. Wi-Dog anomalous transition detection differs from traditional methods in that it makes use of the target frequency band's signal complexity to monitor the amount of irregularity and intensity change. The system further enhances location-independent detection through cross-correlation of adjacent subcarriers. For the differentiation of assaults, novel features such as Doppler frequency shifts are extracted to represent intensity levels. Employing a

SVM classifier in local analysis, Wi-Dog reduces false alarms by considering irregularity and continuity over longer time durations. During the experimental study, when two volunteers simulate real physical collisions where drastic conflicts exhibit significant intensity cues such as speed, acceleration, and kinetic energy, the fine-grained spectrogram resulting from distinct power variations in frequency bands is shown in Figure 4.

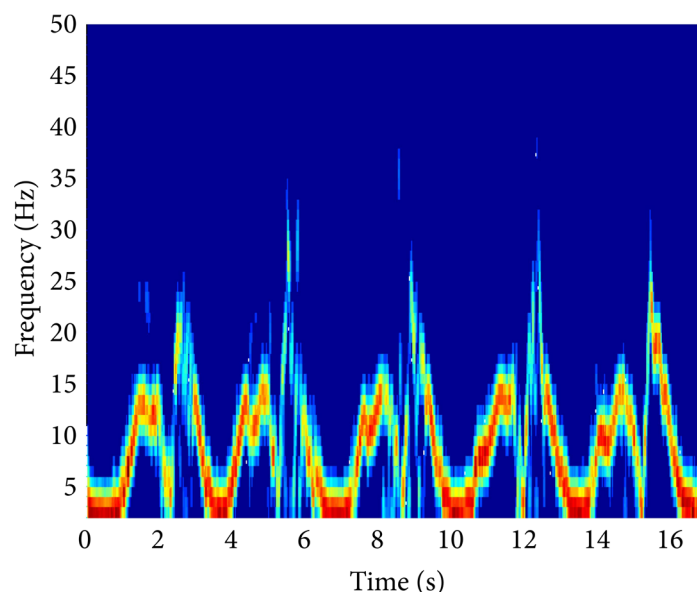


Figure 4. Constructed spectrogram with normal activities and physical assault [22].

This comprehensive methodology showcases Wi-Dog's ability to effectively and innovatively monitor physical assaults in real-time, offering a promising solution for enhancing safety in smart school environments. The research validates Wi-Dog through experiments involving imitated physical attacks in both LOS and NLOS environments, utilising real-time CSI measurements from commercial Wi-Fi devices. The results demonstrate high true detection rates (0.94 in LOS, 0.85 in NLOS) and low false alarm rates (0.08 in LOS, 0.11 in NLOS) across various scenarios and parameter changes, showcasing the system's robustness. Wi-Dog offers several advantages, including non-invasiveness, addressing privacy concerns associated with camera-based monitoring, and its potential for ubiquitous deployment through existing Wi-Fi infrastructures. However, it may be limited in generalisation to specific environments and necessitates further adaptation for broader applications. Despite its promising results, consideration of false positives in complex real-world scenarios remains a point of discussion. The application of Wi-Dog extends beyond school violence prevention, demonstrating its potential for general emergency detection. The proposed technology's versatility is underscored by potential applications, such as injury rescue, elderly healthcare, and terrorist threat warning.

Hsu et al. [23] address the increasing threat of cybercrime, particularly through attacks on public Wi-Fi networks, focusing on the notorious "evil twin" phenomenon. Evil twins are rogue access points that mimic legitimate ones, putting users at risk of data theft. The authors highlight the limitations of existing solutions and suggest a proactive client-side remedy, the wireless packet forwarding detector (WPFDD), designed for Wi-Fi users without requiring specialised equipment or system management. The paper outlines the challenges posed by evil twin attacks, emphasising the need for user-friendly and effective solutions. The authors provide WPFDD, an active client-side solution that makes use of monitoring techniques based on the transmission control protocol/internet protocol (TCP/IP). To identify the existence of a malevolent twin, Monitoring the retransmission behaviour of the corresponding synchronisation/acknowledgment (SYN/ACK) packets, WPFDD transmits SYN packets to well-known websites.

The proposed solution aims to be user-friendly, requiring only the TCP/IP header of wireless packets for detection. WPFDD is designed to operate in real-time, sending probe packets to significant websites for detection. The WPFDD method presents several advantages as a user-friendly solution for Wi-Fi users, eliminating the need for specialised equipment or system management. WPFDD claims to provide accurate and fast detection of evil twins through its active approach, offering independence from specific network information, such as legal access points/internet protocols or training data. Notably, WPFDD sets itself apart by seamlessly integrating both utilising one WNIC in both passive monitor mode and active probe packets.

However, the paper has shortcomings, including a lack of experimental details, as specific datasets or real-world experiments validating WPFDD's effectiveness are not provided. Additionally, the limited depth of the security discussion raises the need for a more thorough analysis of potential vulnerabilities and countermeasures to strengthen the overall robustness of the proposed solution. The primary application of WPFDD is to enhance the security of Wi-Fi users by actively detecting and preventing evil twin attacks. It offers a practical and efficient solution for individuals using public Wi-Fi networks, where the risk of evil twin attacks is prevalent. In conclusion, the paper introduces WPFDD as a user-side solution to address the security concerns associated with evil twin attacks. While it emphasises user-friendliness and effectiveness, further validation through detailed experiments and a more thorough security analysis would contribute to establishing the robustness of WPFDD in real-world scenarios.

Liu et al. [24] present an inventive strategy for identifying violent behaviour by leveraging CSI from wireless signals, specifically Wi-Fi. The authors highlight the severe psychological impact of violence on victims, including depression, anxiety, and suicide, and address the challenges associated with monitoring unpredictable incidents in diverse settings. Critiquing existing methods for their costliness and privacy concerns, the paper proposes a cost-effective and privacy-friendly alternative based on CSI. Emphasising the advantages of wireless technology, particularly the resilience of CSI-based methods to environmental factors, the authors argue for the accessibility and affordability of their approach. They position their method in the broader context of CSI-based human behaviour recognition, citing previous research on applications like fall detection and gesture recognition. This places the proposed violent behaviour detection method within the evolving landscape of CSI-based technologies. The proposed method leverages the advantages of wireless technology for human behaviour recognition, specifically CSI.

The authors contend that CSI-based techniques are advantageous for maintaining privacy because they are unaffected by external variables like light and temperature. The method involves extracting features from the frequency domain, time domain, and image domain, adopting a multi-domain approach to capture more information from CSI. The model considers the complex indoor wireless signal propagation environment, emphasising the effects of human behaviour on received signals, including Doppler frequency shifts. The experiments employ an emerging class of commercial Wi-Fi equipment based on orthogonal frequency division multiplexing—multiple input multiple output (OFDM-MIMO) to collect fine-grained CSI information. The data collection process aims to measure changes in CSI resulting from distinguishable propagation paths, including direct paths, reflections, diffractions, and refractions. The experimental findings underscore the efficacy of the suggested approach in identifying violent conduct.

Specifically, the average recognition accuracy is reported as 97.3% in darkroom scenarios and 92.7% in laboratory scenarios. These outcomes emphasise the system's robust performance and its capacity to function optimally using existing Wi-Fi infrastructure. This characteristic positions the method not only as an accurate but also a cost-effective and scalable solution. One advantage of the proposed method lies in its reliance on wireless signals. By avoiding the use of cameras, it minimises privacy concerns that are often associated with camera-based methods. This feature enhances the acceptability and ethical considerations of the system. The utilisation of existing Wi-Fi infrastructure is a key cost-saving aspect. It

eliminates the need for additional, potentially expensive hardware, making the solution economically viable for widespread adoption in various settings. The system demonstrates impressive accuracy in detecting violent behaviour across diverse scenarios.

The consistently high recognition accuracy underscores its reliability in identifying potential threats, contributing to its overall efficacy. The study candidly acknowledges potential challenges in distinguishing between violent and regular activities. This recognition prompts a call for further refinement, suggesting an avenue for improvement to enhance the system's capability in accurately discerning different behavioural patterns. The paper notes a decrease in the system's effectiveness in semi-closed spaces. This limitation implies that the method might encounter challenges in environments with specific structural characteristics, potentially influencing its applicability in certain settings. The proposed CSI-based violence detection method holds promise for enhancing security in various domains, especially in public spaces where the risk of violent incidents exists. Its advantages, including privacy preservation, cost-effectiveness, and high accuracy, position it as a promising solution for real-world deployment. The adaptability of the method to existing Wi-Fi infrastructure makes it suitable for widespread use, effectively addressing the limitations associated with previous hardware-dependent approaches.

4. Mobile Sensing

Ehatisham-ul-Haq et al. [25] address the growing concern of security and privacy in smartphones, considering the increasing reliance on these devices for daily tasks. With the drawbacks of conventional authentication techniques such as passwords and biometrics, the authors propose a novel continuous authentication scheme in accordance with recognising activity patterns using passive mobile sensing. The proposed scheme focuses on leveraging three integrated sensors, an accelerometer, a gyroscope, and a magnetometer, to record the physical activity patterns of users. Six common daily activities (ascending and descending staircases, walking, running, standing, and sitting) were chosen for user recognition. The study employs a pre-existing dataset for the recognition of physical activity, utilising machine learning classifiers (SVM, DT, and k-NN) to recognise users based on extracted features. The authors utilise a pre-existing dataset for the recognition of physical activities, maintaining consistency with the proposed scheme's pipeline.

The dataset includes ten participants engaging in six activities and considers that there are five distinct smartphone placements on the body for user recognition. The research employs three machine learning classifiers and extensively compares their performances for user recognition. The results obtained provide evidence that the proposed scheme is successful in differentiating specific users according to their activity patterns. This research examines the issue of position sensitivity in movement sensors for smartphones, with the aim of mitigating false positives and establishing secure user authentication. The presented continuous authentication scheme offers several noteworthy advantages.

Firstly, it introduces an innovative approach by leveraging activity pattern recognition for user authentication, marking a departure from conventional methods. The study also effectively mitigates the issue of position sensitivity in smartphone motion sensors, thereby enhancing the accuracy of user recognition across various activities and body positions. Furthermore, the paper makes a valuable contribution by conducting a comprehensive comparison of three machine learning classifiers (SVM, DT, and k-NN) providing insights into their respective performances for user authentication.

However, the study acknowledges some shortcomings that warrant consideration. The potential obstacle of gathering real-time data in dynamic and open environments is acknowledged, underscoring the intricacy of applying the proposed scheme in practical situations. Additionally, while the research addresses position sensitivity, its reliance on fixed smartphone positions may introduce limitations in practical situations where users carry smartphones in diverse and dynamic ways. These drawbacks underscore the need for further research to refine the proposed approach and address these challenges for broader applicability. The presented continuous authentication scheme holds promise

for enhancing smartphone security by providing a non-intrusive and reliable method for user identification. The application of this method extends to scenarios where traditional authentication methods fall short, offering a solution for maintaining the privacy and security of sensitive information stored on mobile devices.

In conclusion, the paper gives a pioneering approach to smartphone user authentication, leveraging behavioural biometrics through activity pattern recognition. Despite the acknowledged challenges, this method demonstrates effectiveness and addresses critical issues in current authentication practices. The study contributes to advancing the field of mobile device security, offering a potential solution to authenticate users continuously and without intrusion.

5G/6G Sensing

Chen et al. [26] explore the application of 5G signals in radio sensing, focusing on healthcare-related scenarios. The authors introduce the concept of radio sensing, emphasising its advantages over traditional sensing methods, such as its sensor-less and contactless operation, low hardware cost, and privacy protection. Their paper discusses the unique merits of 5G signals, including high carrier frequency, large channel bandwidth, large antenna arrays, dense network deployment, and other features. In the healthcare domain, the paper presents several applications of 5G radio sensing, including motion and fall detection, monitoring of vital signs and respiration, and vital sign detection. The authors conducted experiments using 5G C-band signals, capturing CSI values and using machine learning algorithms for classification. For instance, in fall detection, the study achieved high accuracy using the SVM algorithm, and similar success was reported in vital sign monitoring and breathing detection. The paper highlights the potential of 5G radio sensing in improving healthcare monitoring for conditions such as multiple sclerosis and Parkinson's disease. The advantages of 5G signals, such as high carrier frequency and large channel bandwidth, contribute to improved ranging and localisation resolutions, making 5G signals suitable for precise and accurate radio sensing applications. The authors also discuss the challenges and limitations of 5G radio sensing, including its limited range, coverage, and high energy requirements.

Wymeersch et al. [27] discuss the evolution of mobile communication systems, particularly focusing on the shift from 5G to 6G. The primary emphasis is on the integration of sensing and communication capabilities in 6G, with a vision presented by the Hexa-X consortium, a collaboration of 25 academic and industry partners. The evolution from 5G to 6G involves a significant increase in carrier frequencies, especially in the millimeter-wave (mmWave) and potentially the terahertz (THz) bands, striving for enhanced communication and pinpoint localisation in dynamic environments. The paper introduces the concept of joint radar communication, computation, localisation, and sensing (JRC2LS) as a key foundation of 6G. Local trust zones, sustainable development, massive twinning, telepresence, and cooperating robotics (cobots) are among the five families of 6G use cases classified by the authors. These use cases rely on extreme localisation accuracy, low latency, and integrity, highlighting the need for a holistic approach in the design of 6G systems.

The Hexa-X vision presents two main pillars for 6G localisation and sensing: extreme performance and JRC2LS. Extreme performance refers to the ability to attain precise values for 3D localisation, orientation, and their derivatives, thereby exceeding the capabilities of current sensor technologies such as cameras, radar, and lidar. The convergence, coexistence, or joint design of sensing, computation, communication, and localisation capabilities in 6G services is referred to as JRC2LS. The paper acknowledges the challenges in achieving the proposed vision, in particular the hardware constraints that arise at higher frequencies and the varied propagation phenomena that occur across distinct frequency ranges. Hardware imperfections, such as phase noise and non-linearities, impact localisation accuracy and require robust compensation mechanisms. The propagation channel characteristics vary with frequency, influencing the performance of localisation systems.

The paper provides a comprehensive synopsis of the integration of communication and sensing in 6G, presenting the vision of Hexa-X, use cases, and key technological enablers. The proposed pillars of extreme performance and JRC2LS address the requirements of emerging 6G applications, but the paper recognises the challenges that need to be overcome in hardware design and propagation modelling. The work sets the stage for further research and development in realising the ambitious goals of 6G wireless communication systems.

5. Datasets

The available datasets for Wi-Fi sensing based on CSI are limited, but they provide valuable resources for researchers in this field.

The CSI Dataset for Wireless Human Sensing on 80 MHz Wi-Fi Channels [28] offers data for activity recognition, people identification, and people counting through the use of Wi-Fi CSI. This dataset comprises more than 13 h of channel readings obtained from diverse settings, such as a bedroom, living room, kitchen, and others. Another dataset, known as Wi-Gitation [29], specifically focuses on the recognition of physical agitation activity using Wi-Fi CSI. The WiMANS dataset [30] is a pioneering dataset that enables multi-user sensing analysis using Wi-Fi CSI. Each sample in the dataset can include anywhere from zero to five users engaged in simultaneous activities.

Although these datasets hold significant value, finding comprehensive and high-quality CSI datasets specifically for Wi-Fi sensing can be difficult. Numerous current datasets have a limited scope because they concentrate on specific tasks or environments, and do not possess the diversity and scale required for more advanced research. The SenseFi benchmark [31] seeks to tackle this issue by offering a library and evaluation framework for cutting-edge deep learning models on various public CSI datasets. In general, the lack of easily accessible, extensively labelled CSI datasets poses a major obstacle to the progress of Wi-Fi-based human sensing studies.

The Wi-Fi Activity Recognition [32] dataset provides data for seven activities, accompanied by model code examples. The dataset comprises more than 13 h of Wi-Fi CSI data gathered from different settings, including bedrooms and living rooms. The dataset facilitates research on activity recognition, individual identification, and counting using Wi-Fi CSI.

The CSI Trace Dataset for six activities [33] includes CSI data collected from multiple subjects on different days. The objective is to simplify the process of conducting replicable studies on activity recognition using Wi-Fi technology.

The Wi-Fi-Based Human-To-Human Interaction Dataset [34] comprises data from 40 individuals engaged in 12 distinct activities involving interaction with other humans. The data is from both line-of-sight and non-line-of-sight scenarios in indoor environments.

The WiAR [35] dataset contains sixteen activities, including coarse-grained activities and gestures performed by ten volunteers, with every volunteer performing the activities 30 times. The data includes CSI and RSSI.

The listed datasets illustrate the capability of utilising common Wi-Fi infrastructure for discrete detection of human activities. However, finding comprehensive, annotated CSI datasets remains challenging, with many datasets limited in scope or lacking inclusivity [32,34]. Additional extensive and versatile datasets are required to further advance the field of Wi-Fi and 5G/6G sensing technologies.

Several current CSI datasets primarily concentrate on recognising general activities, but they do not provide the specific data required for detecting violence. The scarcity of extensive and varied datasets poses a significant obstacle to research progress in this field. Researchers in this field face a significant obstacle: the limited availability of publicly accessible CSI datasets for violence detection. Additional attempts are necessary to generate and distribute a wide range of annotated datasets in order to advance the development of violence detection with Wi-Fi and 5G/6G sensing approaches.

6. Discussions

The data shown in Table 1 provides a comprehensive overview of the Wi-Fi sensing technology used in different research investigations. An interesting observation is the widespread employment of Intel 5300 NIC for gathering CSI samples, frequently accompanied by SVM classifiers for analysis. To address cost concerns and foster innovation, an alternative approach worth exploring involves the integration of the ESP32 micro-controller, featuring an embedded printed circuit board antenna for CSI data collection. This proposed change necessitates a more thorough investigation into the technological capabilities and implications linked to this alternative hardware selection.

Table 1. Comparison of the Wi-Fi sensing works for violence detection.

Existing Works	Components	Antenna		Spaces Covered	Activity	Methodology
		Transmitter	Receiver			
[21]	Intel5300 NIC network card	1	3	Laboratory, Office, Dorm-Room	Kick, Punch, Slap, Push, Beat, Strangle	PCA—Feature extraction, LSSVM—Classifier
[22]	Intel5300 NIC network card	1	3	Classroom, Narrow Corridor	Push	PCA—to extract common variations, SVM—Classifier
[24]	Intel5300 NIC network card	1	3	Dark room, Laboratory	Fist, Slap, Push, Kick	Gray-Level Co-occurrence Matrix—to extract the texture characteristics of the CSI matrix, SVM—Classifier

6.1. Advantages

Wi-Fi sensing for violence detection using CSI features offers several advantages. Firstly, its non-intrusive nature allows for discreet monitoring, respecting privacy while providing valuable insights into the activities that occur within the environment. The ubiquitous infrastructure of Wi-Fi facilitates violence detection in diverse settings, from public spaces to schools and smart homes, without the need for additional sensor deployment. This approach proves cost-effective by leveraging existing Wi-Fi networks and infrastructure, reducing the financial burden associated with deploying dedicated sensors, and making the technology accessible for implementation in various scenarios. Wi-Fi sensing ensures real-time monitoring, enabling an immediate response to and intervention in potentially violent situations. The ability to perform multi-person tracking using Wi-Fi CSI features allows for the analysis of collective behaviours, contributing to the identification of potential violent incidents. Additionally, the capability of Wi-Fi signals to penetrate walls enhances security measures, enabling violence detection in concealed spaces. Furthermore, the low energy consumption associated with Wi-Fi sensing makes it a sustainable and feasible solution for continuous monitoring over an extended period of time.

6.2. Disadvantages

The limited spatial resolution of Wi-Fi signals can pose difficulties in precisely pinpointing the location of a violent incident, particularly in densely populated or crowded areas. Additionally, vulnerability to signal interference from various sources, such as electronic devices and physical obstacles, may impact the accuracy and reliability of violence detection using Wi-Fi CSI features. Privacy concerns also emerge as a disadvantage, despite Wi-Fi sensing being non-intrusive, as it involves indirectly monitoring individuals within the range of Wi-Fi signals without their explicit consent. Moreover, the effectiveness of violence detection using Wi-Fi CSI features is contingent on the availability and stability of Wi-Fi networks, introducing a dependency that may vary across different environments. Finally, Wi-Fi sensing may struggle to discriminate between violent actions and other activities exhibiting similar patterns, potentially leading to false alarms. These limitations underscore the importance of addressing technical and ethical considerations for the widespread and responsible implementation of Wi-Fi sensing in violence detection applications.

7. Future Directions

The future trajectory of Wi-Fi sensing for violence detection using CSI features involves multifaceted advancements. Primarily, there is a need to develop and refine machine learning algorithms capable of better interpreting the intricate CSI features, thus enhancing the accuracy and reliability of violence detection. Exploring integration with multiple sensors, such as video cameras or audio sensors, is another critical avenue to create a more comprehensive and robust violence detection system. To address privacy concerns, future directions include investigating and implementing privacy-preserving techniques, like anonymisation or encryption, to ensure individual privacy during Wi-Fi sensing for violence detection. The establishment of standardised protocols for Wi-Fi sensing in violence detection is essential to guarantee interoperability and consistency across different systems and deployments.

Advanced real-time decision support systems that not only detect violence but also assist in decision-making for timely and appropriate intervention strategies represent another future direction. Additionally, addressing ethical considerations and engaging with communities are vital to ensuring the responsible and transparent deployment of Wi-Fi sensing technologies for violence detection. Lastly, encouraging cross-disciplinary collaboration among researchers in wireless communication, machine learning, psychology, and sociology enables gaining a more holistic understanding of violence indicators and enhancing the overall effectiveness of Wi-Fi sensing applications.

Furthermore, smartphones have become an essential part of everyone's life. This presents a substantial opportunity; therefore, technologies such as mobile sensing, including 5G/6G sensing, as well as the utilisation of commercial Wi-Fi technologies, offer great potential. The progress made in this research field will facilitate the implementation of an ambient violence detection system in all network-enabled locations. For instance, these systems may be employed in residential dwellings to address instances of domestic violence, in educational institutions to prevent conflicts among children, and in various other public settings to improve the early detection of violent incidents. However, the lack of open-source resources, particularly datasets, has hindered the advancement of research in this field. Creating openly available CSI datasets that cover a wide range of violent actions, such as beating, slapping, strangling, and kicking, would greatly expedite research advancements and facilitate the development of more efficient violence detection solutions.

8. Conclusions

This review paper explored the evolving landscape of violence detection through Wi-Fi and 5G/6G sensing, with a focus on the detailed analysis of CSI features. Evaluation of machine learning algorithms for CSI interpretation reveals the potential for accuracy refinement within violence detection systems. The integration of various sensors and the adoption of privacy-preserving techniques form an accurate approach, addressing both system robustness and individual privacy. Looking forward, the call for standardised protocols becomes apparent, aiming to establish a framework for interoperability and consistency across diverse systems. The proposal of real-time decision support systems, driven by machine learning paradigms, holds promise for going beyond detection to guide timely interventions. Ethical considerations and community engagement emerge as crucial aspects in the responsible deployment of Wi-Fi and 5G/6G sensing technologies. This study envisions a convergence of technological ability, ethical sensitivity, and community collaboration, indicating a transformative time in violence detection. This blend will not only strengthen security measures but also contribute to the establishment of a safer and more secure societal setting.

Author Contributions: Conceptualization, A.Z.K.; methodology, A.K. and A.Z.K.; formal analysis, A.K.; investigation, A.K. and A.Z.K.; resources, A.Z.K.; data curation, A.K.; writing—original draft preparation, A.K.; writing—review and editing, A.K. and A.Z.K.; supervision, A.Z.K.; project administration, A.Z.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Australian Institute of Health and Welfare. Available online: [https://www.aihw.gov.au/family-domestic-and-sexual-violence/resources/fdsv-summary#:~:text=It%20is%20estimated%20that%20of,family%20member%20\(ABS%202023c](https://www.aihw.gov.au/family-domestic-and-sexual-violence/resources/fdsv-summary#:~:text=It%20is%20estimated%20that%20of,family%20member%20(ABS%202023c) (accessed on 2 April 2024).
2. Kouzani, A.Z. Technological Innovations for Tackling Domestic Violence. *IEEE Access* **2023**, *11*, 91293–91311. [[CrossRef](#)]
3. The University of St Andrews. Available online: <https://reportandsupport.st-andrews.ac.uk/support/what-is-physical-violence> (accessed on 2 April 2024).
4. Zhang, T.; Jia, W.; Yang, B.; Yang, J.; He, X.; Zheng, Z. MoWLD: A robust motion image descriptor for violence detection. *Multimed. Tools Appl.* **2017**, *76*, 1419–1438. [[CrossRef](#)]
5. Vijeikis, R.; Raudonis, V.; Dervinis, G. Efficient Violence Detection in Surveillance. *Sensors* **2022**, *22*, 2216. [[CrossRef](#)] [[PubMed](#)]
6. Omarov, B.; Narynov, S.; Zhumanov, Z.; Kumar, A.; Khassanova, M. State-of-the-art violence detection techniques in video surveillance security systems: A systematic review. *PeerJ Comput. Sci.* **2022**, *8*, e920. [[CrossRef](#)] [[PubMed](#)]
7. Hsu, Y.L.; Yang, S.C.; Chang, H.C.; Lai, H.C. Human Daily and Sport Activity Recognition Using a Wearable Inertial Sensor Network. *IEEE Access* **2018**, *6*, 31715–31728. [[CrossRef](#)]
8. Tao, S.; Kudo, M.; Nonaka, H. Privacy-preserved behavior analysis and fall detection by an infrared ceiling sensor network. *Sensors* **2012**, *12*, 16920–16936. [[CrossRef](#)]
9. Wu, F.; Zhao, H.; Zhao, Y.; Zhong, H. Development of a Wearable-Sensor-Based Fall Detection System. *Int. J. Telemed. Appl.* **2015**, *2015*, 576364. [[CrossRef](#)] [[PubMed](#)]
10. Everything RF. Available online: <https://www.everythingrf.com/community/what-is-wi-fi-sensing> (accessed on 2 April 2024).
11. Nami. Available online: <https://nami.ai/blog/what-is-wi-fi-sensing/> (accessed on 2 April 2024).
12. Microwave Journal. Available online: <https://www.microwavejournal.com/articles/40518-wi-fi-sensing-the-next-big-evolution-of-wi-fi> (accessed on 2 April 2024).
13. Kabir, M.H.; Hasan, M.A.; Shin, W. CSI-DeepNet: A Lightweight Deep Convolutional Neural Network Based Hand Gesture Recognition System Using Wi-Fi CSI Signal. *IEEE Access* **2022**, *10*, 114787–114801. [[CrossRef](#)]
14. Ali, M.; Hendriks, P.; Popping, N.; Levi, S.; Naveed, A. A Comparison of Machine Learning Algorithms for Wi-Fi Sensing Using CSI Data. *Electronics* **2023**, *12*, 3935. [[CrossRef](#)]
15. Khalili, A.M.; Soliman, A.-H.; Asaduzzaman, M.; Griffiths, A. Wi-Fi Sensing: Applications and Challenges. *arXiv* **2019**, arXiv:1901.00715. [[CrossRef](#)]
16. Liu, J.; Wang, L.; Fang, J.; Guo, L.; Lu, B.; Shu, L. Multi-Target Intense Human Motion Analysis and Detection Using Channel State Information. *Sensors* **2018**, *18*, 3379. [[CrossRef](#)]
17. Gu, Y.; Ren, F.; Li, J. PAWS: Passive Human Activity Recognition Based on WiFi Ambient Signals. *IEEE Internet Things J.* **2016**, *3*, 796–805. [[CrossRef](#)]
18. Sahoo, A.; Kompally, V.; Udgata, S. Wi-Fi Sensing based Real-Time Activity Detection in Smart Home Environment. In Proceedings of the 2023 IEEE Applied Sensing Conference (APSCON), Bengaluru, India, 23–25 January 2023; pp. 1–3. [[CrossRef](#)]
19. Yang, X.; Cao, R.; Zhou, M.; Xie, L. Temporal-Frequency Attention-Based Human Activity Recognition Using Commercial WiFi Devices. *IEEE Access* **2020**, *8*, 137758–137769. [[CrossRef](#)]
20. Feng, C.; Arshad, S.; Zhou, S.; Cao, D.; Liu, Y. Wi-Multi: A Three-Phase System for Multiple Human Activity Recognition With Commercial WiFi Devices. *IEEE Internet Things J.* **2019**, *6*, 7293–7304. [[CrossRef](#)]
21. Zhang, L.; Ruan, X.; Wang, J. WiVi: A Ubiquitous Violence Detection System with Commercial WiFi Devices. *IEEE Access* **2020**, *8*, 6662–6672. [[CrossRef](#)]
22. Zhou, Q.; Wu, C.; Xing, J.; Zhao, S.; Yang, Q. Enabling Noninvasive Physical Assault Monitoring in Smart School with Commercial Wi-Fi Devices. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 8186573. [[CrossRef](#)]
23. Hsu, F.-H.; Wu, M.-H.; Hwang, Y.-L.; Lee, C.-H.; Wang, C.-S.; Chang, T.-C. WPPD: Active User-Side Detection of Evil Twins. *Appl. Sci.* **2022**, *12*, 8088. [[CrossRef](#)]
24. Liu, H.; Chang, J.; Zhang, L.; Huang, B. CSI-Based Violent Behavior Detection Method. In Proceedings of the 2021 7th International Conference on Computer and Communications (ICCC), Chengdu, China, 10–13 December 2021; pp. 1727–1732. [[CrossRef](#)]
25. Ehatisham-ul-Haq, M.; Awais Azam, M.; Naeem, U.; Amin, Y.; Loo, J. Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing. *J. Netw. Comput. Appl.* **2018**, *109*, 24–35. [[CrossRef](#)]
26. Chen, Y.; Zhang, J.; Feng, W.; Alouini, M.S. Radio Sensing Using 5G Signals: Concepts, State of the Art, and Challenges. *IEEE Internet Things J.* **2022**, *9*, 1037–1052. [[CrossRef](#)]
27. Wymeersch, H.; Shrestha, D.; Lima, C.M.d.; Yajnanarayana, V.; Richerzhagen, B.; Keskin, M.F.; Schindhelm, K.; Ramirez, A.; Wolfgang, A.; Guzman, M.F.d.; et al. Integration of Communication and Sensing in 6G: A Joint Industrial and Academic Perspective. In Proceedings of the 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Virtual, 13–16 September 2021; pp. 1–7.

28. Meneghello, F.; Dal Fabbro, N.; Garlisi, D.; Tinnirello, I.; Rossi, M. CSI Dataset for Wireless Human Sensing on 80 MHz Wi-Fi Channels. *IEEE Dataport* **2022**. [[CrossRef](#)]
29. Sharma, N.; Klein Brinke, J.; Braakman Jansen, L.M.A.; Havinga, P.J.M.; Le, D.V. Wi-Gitation: Replica Wi-Fi CSI Dataset for Physical Agitation Activity Recognition. *Data* **2024**, *9*, 9. [[CrossRef](#)]
30. Huang, S.; Li, K.; You, D.; Chen, Y.; Lin, A.; Liu, S.; Li, X.; McCann, J.A. WiMANS: A Benchmark Dataset for WiFi-based Multi-user Activity Sensing. *arXiv* **2024**. [[CrossRef](#)]
31. Yang, J.; Chen, X.; Wang, D.; Zou, H.; Lu, C.X.; Sun, S.; Xie, L. SenseFi: A Library and Benchmark on Deep-Learning-Empowered WiFi Human Sensing. *arXiv* **2023**. [[CrossRef](#)] [[PubMed](#)]
32. Yousefi, S.; Narui, H.; Dayal, S.; Ermon, S.; Valaee, S. A Survey on Behavior Recognition Using WiFi Channel State Information. *IEEE Commun. Mag.* **2017**, *55*, 98–104. [[CrossRef](#)]
33. Klein Brinke, J. *Channel State Information (WiFi Traces) for 6 Activities*; 4TU.Centre for Research Data: Delft, The Netherlands, 2019. [[CrossRef](#)]
34. Alazrai, R.; Awad, A.; Alsaiy, B.A.; Hababeh, M.; Daoud, M.I. A dataset for Wi-Fi-based human-to-human interaction recognition. *Data Brief* **2020**, *31*, 105668. [[CrossRef](#)]
35. Guo, L.; Wang, L.; Lin, C.; Liu, J.; Lu, B.; Fang, J.; Liu, Z.; Shan, Z.; Yang, J.; Guo, S. Wiar: A Public Dataset for Wifi-Based Activity Recognition. *IEEE Access* **2019**, *7*, 154935–154945. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.