FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 20-27 | e-ISSN: 2347-470X

Parameters Measurement and Secrecy Diversity Analysis for Physical Layer Security in WSNs using Projection Pursuit Gaussian Process Regression

Shruti Sharma*
[1]*CEO, Brindavan Group of Institutions, Dwarakanagar, Bagalur Main Road, Yelahanka, Bangalore-63, Karnataka; ceo@brindavancollege.com*

***Correspondence:** Shruti Sharma; ceo@brindavancollege.com

ABSTRACT- Wireless sensor networks are specialized networks, geographically dispersed monitors that keep track of environmental external factors and conduct the collected information to a centralized opinion. The rapid growth of wireless sensor networks and its connected have pushed the saturation level of the communication. Moreover, the information passed is prone to the attacks and hence researchers have considered these as crucial factors in wireless sensor networks. Physical layer security is the one of the main approaches to ensure the secrecy of wireless sensor networks and has been attained with several encryption and signal processing approach. In our approach we propose a novel Projection Pursuit Gaussian Process regression (PPGPR) technique to analyze the diverse secrecy of physical layer in wireless sensor networks. The proposed approach is utilized to safeguard the sensitive data with secured physical layer. Simulations are performed and made an analogous study with state-of-art works to ensure the secrecy of the proposed work. The proposed work can use for the secured wireless communication with higher secrecy capacity than the existing approaches. The performance is analyzed with the parameters such as secrecy capacity, secrecy outage probability, packet delivery ratio, secrecy throughput, and energy consumption.

Keywords: Wireless sensor networks, Physical layer security, Gaussian process regression, diverse secrecy.

ARTICLE INFORMATION

Author(s): Shruti Sharma;
Received: 31/10/2023; **Accepted**: 28/12/2023; **Published**: 20/01/2024;
e-ISSN: 2347-470X;
Paper Id: IJEER 3110-23;
Citation: 10.37391/IJEER.120104
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-12/ijeer-120104.html

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

External variables including weather, vibrations, air quality, moisture, and pressure measured by television stations. When comparing with ad hoc networks [1] with wireless connections based on internet access and occurrence of systems on its own to communicate information collected by sensors remotely, these networks keep close tabs on environmental factors including stress, noise, and humidity. Contemporary networks are mutual, allow to manage sensory performance and a collection of knowledge, the system formation was stimulated with military uses such as battlefield monitoring [2].

Such systems are utilized in commercial and residential usage, including agricultural [3] commercial automation, computer maintenance, and usage by consumers. The node present in the web-based system that varies from the handful to numerous or several thousand in which the additional sensors link to each node [4]. Whereas, the proportions of nanoscale never realized, an imaging node may vary in shape from a pair of sneakers to conceptually a particle of particles, according to difficulty of node, prices of sensor node that differ from a some to countless bucks.

Assets including vitality, recollection, computing acceleration, and transmission [5] throughput are limited by cost and dimension restrictions, commercial sensor networks with wireless connections provide a number of cost-cutting advantages overall. Employing wireless technology effectively allows businesses to cut labor costs, increase environmental sustainability, and enhance reliability. These networks are susceptible to a range of assaults, including interference, counterfeiting, and surveillance. A significant difficulty is maintaining the integrity of the system and all the information it gathers, it is frequently set up in settings with a lot of connected network disturbance.

Secrecy [6] is described as the variance between the greatest eavesdropper velocity and the primary interaction channel's frequency, whatever occurs when a magnetic field departs our gadget is described in the layer known as physical. Secure wireless networks are essential for preventing unauthorized access to personal information, although the networks using Wi-Fi utilize electromagnetic waves to transport data, anybody within proximity to the signal generated by the network has the ability to gain access to any information being delivered, making them especially susceptible to intrusions. Utilizing the communication channel's physical attributes to establish physical layer security (PLS) [7] protects our data from eavesdroppers. The traditional right to the privacy of letters the obligation to preserve the secret of correspondence, along with the message itself, it also safeguards the details of whenever and to where any communications were originally transmitted.

It costs less to establish and sustain internet connections that are wireless, more quickly and more rapid data transmission is achieved, decreased construction and upkeep costs in comparison to other infrastructures. Everywhere, at any moment, can connect to a wireless network. It is more vulnerable since interaction takes place in public, resulting in unreliability, greater susceptibility to intrusion, and a higher probability of blocking, in contrast, the gearbox speed is slower, it has a constrained capacity for communication, and is vulnerable to safety holes on the network, broadband networks [8] are vulnerable to hacking.

Secrecy capacity of the physical layer can ensure the security of the communication among the wireless sensor networks. To attain this, we propose a novel approach known as Projection Pursuit Gaussian Process regression (PPGPR) technique which can be used to analyze the secrecy of the physical layer. Major contributions are,

- To design the system model of the physical layer with three nodes such as Alice, Bob, and Eve with channels such as main channel and write tap channel. To avoid the interception of Eve the Alice must ensure security over the sensitive data.
- For secrecy analysis the proposed PPGPR approach is used to predict the capacity of the secrecy of the physical layer.

The remaining section of paper is arranged as: In *section 2*, the literature survey is examined with the merits and demerits. The system model is entitled in *section 3*, the proposed approach is elucidated with more context in *section 4*. In *section 5* the simulation of the work is enclosed with the comparative study. The summary of the work is enclosed in *section 6*.

2. LITERATURE SURVEY

Guo et al. [9] have implemented a threshold-based scheduling scheme for a multiuser Satellite communication method's secure physical layer in the scenario of several listeners. When the eavesdropper is not accessible, a closed-form equation for the likelihood of confidentiality outages is developed for an undetected monitoring situation. The system under consideration has been deduced using closed-form formulations. Asymptotic solutions for the Standard Operating Procedure have also been produced to get a greater understanding of high noise levels. Numerical outcomes demonstrated that the strategy provided a substantially effective technique to assess the privacy efficiency of SatComs. Hence, it is an impossible assumption and extremely constrained in real-world circumstances.

Khoshafa et al. [10] have presented a cooperative system model for the wireless network's physical component protection by enhancing Device-to-Device (D2D) communications with the use of an underlay transmission. The device functions as a benevolent suppressor to weaken the wiretapped transmission at a surveillance device in exchange for being permitted to occupy the frequency band of the wireless network. The investigation and testing demonstrate that collaboration improves the D2D breakdown probability. But in terms of devices, space, and strength, several transmission chains linked to numerous antennas are costly.

Singh et al. [11] have measured the Free-space optical-radio frequency synchronized wireless information and power transfer (FSO-RF SWIPT) model. When a listener has access to the radio frequency connection, on the other hand, the system dependability increases with effective physical activity. As a result, connections need to be created so that, in the event of transparent surveillance, effective PAs may be utilized to present high levels of safety, while, in the event of RF tracking, the innovator has the adaptability to reduce the effectiveness of PAs in order to create a protected communication channel between those being monitored. Hence, the requirements of wireless communication cannot be met by standard encryption procedures.

Chen et al. [12] have developed a non-orthogonal multiple access enabled (NOMA-enabled) underlay physical layer security (PLS) confidentiality capability that is improved by the signaling technique. Additionally, the power being restricted is employed to ensure the regular transmission of PU while taking into account the disruption induced by supplementary broadcasters for a persistent user. This transmission method can efficiently increase the network under consideration's spectrum utilization while simultaneously ensuring the safety of information. But because of widespread access, spectrum resources are now limited and congested.

Li et al. [13] have demonstrated the safety and reliability trade-off (SRT) in which there is a singular cluster head (CH), a number of members, and a single eavesdropper (E) and the observer tries to intercept the private communication between the different users and his counterpart. Additionally, by describing the asymptotic activities of the likelihood of failure by a specific intersection frequency in the large noise-to-signal area, and doing a confidentiality variance examination for each of the proposed methods. It improves the system's gearbox safety and dependability. Nevertheless, there is greater processing and transmission capability.

Tashman et al. [14] have designed a single-input-multiple-output (SIMO) system that explores the protection of the physical layer across cascading layers that are disappearing. Both the receiver at the endpoint and the observer uses different antennas and combine several reproductions of the received information using a maximum rate. Also, two metrics the chance of a privacy loss and the possibility of a greater than zero privacy capacity, were used to assess the degree of confidentiality. More antennae can be used at the legal receiver to increase the secrecy of the secondary user. However, it may not be able to keep up with the unprecedented rise in the need for transmission.

Choi et al. [15] suggested a space time line codes (STLCs) method to secure multiple access points for single-antenna consumers enabling no coherent identification at the genuine access point, requiring channel state information (CSI), and achieving complete geographic variety. A significant number of antennas are needed to reduce disturbances between users because antennas are divided into several clusters to simultaneously broadcast numerous streams of information. The suggested solution, however, boosts the cumulative secrecy level while using significantly fewer broadcast antennas. Hence, the consequences of linked networks should be examined.

Wang et al. [16-18] highlighted Wyner's wiretap model with two-Nakagami disappearing pathways, the privacy function of wireless portable device network connections. Additionally developed were the precise closed-form equations for the reduced constraint for the ideal application System. It examined and verified the radio-frequency mobile detector transmission systems' privacy efficacy using simulators. The transmission antenna increases performance to optimize the position. However, the channel was not completely self-sustaining in the real world.

3. SYSTEM MODEL

The system model of physical layer of wireless sensor networks is depicted in *figure 1* and it is employed with three communication nodes. The physical layer of WSNs is responsible for transmitting raw binary data over the wireless medium. It deals with the transmission and reception of signals, modulation and demodulation, channel access mechanisms, and physical characteristics of the wireless communication medium. It's important to note that the specific details of the physical layer can vary depending on the wireless communication standard used in the WSN, such as Zigbee, Bluetooth, or IEEE 802.15.4. The design choices are also influenced by the application requirements, environmental conditions, and energy constraints of the sensor nodes.

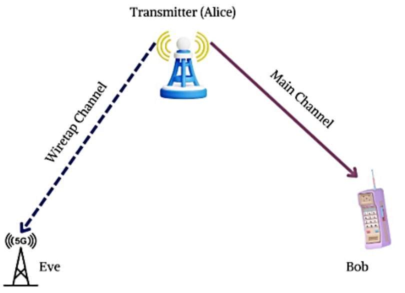

Figure 1: System Model of Physical layer of the wireless sensor networks

The initial node is named as legitimate transmitter and also termed as Alice in network security jargon [19]. The second node is known as Bob the intended receiver and the last one is eavesdropper also termed as Eve. The channel that formed between first and second node i.e., is Alice and Bob is termed as legitimate channel and formed among the Alice and Eve is termed as Eavesdropper or wiretap channel. The sensitive data are transformed to the Bob by the Alice and the decoding is intended in the Eve node after receiving the data. Hence it is necessary to transmit the data with high security from Alice to Bob to avoid the interception of Eve [20]. The secrecy of the wireless sensor networks can be achieved with the signal processing approaches with the deployment of channel features, noises, fading, and interferences. Another important parameter to be considered while deeming the wiretap channel is the presence of channel state information (CSI) of each node. The CSI is not a constant value and varies with nodes and it would be partial, complete, or null.

4. PROPOSED DIVERSE SECRECY ANALYSIS AND ENHANCEMENT APPROACH

This section is to extend the diverse secrecy analysis and enhancement approach in wireless sensor networks with the novel approach known as Projection pursuit Gaussian process regression method. This method ensures the positive secrecy and the brief details is presented in the following section.

In the context of wireless sensor networks (WSNs), combining diverse secrecy analysis with an enhancement approach using Projection Pursuit and Gaussian Process Regression can be an interesting and challenging task. Here's a more detailed approach:

Data Collection and Preprocessing:

- Collect data from the wireless sensor network, including relevant parameters such as sensor readings, network traffic, and security-related events.
- Preprocess the data to handle missing values, outliers, and ensure it is suitable for analysis.

Projection Pursuit in WSN:

- Apply Projection Pursuit to identify relevant features or projections in the high-dimensional sensor data.
- The goal is to uncover hidden structures that may be indicative of security threats or vulnerabilities.

Gaussian Process Regression in WSN:

- Use Gaussian Process Regression to model the relationships between the identified features.
- Train the model on historical data to predict future sensor readings or potential security incidents.

Diverse Secrecy Analysis in WSN:

- Define diverse secrecy dimensions relevant to WSNs, such as confidentiality, integrity, and availability.
- Evaluate the model's predictions in the context of these secrecy dimensions.

Enhancement Approach in WSN:

- Based on the analysis, identify areas of improvement for the wireless sensor network's security.
- Implement enhancements such as improved encryption, anomaly detection algorithms, or dynamic reconfiguration strategies.

Feedback Loop:

- Continuously monitor the wireless sensor network and gather new data.
- Update the Projection Pursuit and Gaussian Process Regression models periodically to adapt to evolving network conditions and emerging security threats.

Security Policy Integration:

- Integrate the findings into the overall security policy of the wireless sensor network.
- Ensure that the enhancements align with the broader security goals and policies.

Documentation and Reporting:

- Document the results of the diverse secrecy analysis and enhancement approach.
- Provide reports and insights to relevant stakeholders for decision-making.

The success of this approach depends on the quality and representativeness of the data, the choice of features, and the appropriateness of the Gaussian Process Regression model. It's also important to consider the practical aspects of implementing enhancements in a real-world wireless sensor network. Regular updates and adaptation to new security challenges are crucial for the long-term effectiveness of the approach.

4.1 Projection Pursuit Gaussian Process regression (PPGPR)

For analyzing the secrecy of the physical layer [17] we have taken the multi-dimensional functions to denote the most intricate form. The projection pursuit regression function can be formulated as,

$$m(y) = g(W_1^T y, W_2^T y, \ldots\ldots., W_N^T y) \qquad (1)$$

Here, the positive integer is N with the additive function of g and unknown vectors $W_1, \ldots.., W_N$. The additive function can be written as,

$$g(W_1^T y, W_2^T y, \ldots., W_N^T y) = g_1(W_1^T y) + g_2(W_2^T y) + \ldots + g_N(W_N^T y) \qquad (2)$$

The univariate functions are defined as $g_1, \ldots.., g_N$. Moreover, the projection pursuit model can be implied in a four-layer neural network form as depicted in *figure 2*. The only difference between the neural networks and projection pursuit approach is activation function. In neural networks the activation functions are fixed and in projection pursuit the activation function is a measured one. The hidden layers are considered as transformation layers [18].

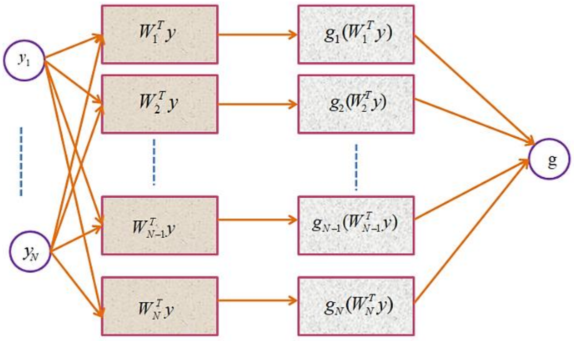

Figure 2: PPGPR with Neural network structure

The implementation of multivariate non-parametric regression is effectuated with the reduction of single index model with N=1. The proposed approach utilized projection pursuit Gaussian process regression approach and the underlying functions are reconstructed using below points.

- The parametric weight$W = (W_1, W_2, .. W_N)$ is computed.
- Gaussian registration process (W) gives the combination function g is reconstructed.

Where, $Y = (y_1, y_2, .. y_N)^T, y_j \in \Re^d forj = 1,2,..,m$ denotes the design matrix and $Y = \left(g(y_1), g(y_2), \ldots., g(y_m)\right)^T$ is the response. The Gaussian realization process is g with it has the function of additive correlation [23].

Select Was initial weight parameter and the iterative approach train the proposed model depending upon the initial weight, the starting correlation matrix

$k_W = \left(\frac{1}{N}\sum_{k=1}^{N} \vartheta\left(W_k^T(y_j - y_k)\right)\right)_{j,k}$ is computed.

$$\vec{g}\,(y) = R^T(W^T y)(k_W + \gamma I)^{-1} X \qquad (3)$$

The numerical stability is enhanced by the term of nugget is γ. Gaussian regression process of log likelihood function is maximized [21].

$$\underset{W}{Min}(I(W)) = \underset{W}{Min}(X^T(k_W + \gamma I)^{-1} X + log\, det(k_W + \gamma I)) \qquad (4)$$

The model loss is $I(W)$.

$$\frac{\partial(I(W))}{\partial W_k} = -\frac{1}{N}\sum_{j=1}^{m}\sum_{k=1}^{m}\left(X^T k_W^{-1}\frac{\partial k_W}{\partial W_k} k_W^{-1} X + Tr(k_W^{-1})(y_j - y_k)\right)^T \qquad (5)$$

The below facts of Matern correlation function computes the matrix derivation k_W.

$$\frac{\partial}{\partial y}\vartheta(y; v, \beta) = -\frac{2v\beta^2 y}{v-1}\vartheta\left(\sqrt{\frac{v}{v-1}y; v-1, \beta}\right) \qquad (6)$$

Iteratively update the gradient decent model.

$$W_k \leftarrow W_k - \lambda\frac{\partial l(W)}{\partial W_k} \qquad (7)$$

The step length is λ. By using equation (3), reconstruct when the techniques met the stopping criterion. The number of epochs is selected to implement early stopping criteria and avoid over fittings [22]. The co-variance functions are N and $\lambda$to adjust the parameter activity. For parameter tuning the below mentioned general suggestions are followed.

- Due to over fit with smaller size of samples, the covariance of hyper parameters is computed using ML estimators.
- The stable training procedure is maintained and the cross validation find appropriate learning rate λ.
- Till the testing point performance initiate to deteriorate, the representative node size N is increased.
- When the number of epochs to neglect over fitting, the early stopping policies are adopted in the training procedure.
- The covariance function based hyper parameters are selected using cross validation.

The optimal parameters may vary depending on the specific characteristics of your data and the goals of your analysis. The model's performance using validation data or cross-validation to ensure that your chosen parameters generalize well to unseen data.

Joint Considerations:

Cross-Validation: Use cross-validation to assess the performance of different parameter choices. This is crucial to avoid overfitting to the training data.

Grid Search or Random Search: For both Projection Pursuit and Gaussian Process Regression, consider using grid search or random search to explore the hyperparameter space efficiently.

Domain Knowledge: Leverage domain knowledge to guide your choices. For example, if you know that certain features are more important in your data, you might emphasize them during the Projection Pursuit analysis.

Iterative Refinement: It's often an iterative process. Start with a broad search, evaluate performance, and then refine your parameter choices based on the results.

4.2 Proposed PPGPR based Diverse Secrecy Analysis

The performance of the physical layer is analyzed with the maximized secrecy rate attained with the proposed PPGPR approach. The proposed approach ensures the maximum rate in which the sensitive data are transmitted with the decoded information and the legitimate or authorized receiver with randomly small error. The presence of non-Gaussian distribution also affects the secrecy rate. The secrecy rate is accomplished by the derived SNR expressions and overall secrecy rate using the proposed PPGPR can be framed as below,

$$C_0^D = (C_0^H - C_0^L)^+$$

$$C_0^D = (log(1+\zeta_H) - log(1+\zeta_L))^+ \qquad (8)$$

The capacity of the receiver channel to receive the information is taken as C_0^D and the capacity of the eavesdropper channel is C_0^L. The capacity of the eavesdropper and the relay incorporated with the highest signal reception is given as $\zeta_H$and ζ_L. Since the noise at the eavesdropper is unknown the proposed approach can provide secrecy by analyzing the worst-case scenario. The security at the physical level can be ensured when the SNR at receiver must be higher than the maximum SNRs at the eavesdropper and can be formulated as,

$$\zeta_H > \zeta_{Lmax} \qquad (9)$$

The transmission of data can secure when the $\zeta\ max\{\zeta Ln\}_{Lmax}$.

5. EXPERIMENTAL INCESTIGATION AND DISCUSSION

This section verifies proposed frameworks performances with respect to the different measurement criterion as well as state-of-art approaches namely TS [9], FSO-RF SWIPT [11], NOMA [12] and SRT [13].

5.1 Evaluation Measures

Few of the proposed secrecy model performance is enhanced using different evaluation measures namely the secrecy throughput, probability for secrecy outage, capacity of secrecy, Fractional equivocation and etc.

The capacity of secrecy (*CS*) is the variation among the channels of main as well as wiretap. Below expression formulates the case of quasi static fading channel in *CS*.

$$CS = max\,i\,mum\{B_C - E_C, 0\} \qquad (10)$$

Both wiretap and main channels are $E_C$and B_C.

The capacity of secrecy tends down the rate of secrecy target is described by the probability of secrecy outage (PSO). When occurring secrecy outage, the present *CS* is never more to target of pre-established PS.

$$PSO = Pb\{CS(\delta_B, \delta_E) < PS\} \qquad (11)$$

where, Pb is the probability with δ_B and δ_E are two squared random variables.

Because of the characteristics of propagation medium fading, the random quantity is fractional equivocation (FE). Below formula provides the fading realization of fractional equivocation.

$$\Delta = \begin{cases} 1, if\, E_C \le B_C - PS \\ (B_C - E_C)/PS\, , if\, B_C - PS < E_C < B_C \\ 0, if\, B_C \le E_C \end{cases} \qquad (12)$$

The secrecy performance is assessed using throughput in the design of secure transmission. The confidential transmission of data defines the secrecy throughput.

5.2 Performance Analysis

The probability of secrecy outage (PSO) with its comparative result is plotted in *figure 3*. Rapidly increase the PSO when the SNR (dB) changes from 0 to 25.

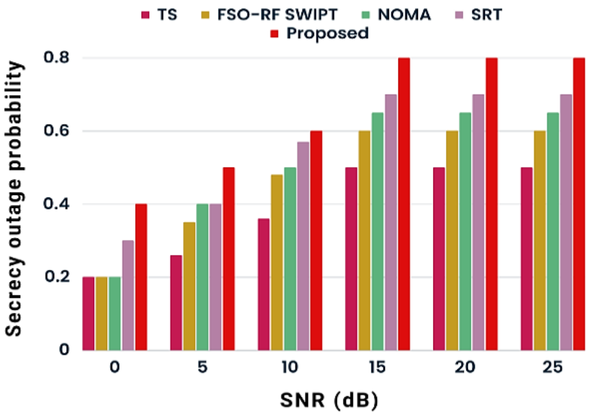

Figure 3: Performance analysis of probability for secrecy outage

The proposed methods with existing models of TS [9], FSO-RF SWIPT [11], NOMA [12] and SRT [13] are used to analyze the PSO performance. Based on each state-of-art methods, the lower secrecy outage probability with higher PSO is attained in each SNR values. The transmitting power reduction leads to desired receiver. At the SNR value of 25th, each method like TS [9], FSO-RF SWIPT [11], NOMA [12] and SRT [13] and proposed validates 0.5, 0.6, 0.65, 0.7 and 0.8 of probability of secrecy outage values. Though, the proposed authenticate superior probability of secrecy outage than the existing methods.

The secrecy capacity is analyzed in *figure 4* by using the state-of-art methodologies like TS [9], FSO-RF SWIPT [11], NOMA [12] and SRT [13] with proposed approach. Vary the SNR level from 0 to 25 to execute the secrecy capacity measurement in terms of bits per Hz. The plots slowly increase from 0 SNR level to the highest score secrecy capacity of SNR level is 25.

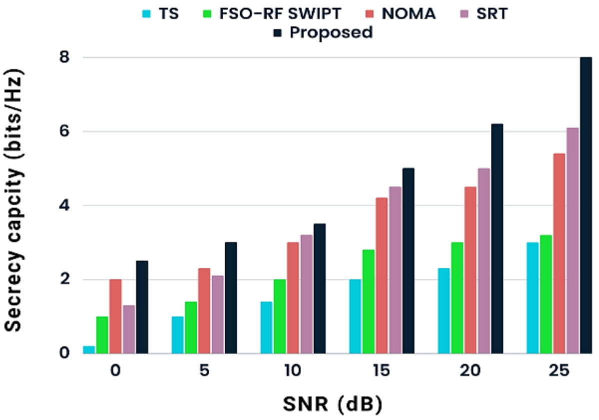

Figure 4: Performance measurement of secrecy capacity

Figure 5 outlines the graphical representation to reveals the performance of average fractional equivocation. Here, the average fractional equivocation of proposed method is investigated by using the target of pre-established as is from the ranges of 0.5, 0.6 and 0.7 respectively. This graph exposes that the proposed approach with its PS rate gradually decreases with respect to the variances from one to six. But the PS rate increases the proposed average fractional equivocation get increased gradually.

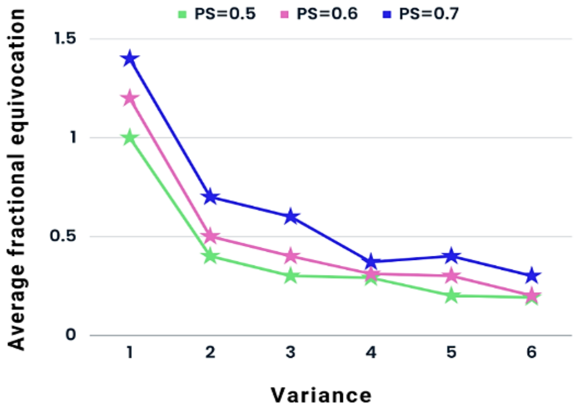

Figure 5: Performance investigation of average fractional equivocation

The performance investigation of secrecy throughput is as shown in *figure 6*. The methods of TS [9], FSO-RF SWIPT [11], NOMA [12], SRT [13] and proposed are selected to compute the secrecy throughput. By this plot, the graphical charts expose the trust factor and the secrecy throughput gets changed with respect to each method.

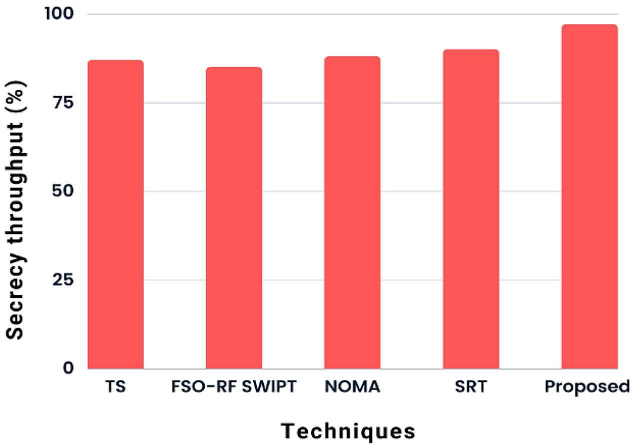

Figure 6: Performance investigation of secrecy throughput

The PDR with its comparison is measured in *table 1*. The existing methodologies namely TS [9], FSO-RF SWIPT [11], NOMA [12] and SRT [13] with proposed techniques is to compute the percentage of PDR is 74%, 82%, 87%, 91% and 97.2%. Besides, the proposed method beat the existing techniques with respect to the result of packet delivery ratio.

Table 1: State-of-art measurement of packet delivery ratio (PDR)

Methods	PDR (%)
TS [9]	74%
FSO-RF SWIPT [11]	82%
NOMA [12]	87%
SRT [13]	91%
Proposed method	97.2%

The measurement of communication overhead performance is plotted in *figure 7*.

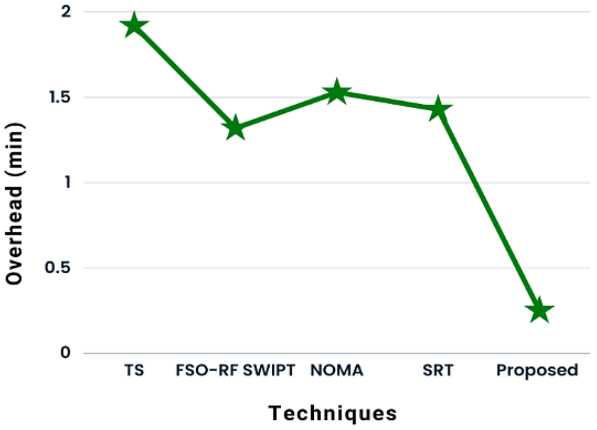

Figure 7: Performance measurement based on communication overhead

Performance analysis-based energy consumption (J) is displayed in *table 2*. The energy consumption increases with the attacks that are if the Eve intercepts, then it will increase the energy consumption of the network. The proposed approach effectively avoids the interceptions and then the consumption of the energy reduced, thus the energy consumed by the proposed work is 16.83J and the other approaches TS [9], FSO-RF SWIPT [11], NOMA [12] and SRT [13] consume energy of 67.89J, 98.32J, 121.63J, and 56.39J.

Table 2: State-of-art measurement of energy consumption

Methods	Energy consumption(J)
TS [9]	67.89
FSO-RF SWIPT [11]	98.32
NOMA [12]	121.63
SRT [13]	56.39
Proposed method	16.83

Figure 8 explains the performance investigation of overall efficiency. This graphical plot shows the overall efficiency of TS [9], FSO-RF SWIPT [11], NOMA [12], SRT [13] and proposed methods.

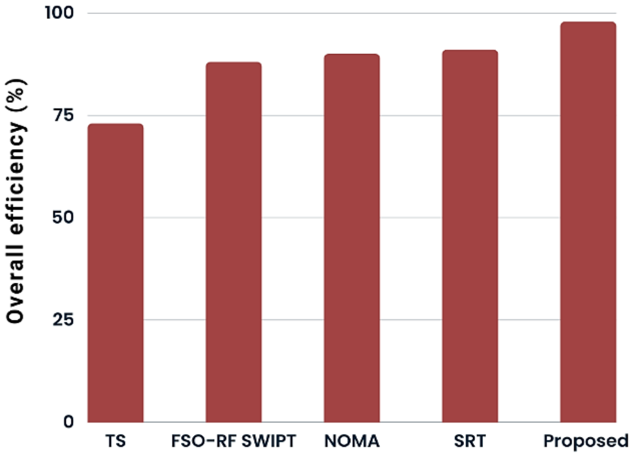

Figure 8: Performance assessment for overall efficiency

6. CONCLUSION

In a nutshell the security of the Physical layer of wireless sensor networks is very important to analyze the secrecy capacity. For that Secrecy outage probability, secrecy capacity, and secrecy throughputs are important. To attain this, we proposed an innovative approach known as Projection Pursuit Gaussian Process regression (PPGPR) which effectively analyzes the physical layer security. Moreover, it also helped to prevent the interception of Eve with other main channel communication and reduces the leakage of secret messages. Meanwhile, the proposed approach increased the secrecy capacity, packet delivery ratio, secrecy throughput and reduces the energy consumption with the prevention of interruption of Eve in the communication channel. Further, the performances of proposed work were compared with state of art works such as TS, FSO-RF SWIPT, NOMA and SRT and our work ensures better secrecy than other approaches with the capacity of 8 bits/Hz at 25th dB of SNR and reduced energy of 16.83J. The future of parameters measurement and secrecy diversity analysis in Physical Layer Security for WSNs will likely involve a multidisciplinary approach, combining expertise in wireless communication, cryptography, machine learning, and network security.

Author Contributions

Shruti Sharma; Study conception, design, data collection, analysis and interpretation of results; draft manuscript preparation, reviewed the results and approved the final version of the manuscript.

Acknowledgments

The authors would like to thank the reviewers for all of their careful, constructive and insightful comments in relation to this work.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] Xu, J.; Yuen, C.; Huang, C.; Ul Hassan, N.; Alexandropoulos, G.C.; Di Renzo, M.; Debbah, M. Reconfiguring wireless environments via intelligent surfaces for 6G: reflection, modulation, and security. Science China Information Sciences 2023, Volume 66, No 3, pp. 130304.

[2] Al-Shareeda, M.A.; Anbar, M.; Hasbullah, I.H.; Manickam, S. Survey of authentication and privacy schemes in vehicular ad hoc networks. IEEE Sensors Journal 2020, Volume 21, No. 2, pp. 2422-2433.

[3] Sehito, N.; Yang, S.; Ali, E.M.; Khan, M.A.; Larik, R.S.A.; Bari, I.; Kamal, M.M.; Khan, S.; Alibakhshikenari, M.; Limiti, E. Physical layer secrecy by power splitting and jamming in cooperative multiple relays based on energy harvesting in full-duplex network. Electronics 2021, Volume 11, No 1, pp. 40.

[4] Li, Y.; Chen, X.; Lin, Y.; Srivastava, G.; Liu, S. Wireless transmitter identification based on device imperfections. IEEE Access 2020, Volume 8, pp. 59305-59314.

[5] Qoria, T.; Rokrok, E.; Bruyere, A.; François, B.; Guillaud, X. A PLL-free grid-forming control with decoupled functionalities for high-power transmission system applications. IEEE Access 2020, Volume 8, pp.197363-197378.

[6] Ji, B.; Li, Y.; Cao, D.; Li, C.; Mumtaz, S.; Wang, D. Secrecy performance analysis of UAV assisted relay transmission for cognitive network with energy harvesting. IEEE Transactions on Vehicular Technology 2020, Volume 69, No. 7, pp. 7404-7415.

[7] Wei, Z.; Masouros, C.; Liu, F.; Chatzinotas, S.; Ottersten, B. Energy-and cost-efficient physical layer security in the era of IoT: The role of interference. IEEE Communications Magazine 2020, Volume 58, No. 4, pp. 81-87.

[8] Gomez-Barquero, D.; Lee, J.Y.; Ahn, S.; Akamine, C.; He, D.; Montalaban, J.; Wang, J.; Li, W.; Wu, Y. IEEE transactions on broadcasting special issue on: Convergence of broadcast and broadband in the 5G era. IEEE Transactions on Broadcasting 2020, Volume 66, No. 2, pp. 383-389.

[9] Guo, K.; An, K.; Zhang, B.; Huang, Y.; Tang, X.; Zheng, G.; Tsiftsis, T.A. Physical layer security for multiuser satellite communication systems with threshold-based scheduling scheme. IEEE Transactions on Vehicular Technology 2020, Volume 69, No. 5, pp. 5129-5141.

[10] Khoshafa, M.H.; Ngatched, T.M.; Ahmed, M.H. On the physical layer security of underlay relay-aided device-to-device communications. IEEE

Transactions on Vehicular Technology 2020, Volume 69, No. 7, pp.7609-7621.

[11] Singh, R.; Rawat, M.; Jaiswal, A. On the physical layer security of mixed FSO-RF SWIPT system with non-ideal power amplifier. IEEE Photonics Journal 2021, Volume 13, No. 4, pp. 1-17.

[12] Chen, Y.; Zhang, T.; Liu, Y.; Qiao, X. Physical layer security in NOMA-enabled cognitive radio networks with outdated channel state information. IEEE Access 2020, Volume 8, pp. 159480-159492.

[13] Li, B.; Zou, Y.; Zhu, J.; Cao, W. Impact of hardware impairment and co-channel interference on security-reliability trade-off for wireless sensor networks. IEEE Transactions on Wireless Communications 2021, Volume 20, No. 11, pp.7011-7025.

[14] Tashman, D.H.; Hamouda, W. Physical-layer security on maximal ratio combining for SIMO cognitive radio networks over cascaded κ-μ fading channels. IEEE Transactions on Cognitive Communications and Networking 2021, Volume 7, No. 4, pp. 1244-1252.

[15] Choi, J.; Joung, J.; Jung, B.C. Space–time line code for enhancing physical layer security of multiuser MIMO uplink transmission. IEEE Systems Journal 2020, Volume 15, No. 3, pp. 3336-3347.

[16] Wang, H.; Xu, L.; Lin, W.; Xiao, P.; Wen, R. Physical layer security performance of wireless mobile sensor networks in smart city. IEEE Access 2019, Volume 7, pp. 15436-15443.

[17] Chen, Gecheng, Rui Tuo. Projection pursuit Gaussian process regression. IISE Transactions 2023, Volume 55, No. 9, pp. 901-911.

[18] Mutny, Mojmir, Johannes Kirschner, Andreas Krause. Experimental design for optimization of orthogonal projection pursuit models. In Proceedings of the AAAI Conference on Artificial Intelligence 2020, Volume 34, No. 06, pp. 10235-10242.

[19] Bashar, Abul, Smys. S. Physical layer protection against sensor eavesdropper channels in wireless sensor networks. IRO Journal on Sustainable Wireless Systems 2021, Volume 3, No. 2, pp. 59-67.

[20] Gao, Ning, Qiang Ni, Daquan Feng, Xiaojun Jing, Yue Cao. Physical layer authentication under intelligent spoofing in wireless sensor networks. Signal Processing 2020, Volume 166, pp. 107272.

[21] Saju, Chinju, Prawin Angel Michael, Jarin. T. Modeling and control of a hybrid electric vehicle to optimize system performance for fuel efficiency. Sustainable Energy Technologies and Assessments 2022, Volume 52, pp. 102087.

[22] Vijay, M. M.; Punithavathani, S. D. Implementation of memory-efficient linear pipelined IPv6 lookup and its significance in smart cities. & quot; Computers & amp; Electrical Engineering 2018, Volume 67, pp.1-14.

[23] Ramana, T. V.; Pandian, A.; Ellammal, C.; Jarin, T.; Ahmed Nabih Zaki Rashed; Sampathkumar. A. Numerical analysis of circularly polarized modes in coreless photonic crystal fiber. Results Phys 2019, Volume 13, No. 102140, pp. 10-1016.