Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 4, August 2026, pp. 3338~3346
ISSN: 2302-9285, DOI: 10.11591/eei.v15i4.11366

Enhancing reliability and security in wireless sensor networks using direct sequence spread spectrum

Rachamadugu Prakash Kumar[1], Durgachandramouli Yenugu[2], Pinjala Naga Malleswari[3], Chavakula Sridevi[4], Kompella Bhaskara Srinivasa Deekshitha Sarma[4], Annam Ramana Kumari[5]
[1]Department of Electronics and Communication Engineering, CVR College of Engineering, Hyderabad, India
[2]Department of Electronics and Communication Engineering, Aditya University, Surampalem, India
[3]Department of Electronics and Communication Engineering, Sasi Institute of Technology and Engineering, Tadepalligudem, India
[4]Department of Electronics and Communication Engineering, Bonam Venkata Chalamayya Engineering College, Odalarevu, India
[5]Department of Electronics and Communication Engineering, Vignan's Lara Institute of Technology and Science, Guntur, India

Article Info

Article history:

Received Sep 9, 2025
Revised May 1, 2026
Accepted Jun 19, 2026

Keywords:

Direct sequence spread spectrum
Interference mitigation
Internet of things
Physical layer security
Wireless sensor networks

ABSTRACT

Wireless sensor networks (WSNs) are increasingly being used in vital environmental tracking, healthcare, and industrial automation, with reliability and security being key concerns. However, the liability to interference, multipath fading, and malicious attacks associated with WSNs is very high due to their limited power, as well as their open medium. This paper investigates the usage of direct sequence spread spectrum (DSSS) to improve the security and reliability of the physical layer in WSNs. DSSS makes it more challenging for narrowband interference to occur, minimizes the bit error rate (BER), and mitigates the effects of eavesdropping. A MATLAB-based simulation model is derived to assess the associated performance of DSSS- constrained WSNs under the additive white gaussian noise (AWGN) and interference conditions. The results indicate an enormous gain over signal-to-noise ratio (SNR), the throughput and the packet delivery ratio (PDR) as against conventional non-spread spectrum transmission. The results show that the usage of DSSS in WSN is most robust and confidential especially for secure and reliable applications in the internet of things (IoT) environments.

Corresponding Author:

Rachamadugu Prakash Kumar
Department of Electronics and Communication Engineering, CVR College of Engineering
Hyderabad, India
Email: prakash.rachmagdu@gmail.com

1. INTRODUCTION

Wireless sensor networks (WSNs) have emerged as a key enabling technology in internet of things (IoT) applications, ranging from environmental monitoring and precision agriculture to healthcare, military surveillance, and industrial automation [1], [2]. Despite their widespread adoption, WSNs face significant challenges including limited energy resources, multipath fading, interference, and security vulnerabilities [3]–[5]. Traditional narrowband communication systems are particularly susceptible to jamming and noise, which degrade reliability and packet delivery performance.

Direct sequence spread spectrum (DSSS) is a spread spectrum technique designed to enhance robustness against interference by spreading the signal using a pseudo-noise (PN) code [6], [7]. DSSS exhibits multipath resistance and provides inherent physical-layer security because the transmitted signal appears noise-like to unintended receivers [8]. In recent years, research has demonstrated that spread spectrum processing greatly enhances both in bit error rate (BER) performance and overall robustness [9].

When used in WSNs, DSSS reduces packet loss, improving network throughput, and extending networks life time through fewer retransmissions due to channel errors. In addition its low probability of interception (LPI) and jam immunity, making highly suitable for mission critical, and security sensitive IoT applications [10].

In this paper, we propose the integration of DSSS into WSN communication to enhance both reliability and security. A MATLAB-based simulation model is developed to evaluate the performance of DSSS-enabled WSNs under additive white gaussian noise (AWGN) and interference scenarios. Key performance metrics such as BER, throughput, and packet delivery ratio (PDR) are analyzed to demonstrate the effectiveness of DSSS compared to conventional narrowband transmission. The rest of the paper is described as follows: section 2, the related works in the field of DSSS in WSNs are discussed. The proposed method of communication using the DSSS is described in section 3. The simulation setup and performance evaluation and the results are presented in section 4. The results that were obtained in this study and their implications are discussed in section 5. Finally, the paper ends with the key findings and future work direction in section 6.

2. RELATED WORKS

In recent years, research has increasingly focused on applying spread spectrum techniques such as DSSS in IoT and WSN-based applications for enhanced security and resilience. Most recent works investigated application of DSSS in IoT and WSN applications to enhance the reliability, security, and energy efficiency of communication. Recent research have investigated DSSS for reliable wireless communications in the presence of difficult channel characteristics. For example, the techniques of communication for ultra-reliable and low latency wireless systems were discussed in [11], focusing on the capability of a strong transmitter in a multipath fading channel. Like that, IEEE [12] introduced the IEEE 802.15.4 standard, with DSSS physical layer to improve interference resistance and to allow energy efficient communication. A machine learning framework for interference sensing and modelling in IoT frequency bands, for the purpose of adapting communication strategies for dense wireless environments was proposed [13]. In addition, there has been a lot of interest in the physical-layer security together with multi-antenna communication. Research by Wu *et al.* [14] has shown that the techniques based on MIMO can enhance the communication reliability and confidentiality by introducing spatial diversity. Interference mitigation and coexistence of other wireless technologies in the ISM 2.4 GHz band was explored, with particular focus on the design of signals that will enable reliable communication [15]. Moreover, [16], [17] highlighted the communication security and reliability issues for healthcare and industrial IoT respectively. The survey in [18] has concluded that spread-spectrum techniques still have a good deal of potential to improve reliability, scalability and security in heterogeneous WSNs. The work that has been done there so far has been aimed at optimizing the design of spreading codes to achieve better communication performance [19] and incorporating cognitive radio concepts to improve spectrum utilization [20]. Secure authentication and trust management for WSNs with IoT is also explored [21], [22]. Lastly, comparative studies [23]–[25] have been performed that illustrate the advantages that DSSS offers in terms of energy efficiency, interference rejection, reliability, and complexity. The key findings of these new studies are summarized in Table 1 highlighting different DSSS enhancement strategies for WSN applications.

Table 1. Summary of related works and literature survey

Title of the paper	Methodology	Key contribution
Ultra-reliable and low-latency wireless communication: tail, risk and scale [11]	URLLC framework	Improved communication reliability.
IEEE Std 802.15.4-2020: IEEE standard for low-rate wireless networks [12]	DSSS-based IEEE 802.15.4 PHY	Enhanced interference resistance.
Machine learning framework for sensing and modeling interference in IoT frequency bands [13]	Machine learning-based interference modeling	Improved interference prediction.
A survey of physical layer security techniques for 5G wireless networks and challenges ahead [14]	MIMO-based physical-layer security	Enhanced reliability and security.
A survey on interference avoiding methods for WSNs working in the 2.4 GHz frequency band [15]	Interference mitigation techniques	Reduced wireless interference.
Securing wireless communications of the internet of things from the physical layer: an overview [16]	Physical-layer security	Improved secure communication.
A survey of cognitive radio handoff schemes, challenges and issues for industrial WSNs [17]	Cognitive radio for Industrial WSN	Improved communication robustnes.
Coexistence management in wireless networks: a survey [18]	Literature survey	Summarized coexistence techniques.

3. PROPOSED METHOD

The proposed work focuses on improving the reliability and security of WSNs by incorporating DSSS at the physical layer of communication. In the conventional WSN model, sensor nodes transmit data using narrowband modulation techniques, which are highly susceptible to interference, multipath fading, and malicious jamming attacks. To overcome these challenges, DSSS is employed to spread the original data signal using a PN sequence before transmission.

In this method, each data bit is multiplied by a high-rate PN code, thereby generating a wider bandwidth signal. At the receiver, the PN code used to spread the signal is passed through a despreader; this prevents replicas of the original signal from other parties without the correct code. To a large extent, this is done to increase resistance to interference and eavesdropping. The system model consists of sensor nodes, a cluster head, and a base station. Each node is equipped with a DSSS transmitter that includes a PN sequence generator, a binary phase shift keying (BPSK) modulator, and a spreading unit. A correlator-based DSSS demodulator is designed at the receiver side to recover the original transmitted data. The proposed system is assessed through the quality metrics BER, throughput, power spectral density (PSD), and resilience against jamming. Additionally, this method integrates lightweight key-based PN code allocation to strengthen security and prevent unauthorized decoding of sensor data. This reduces the vulnerability of WSNs to external attacks while maintaining energy efficiency for low-power IoT devices. Simulation experiments are conducted using MATLAB to compare system performance with and without DSSS.

DSSS-based wireless sensor node communication system, the process begins at the sensor node, where raw environmental data is sensed, digitized, and formatted into packets containing the payload, node ID, and error-checking bits. The data then is also packetized and directed to the spreader where it is multiplied by a high-rate PN code to widen its bandwidth and lower the PSD, as a way of making it resistant to interference. The spread signal is applied to a BPSK modulator, which maps the data chips to corresponding phase shifts (0 or π) of a carrier wave, generating a wideband noise-like transmitted signal. The signal is then transmitted along the wireless channel, having to face path loss, fading, interferences, and noise. At the demodulation, the signal is first received in the BPSK demodulator where it is detected coherently and is recovered to obtain the symbols. The signal that is demodulated is then run through the despreader where a locally generated synchronized PN code is used to compress the signal back into its original narrowband, in the process boosting the desired signal and diffusing noise and interference. Lastly, the result of the despreader is reconstituted into the recoded signal, the same as that used by the source node to send the sensed information, as shown in Figure 1.

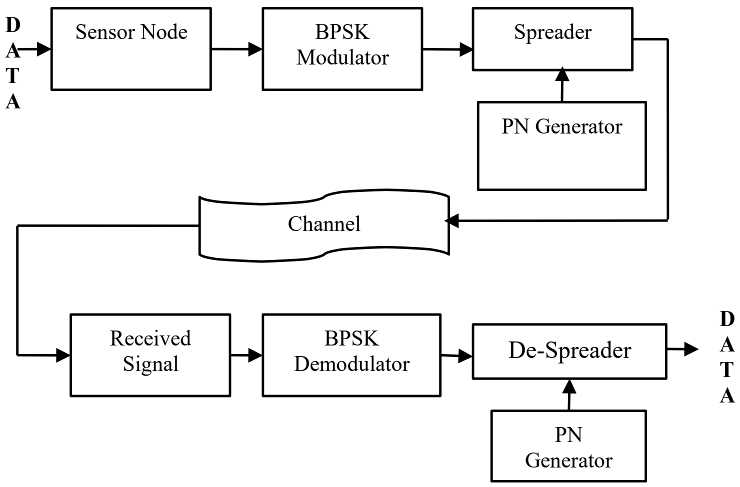

Figure 1. Block diagram of the proposed DSSS-based secure WSN communication system

Starting at the sensor node, a physical transducer (e.g., temperature, vibration, and gas) samples the environment and produces a digital bit stream after simple signal conditioning and ADC. A lightweight packetizer adds a header (node ID, sequence number, and time stamp), a payload (sensor bits), and a short error-control field (CRC). This packet is then passed to the spreading stage, where each data bit is multiplied (chip-wise XOR for {0,1} or ±1 multiplication for BPSK) by a high-rate PN sequence. The PN code is generated by an LFSR (e.g., m-sequence or gold code) with length L_C and chip rate $R_c=G_sR_b$, where Gs is the processing gain and R_b the data rate. Spreading expands the signal bandwidth by Gs, lowering PSD and embedding a “code lock” that only a receiver with the same PN can remove.

The spread chips enter the BPSK modulator, which maps chips {0,1} to {+1,−1} and shapes them with a pulse (typically RRC or NRZ). The result is a wideband, noise-like waveform. A power controller may scale the amplitude to meet the link budget while minimizing energy consumption. The signal thus modulated is then sent into the wireless channel that causes path loss, shadowing, multipath fading, AWGN, and potentially narrowband interference or intentional jamming-exactly what DSSS is intended to be resistant to by virtue of its processing gain Gs.

At the receiver front end, the RF is down-converted and sampled. Timing recovery res synchronizes chip and symbol clocks; carrier recovery eliminates remaining frequency/phase errors. The baseband samples go to the despreader, which multiplies them by a locally generated, time-aligned copy of the same PN code. Proper code synchronization (acquisition then tracking) is essential; a sliding correlator or matched filter searches for the code phase that maximizes correlation, then a delay-locked loop (DLL)/phase-locked loop (PLL) keeps it locked as the channel varies. Despreading re-narrows the desired wideband signal, and interferers and noise are spread, providing a signal-to-noise ratio (SNR) enhancement of about the processing gain (minus synchronization losses). The despread waveform is passed to the BPSK demodulator (correlator or coherent detector). Bit decisions are made by comparing the correlator output to zero; the resulting bit stream is de-packetized and verified by the cyclic redundancy check (CRC). Valid packets are delivered as the received sensor data to the sink/base station. A packet that fails a CRC may be subject to selective retransmission by upper layers, but the lower post-despread BER will tend to mitigate this effect, providing an increase in throughput and energy efficiency.

Security and reliability arise naturally from this flow. The PN code acts as a LPI key: without the correct code and phase, an eavesdropper observes only noise-like energy. Against narrowband interferers or tones, despreading distributes their energy across the wider band, so their impact on any single bit is reduced roughly by 1/Gs. In multipath channels, RAKE-style combining (optional) can align and sum the energy from different paths before demodulation, exploiting DSSS's path diversity. For networks, codes can be per-cluster or per-node to limit cross-correlation; practical choices include Gold or Kasami sets for many users with bounded mutual interference. Finally, selection of Gs is adaptive: high spreading factors in adverse conditions for robustness, low factors in nice conditions to be not so bandwidth/power consuming.

4. RESULTS AND DISCUSSION

The correlation between SNR and BER in the case of WSN using and without DSSS is shown in Figure 2. This observed BER improvement aligns with classical spread spectrum theory [6], [8] and recent WSN implementations [11]-[13]. In both cases there is a clear inverse relationship between SNR and BER; but the system using DSSS is much better in terms of performance. The BER of the conventional system, at lower SNR values, is quite high, which means that it is vulnerable to noise and interference. Conversely, the system enabled by DSSS has significantly lower BER which is around 10 even with noisy channel. This is made possible by the gain of processing that comes with the spreading operation, which spreads the signal power across a wider band and improves the level of interference rejection. The research objective has been met with this improvement in terms of enhancing the reliability of communication in the network of wireless sensor by the spread spectrum methods. The low SNR values of the reduced BER are a confirmation of the resilience of DSSS in the event of impaired channels and narrowband interference. Practically, such an improvement in performance is especially useful in low-power WSN applications in severe or interference-sensitive conditions.

Similar scalability improvements were also reported in DSSS-enabled MIMO WSN architectures and cognitive DSSS systems . The data in Figure 3 presents the correlation in the count of sensor nodes and the normalized throughput in the WSN. The throughput of the conventional system (without DSSS) reduces with the increase in the network size. This is mainly the result of intensified channel contention, interference as well as the occurrence of packet collisions under thick network conditions. In comparison, the system with DSSS enabled has a relatively stable and increased throughput rate despite increasing the number of nodes. This is due to the fact that interference suppression capability of DSSS where spreading minimizes the effect of overlapping transmissions and minimizes multiple-access interference. The obtained findings suggest that DSSS can be used to increase the scaling of the network by maintaining the efficiency of communication in dense networks. This is in direct relation to the research objective of enhancing reliability and performance of WSNs. Practically speaking, the capability of sustaining higher throughput with increasing node density is why the proposed system is applicable to large-scale IoT systems in smart agriculture, environmental monitoring, and industrial sensing systems.

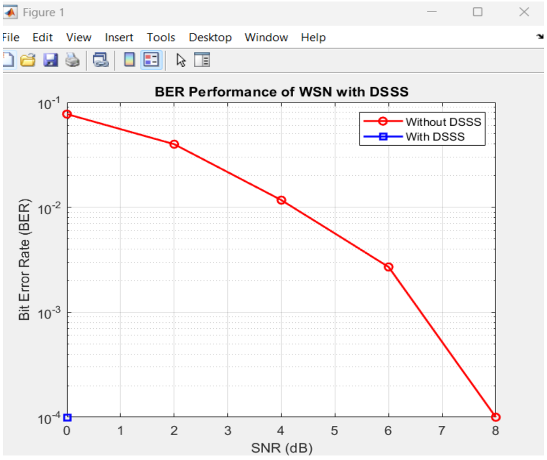

Figure 2. BER performance of with DSSS

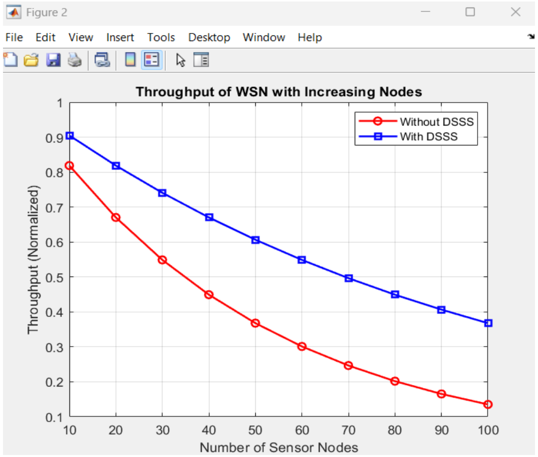

Figure 3. Throughput with increasing nodes

Figure 4 shows the relationship between SNR and PDR of the WSN. Under the standard system with no DSSS, PDR starts at 0.92 at low SNR, and then gradually increases to unity as the channel conditions become good, which in this case is above about 8 dB. This action implies that loss of packets is severe in noisy environment because of increased BER and retransmissions. These results corroborate the findings in healthcare and industrial IoT deployments using DSSS. Conversely, the system, which is made possible by DSSS almost, has a fixed PDR near 1.0 in all SNR values. This regular performance has been attributed to processing gain and mitigation of interferences capability of DSSS, which improves detectability of signals in low SNR conditions. The spreading operation minimizes the chances of observing packet corruption and hence the retransmission is also minimized which enhances the reliability of the entire network. These findings prove that DSSS does not only increase BER performance, but also provides stable packet-level reliability. This is in direct relation to the research purpose of strengthening communication in WSNs. Practically, the ability to deliver packets with the near-perfect performance even in the low SNR conditions is very advantageous in mission-critical IoT, where data integrity and timely delivery are crucial.

The PSD of the DSSS-modulated signal is presented in Figure 5. The spreading operation disperses the signal energy to a very broad frequency band as compared to a conventional narrowband transmission. The effect of this is that the peak PSDis significantly reduced. There are two significant advantages of this spectral spreading. First, the lower peak PSD enhances narrowband interference resistance and premeditated jamming since interference in a thin frequency band has a negligible impact on overall despread signal. Secondly, the noise-like spectral presentation eradicates the possibility of interception therefore improving security in the transmission of WSNs. The spectral spreading behavior is consistent with theoretical models presented in [6], [9].

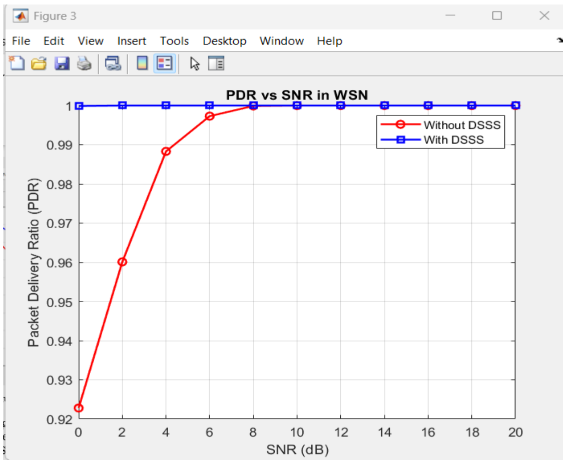

Figure 4. PDR vs SNR in WSN

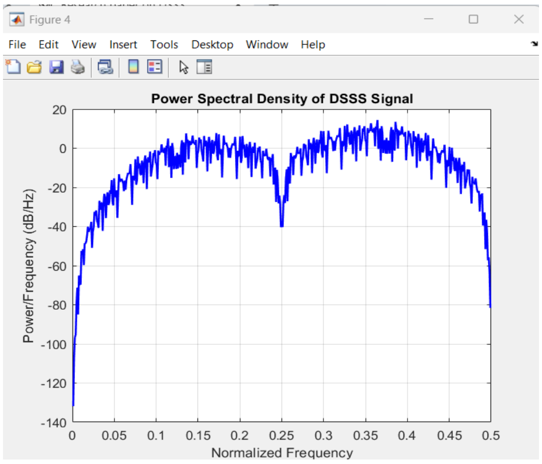

Figure 5. PSD of DSSS signal

The received PSD and theoretical framework of the spread spectrum communication demonstrate that the suggested system relying on the DSSS raises the quality of the BER and the rate of the packet delivery, besides, it increases the security characteristics. Practically, this renders the system particularly suitable in secure WSN systems in industrial monitoring, military sensing systems and critical infrastructure systems where the importance in high regard immunity to interference and eavesdropping. The sharp autocorrelation property is characteristic of gold and m-sequences as discussed in classical spread spectrum studies [7], [8].

Figure 6 shows the properties of autocorrelation of the PN sequence used in the DSSS system. The autocorrelation function has a sharp pronounced peak at the zero lag and very low side lobes at the non-zero lag. This is a basic property of spread spectrum communication as it makes it possible to properly synchronize and despread in an efficient way at the receiver. We know that the sharp autocorrelation peak assures us that the receiver can easily determine when the spreading sequence is correctly aligned hence reducing the self-interference and enhancing the accuracy of bit recovery. Simultaneously, the low side lobes suppress the cross-correlation effects between two or more nodes that are using distinct PN sequences, and facilitates code-division multiple access (CDMA)-based communication in the WSN. This finding supports the theoretical legitimacy of the DSSS implementation and justifies the better BER, PDR, and throughput performance in the former figures. In network scalability terms, a good autocorrelation property allows a number of sensor nodes to co-exist with minimal mutual interference, and as such, it is a system that is applicable to dense WSN applications.

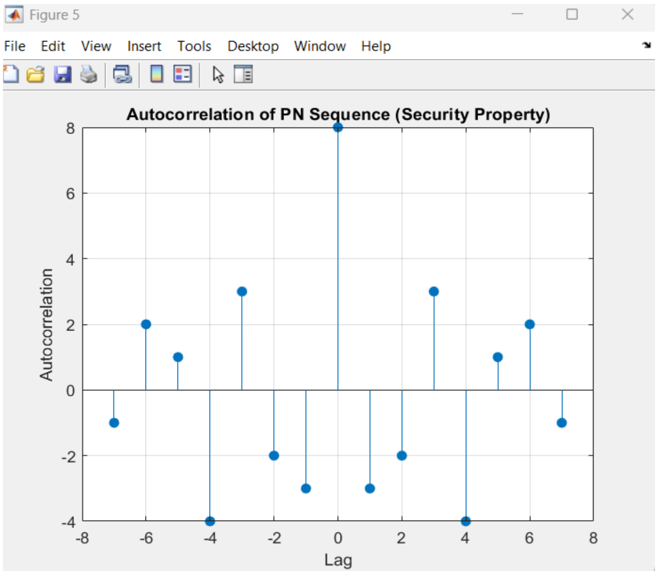

Figure 6. Autocorrelation of PN sequence in DSSS

5. DISCUSSION

The results of the simulation confirm the hypothesis of the research, which states that the incorporation of DSSS in WSN communication results in a higher level of reliability, scalability, and security than the use of a narrowband transmission. The theoretical processing gain benefit in the classical theory of spread spectrum is proved in practical conditions with low SNR by the observed BER improvement [6], [7]. The constant throughput with the growing density of nodes shows the ability of DSSS to reduce multi-user interference and is consistent with the results in DSSS-MIMO and cognitive WSN research works [14], [20]. Moreover, the high PDR is maintained even under different SNR which indicates a high level of robustness to channel impairment, as is also the case in healthcare and industrial IoT applications [16], [17]. Practically, these enhancements greatly lower the number of retransmissions, which thus saves node energy and increases the network lifetime a very important factor when using large-scale IoT deployments. Also, physical-layer security is improved due to the LPI property of the offered architecture, which makes the suggested architecture applicable to mission-critical tasks like military sensing and intelligent infrastructure monitoring.

6. CONCLUSION

This paper explored the effect of the DSSS in the performance of WSNs to improve reliability, scalability and the security of communication in the presence of a noisy and dense network. The research hypothesis according to which DSSS will yield greater error resilience and network robustness than conventional transmission schemes is proved with the help of an extensive simulation analysis. The presented DSSS-based architecture shows a better ability to suppress interference, an increase in the reliability of packets at the packet level, and an increase in the scalability of the system in a multi-node setup. The system is able to enhance communication stability with favourable autocorrelation properties of PN sequences by taking advantage of the spreading mechanism and its favourable autocorrelation properties. The main value of this work is that it offers a systematic performance analysis of DSSS in WSN settings and demonstrates the benefits of the presented tool in the context of reliability, anti-jamming, and multi-user support. The results prove that DSSS can be an appropriate solution to secure and mission-critical applications of WSN.

Future directions can involve real-time hardware deployment through embedded systems, integrating with machine-learning-based adaptive spreading algorithms, testing in realistic fading channel models, and scaling to next-generation IoT and 6G-enabled communication systems.

FUNDING INFORMATION

The authors state no funding involved

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Rachamadugu Prkash Kumar	✓	✓	✓			✓			✓	✓		✓		
Durgachandramouli Yenugu		✓		✓		✓		✓	✓	✓	✓			
Pinjala Naga Malleswari	✓		✓		✓		✓			✓	✓			
Chavakula Sridevi		✓		✓	✓					✓				
Kompella Bhaskara Srinivasa Deekshitha Sarma	✓		✓		✓				✓			✓		
Annam Ramana Kumari	✓			✓		✓				✓				

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing -**O**riginal Draft
E : Writing - Review &**E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–105, 2002, doi: 10.1109/MCOM.2002.1024422.

[2] K. Römer and F. Mattern, “The design space of wireless sensor networks,” *IEEE Wirel. Commun.*, vol. 11, no. 6, pp. 54–61, Dec. 2004, doi: 10.1109/MWC.2004.1368897.
[3] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” *Comput. Networks*, vol. 52, no. 12, pp. 2292–2330, Aug. 2008, doi: 10.1016/j.comnet.2008.04.002.
[4] S. Haykin, *Communication Systems*. New York, NY, USA: John Wiley & Sons, 2001.
[5] H. Chan and A. Perrig, “Security and privacy in sensor networks,” *Computer*, vol. 36, no. 10, pp. 103–105, Oct. 2003, doi: 10.1109/MC.2003.1236475.
[6] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, “Theory of Spread-Spectrum Communications—A Tutorial,” *IEEE Trans. Commun.*, vol. 30, no. 5, pp. 855–884, May 1982, doi: 10.1109/TCOM.1982.1095533.
[7] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. New York: McGraw-Hill, Inc., 1994.
[8] L. B. Milstein, “Interference Rejection Techniques in Spread Snpctrum Communications,” *Proc. IEEE*, vol. 76, no. 6, pp. 657–671, Jun. 1988, doi: 10.1109/5.4455.
[9] D. Torrieri, “Chapter 10 Detection of Spread-Spectrum Signals,” in *Principles of Spread-Spectrum Communication Systems*, Cham: Springer International Publishing, 2015, pp. 565–594, doi: 10.1007/978-3-319-14096-4_10.
[10] C. E. Perkins and P. Bhagwat, “Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 24, no. 4, pp. 234–244, Oct. 1994, doi: 10.1145/190809.190336.
[11] M. Bennis, M. Debbah, and H. V. Poor, “Ultra-Reliable and Low-Latency Wireless Communication: Tail, Risk and Scale,” in *Proc. IEEE*, vol. 106, no. 10, pp. 1834-1853, Oct. 2018, doi: 10.1109/JPROC.2018.2867029.
[12] IEEE Standards Association, *IEEE Standard for Low-Rate Wireless Networks*, IEEE Std 802.15.4-2020, pp. 1–800+, Jul. 23, 2020.
[13] B. Al Homssi, A. Al-Hourani, Ž. Krusevac, and W. S. T. Rowe, “Machine Learning Framework for Sensing and Modeling Interference in IoT Frequency Bands,” *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4461–4471, Mar. 2021, doi: 10.1109/JIOT.2020.3026819.
[14] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, “A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018 , doi: 10.1109/JSAC.2018.2825560.
[15] V. Kulkarni and S. Deshpande, “A Survey on Interference Avoiding Methods for Wireless Sensor Networks Working in the 2.4 GHz Frequency Band,” *J. Eng. Sci. Technol. Rev.*, vol. 13, no. 3, pp. 143–154, 2020, doi: doi:10.25103/jestr13308.
[16] J. Zhang, T. Q. Duong, R. Woods, and A. Marshall, “Securing Wireless Communications of the Internet of Things from the Physical Layer: An Overview,” *Entropy*, vol. 19, no. 8, Aug. 2017, doi: 10.3390/e19080420.
[17] S. S. Oyewobi and G. P. Hancke, “A Survey of Cognitive Radio Handoff Schemes, Challenges and Issues for Industrial Wireless Sensor Networks,” *J. Netw. Comput. Appl.*, vol. 97, pp. 140–156, Nov. 2017, doi: 10.1016/j.jnca.2017.08.016.
[18] A. Hasan, M. M. Islam, and M. R. Amin, “Coexistence Management in Wireless Networks: A Survey,” *IEEE Access*, vol. 10, pp. 53652–53686, 2022, doi: 10.1109/ACCESS.2022.3165223.
[19] D. Torrieri, *Principles of Spread-Spectrum Communication Systems*, 4th ed. Cham, Switzerland: Springer, 2018.
[20] N. Nurelmadina *et al.*, “A Systematic Review on Cognitive Radio in Low-Power Wide-Area Networks for Industrial IoT Applications,” *Sensors*, vol. 13, no. 1, 2021, doi: 10.3390/su13010338.
[21] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, “Authentication protocols for Internet of Things: A comprehensive survey,” *Secur. Commun. Netw.*, no. 1, 2017, doi: 10.1155/2017/6562953.
[22] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, “Physical Layer Security for the Internet of Things: Authentication and Lightweight Security Techniques,” *IEEE Wirel. Commun.,* vol. 26, no. 5, pp. 92-98, October 2019, doi: 10.1109/MWC.2019.180045.
[23] P. Tuset-Peiró, F. Vázquez-Gallego, J. Muñoz, T. Watteyne, J. Alonso-Zárate, and X. Vilajosana, “Experimental Interference Robustness Evaluation of IEEE 802.15.4-2015 OQPSK-DSSS and SUN-OFDM Physical Layers,” *Electronics*, vol. 8, no. 9, 2019, doi: 10.3390/electronics8091045.
[24] Chien-Chung Shen, C. Srisathapornphat, and C. Jaikaeo, “Sensor information networking architecture and applications,” *IEEE Pers. Commun.*, vol. 8, no. 4, pp. 52-59, Aug. 2001, doi: 10.1109/98.944004.
[25] G. J. Pottie and W. J. Kaiser, “Wireless integrated network sensors,” *Commun. ACM*, vol. 43, no. 5, pp. 51–58, May 2000, doi: 10.1145/332833.332838.

BIOGRAPHIES OF AUTHORS

Rachamadugu Prakash Kumar is an Associate Professor in the Department of Electronics and Communication Engineering at CVR College of Engineering, Hyderabad, India, with 18 years of teaching experience. He received his B.Tech. (2006), and M.Tech. (2010) in Electronics and Communication Engineering from JNTUH, and Ph.D. (2024) in Communication and Signal Processing from VTU, Karnataka. His research interests include wireless communications, signal processing, machine learning, and deep learning applications. He is the author/co-author of over 20 research publications. He can be contacted at email: prakash.rachmagdu@gmail.com.

Mr. Durgachandramouli Yenugu has completed his M.Tech. in Department of Electronics and Communication Engineering, Godavari Institute of Engineering and Technology, which is affiliated to JNTUK. He is currently pursuing Ph.D. in Andhra University, Visakhapatnam. His interest research areas are wireless communication, mimo antenna, and image processing. Presently working as Assistant professor in Department of Electronics and Communication Engineering, Aditya University, Surampalem. He can be contacted at email: yd.chandramouli@gmail.com.

Pinjala Naga Malleswari is a Professor in the Department of Electronics and Communication Engineering at Sasi Institute of Engineering and Technology, Andhra Pradesh, India, with 19 years of teaching experience. She received her B.Tech. (2004) and M.Tech. (2009) in Electronics and Communication Engineering from Acharya Nagarjuna University, and Ph.D. (2023) in Communication and Signal Processing from JNTUK, Kakinada. Her research interests include wireless communications, signal processing, biomedical engineering, and deep learning. She has authored/co-authored over 20 research publications. She can be contacted at email: pinjalamalleswari@gmail.com.

Chavakula Sridevi is a Professor in the Department of Electronics and Communication Engineering, Bonam Venkata Chalamayya Engineering College, Andhra Pradesh, India, has 19 years of teaching experience. She received her B.E. (1998) in Electronics and Communication Engineering from Andhra University, Andhra Pradesh, and M.Tech. (2006) in Microwave Engineering from Acharya Nagarjuna University. She is currently pursuing the Ph.D. degree at JNTUK, Kakinada, India. Her research interests include antennas, wireless communications and signal processing. She has published more than 26 research papers in reputed journals and conferences. She can be contacted at email: chavakula.sridevi@gmail.com.

Kompella Bhaskara Srinivasa Deekshitha Sarma is a Professor in the Department of Electronics and Communication Engineering in Bonam Venkata Chalamayya Engineering College, Andhra Pradesh, India, has 25 years of teaching experience. He received his Ph.D. in Signal Processing and VLSI from JNTUH, Hyderabad, in 2015. His research interests are primarily in the area of signal processing, as well as artificial intellegence, machine learning, and deep learning applications, where he is the author/co-author of over 45 research publications. He is the author of Embedded Systems text book. He has 6 patents and attended 15 national and international conferences. He also attended 25 workshops. He can be contacted at email: drkbsdsarma.bvce@bvcgroup.in.

Annam Ramana Kumari is an Associate Professor in the Department of Electronics and Communication Engineering, Vignan's Lara Institute of Technology and Science, Andhra Pradesh, India, with 15 years of teaching experience. She received her B.Tech. (2005) in Electronics and Communication Engineering and M.Tech. (2011) in VLSI System Design from JNTUK, and Ph.D. (2023) in Image Processing from JNTUA, Ananthapur. Her research interests include Image Processing, biomedical engineering and deep learning applications, where she is the author/co-author of over 10 research publications. She can be contacted at email: ramani.etm@gmail.com.