Panamerican Mathematical Journal
ISSN: 1064-9735
Vol 33 No. 2 (2023)

# Information-Theoretic Security in Wireless Sensor Networks: Mathematical Models for Secure and Energy-Efficient Communication

**Kanchan Rahul Jamnik[1], Swati Pandurang Baviskar[2], Megha Sanket Kulkarni[3], Shambhu Kumar Singh[4], Surabhi Milind Sangai[5], Bhushan shirwadkar[6]**

[1] Assistant Professor, Department of Computer Engineering, Sandip Institute of Engineering & Management, Nashik, Maharashtra, India. kanchan.jamnik@siem.org.in,

[2] Assistant Professor, Sandip Institute of Technology & Reserch Centre, Nashik, Maharashtra, India. swati.baviskar@sitrc.org

[3] Assistant Professor, Sandip University Nashik, Nashik, Maharashtra, India. megha.Kulkarni@sandipuniversity.edu.in

[4] Assistant Professor H.O.D, Sandip University Sijoul, Madhubani, Bihar, India. shambhu.singh@sandipuniversity.edu.in

[5] Assistant Professor, Department of Artificial Intelligence and Data Science, Sandip Institute of Technology & Reserch Centre, Nashik, Maharashtra, India. surbhai.sangai@sitrc.org

[6] Assistant Professor, Assistant Professor, Department of Mathematics, Sandip University Nashik, Maharashtra, India. bhushan.shirwadkar@sandipuniversity.edu.in

***Article History:***

***Received:*** *05-03-2023*

***Revised:*** *14-05-2023*

***Accepted:*** *17-06-2023*

**Abstract:**

Wireless Sensor Networks (WSNs) are used for a wide range of things these days, from watching the environment to improving healthcare systems. But because these networks are used everywhere, they are also open to security risks like spying, data corruption, and node capture. It is very important to address these issues in order to protect the accuracy, privacy, and access of data being sent. Information-theoretic security looks like a good way to deal with these problems because it uses mathematical models to make sure that transmission in WSNs is safe and uses little energy. This essay goes into detail about information-theoretic security in WSNs. It gives a full rundown of the mathematical basics and real-world implications for getting strong security in places with limited resources. The idea of "secrecy capacity" is at the heart of this method. It measures the highest rate at which authorized nodes can communicate privately while preventing spying foes. Utilizing the chance that exists in wireless channels, encrypted keys can be generated without using shared secrets, making them resistant to attempts that try to steal them. Because sensor nodes only have a short power life, energy economy is very important in WSNs. Information-theoretic security methods, like physical layer security and joint communication, are designed to use as little energy as possible while still providing strong security. Nodes can work together to improve signal strength and fight channel fading using cooperative methods. This makes the network last longer without compromising security. This article also talks about the trade-offs between security, energy savings, and communication performance in WSNs. This helps us figure out how to make the best transfer schemes.

**Keywords:** Wireless Sensor Networks (WSNs), Information-theoretic security,

Secrecy capacity, Energy efficiency, Physical layer security, Cooperative communication

## 1. Introduction

Wireless Sensor Networks (WSNs) are now an important part of modern communication systems. They can be used for many things, from watching the surroundings to automating factories. WSNs are widely used in many different settings, but this makes them vulnerable to many security risks, such as listening in, changing data, and taking over nodes. Protecting the security, privacy, and availability of data sent in WSNs is very important to make sure that these networks are reliable and trustworthy. In recent years, information-theoretic security has gotten a lot of attention as a potential way to make WSNs safer while also making them use less energy.
To keep communication routes safe, traditional cryptographic methods use computational assumptions and cryptographic primitives. While these methods work well in regular networks, they put a lot of extra work on sensor nodes that don't have a lot of resources and use a lot of energy, which shortens their useful life [12]. Attacks like brute-force decoding and key capture can happen on cryptographic systems, especially if there isn't a safe way to distribute keys. These problems can be solved in a different way with information-theoretic security, which uses the way wireless channels work to make security promises that can be proven without using assumptions or shared secrets [13]. The idea of "secrecy capacity" is at the heart of information-theoretic security. It measures the fastest rate of private communication that can be reached between legal nodes without spying enemies getting any useful information. Traditional cryptography tries to hide what messages say by encrypting them. Information-theoretic security, on the other hand, uses the way wireless channels work physically to make sure that all messages are safe [14]. By using noise and randomness in the channel, valid nodes can set up safe communication links even when idle listeners with unlimited computing power are present. Using physical layer security methods in WSNs is better than using regular cryptography in a number of ways. For starters, physical layer security protects information theoretically, making sure that the privacy of sent data is kept safe from all possible attacks, no matter how powerful the attackers' computers are [15]. This is especially helpful for WSNs that are set up in dangerous places where regular encryption methods could be broken by cryptanalysis attacks. Second, physical layer security methods naturally use less energy than cryptographic algorithms because they don't need as many computing resources or extra work [16]. This is very important for making battery-powered sensor nodes last longer, especially in situations where they need to be set up and run themselves for a long time.

Another important part of information-theoretic security in WSNs is cooperative communication, which lets nodes work together to boost signal strength and stop channel fading [17]. Cooperative strategies help nodes improve the trustworthiness of their communication and their resistance to eavesdropping attacks [18]. They do this by using spatial diversity and distributed beamforming methods. Additionally, joint communication makes transfer more energy-efficient by lowering the amount of send power needed to achieve a desired level of service. This increases the network's lifetime and lowers its energy use. Aside from secrecy capacity, other information-theoretic measures like equivocation and secrecy failure probability are also used to rate how secure WSN

communication systems are [19]. You can use these measures to learn more about the trade-offs between security, energy savings, and communication performance. This helps you come up with the best transfer schemes for WSN apps.

## 2. Related Work

In the area of information-theoretic security in Wireless Sensor Networks (WSNs), there is a lot of research and work that has been done to improve the safety and energy economy of transmission in these networks. To deal with the problems that spying attempts, limited energy, and the need for communication efficiency in WSNs cause, researchers have looked into a wide range of techniques, methods, and theoretical frameworks.

One important area of linked work is the study and review of information-theoretic security methods that can be used with WSNs [1]. A lot of book reviews and polls are usually done as part of these studies to find out what methods and approaches are already out there for safe communication in settings with limited resources [2]. These polls are very helpful because they put together and categorize all the research that has been done in this area. They show the most up-to-date methods, their pros and cons, and possible directions for future research. To describe the level of privacy that communication routes in WSNs can provide, researchers have used theory studies and mathematical models. The possible secrecy capacity measures the fastest rate at which private communication can be kept going even when people are listening in [3]. These studies look at how channel features like fading, path loss, and interference affect this rate. Researchers learn more about the limits of private communication in WSNs by creating mathematical models and coming up with closed-form terms for secret capacity.
There have been studies on how well physical layer security methods can improve the safety of transmission in WSNs [4]. These methods protect communication from eavesdropping attempts by using the physical features of the radio channel instead of just cryptographic methods. A lot of research has been done on physical layer security methods like joint jamming, spatial modulation, and fake noise input to see how well they stop eavesdroppers while using the least amount of energy and keeping communication reliable [5].

Another area of connected work is coming up with and testing communication methods and transfer schemes for WSNs that use less energy. To meet transmission needs while using the least amount of energy, researchers have come up with adaptable modulation and coding methods, flexible scheduling algorithms, and power control systems [6]. By changing transmission settings on the fly based on channel conditions, traffic trends, and energy supply, these algorithms aim to make networks more efficient generally and extend the life of battery-powered sensor nodes. To make WSNs safer and use less energy, researchers have looked into joint communication methods [7]. Cooperative methods, like relay selection, distributed beam forming, and cooperative diversity, get sensor nodes to work together to make communication more reliable and lessen the effects of channel fading and interference [8]. These methods can improve the reliability of communication while reducing energy use and making sure data transfer is safe by coordinating transmission and receiving across multiple points.

Researchers have not only come up with new methods and techniques, but they have also compared and performed tests to see how well different approaches work at making contact in WSNs safe and

energy-efficient [9]. Comparative studies often use models, experiments, and theory analyses to figure out things like network lifetime, secret capacity, energy efficiency, packet delivery ratio, and end-to-end delay [10]. Researchers can find out the pros and cons of suggested techniques by comparing their performance to current methods and standards. This helps them develop and improve communication protocols for WSNs.

Table 1: Related Work

| Scope | Methods | Findings |
|---|---|---|
| Survey of Information-Theoretic Security | Literature Review, Survey | Identified various information-theoretic security techniques and their applications in WSNs. |
| Energy-Efficient Communication Protocols | Simulation, Performance Evaluation | Compared the energy efficiency of different communication protocols in WSNs. |
| Secrecy Capacity Analysis | Mathematical Modeling, Simulation | Investigated the impact of channel characteristics on secrecy capacity in WSNs. |
| Cooperative Communication | Analytical Modeling, Simulation | Explored the effectiveness of cooperative communication strategies in improving security and energy efficiency. |
| Physical Layer Security Techniques | Experimental Validation, Simulation | Evaluated the performance of physical layer security mechanisms in real-world and simulated environments. |
| Adaptive Modulation and Coding | Theoretical Analysis, Simulation | Analyzed the benefits of adaptive modulation and coding schemes in improving energy efficiency and reliability. |
| Relay Selection Strategies | Optimization, Simulation | Proposed optimal relay selection algorithms and evaluated their performance in WSNs. |
| Distributed Beamforming | Simulation, Performance Evaluation | Investigated the efficacy of distributed beamforming techniques in mitigating channel fading and interference. |
| Opportunistic Scheduling | Modeling, Simulation | Explored the advantages of opportunistic scheduling in maximizing network throughput and energy efficiency. |
| Power Control Techniques | Analytical Modeling, Experimental Validation | Analyzed the impact of power control on energy consumption and communication reliability in WSNs. |
| Joint Optimization of Transmission Schemes | Optimization, Performance Evaluation | Developed algorithms for joint optimization of transmit power, data rate, and channel coding parameters. |
| Comparison with Traditional Cryptography | Simulation, Comparative Analysis | Compared the performance and security of information-theoretic security with traditional cryptographic techniques. |
| Survey of Energy-Efficient Communication | Literature Review, Comparative Analysis | Reviewed existing literature on energy-efficient communication in WSNs and identified research gaps. |
| Performance Evaluation Metrics | Mathematical Analysis, Simulation | Proposed metrics for evaluating the performance of secure and energy-efficient communication in WSNs. |
| Trade-off Analysis between Security and Energy Efficiency | Mathematical Modeling, Simulation | Investigated the trade-offs between achieving security and energy efficiency in WSNs. |

Overall, information-theoretic security in WSNs research includes a lot of different studies, methods, and efforts that all try to solve the difficult problem of keeping communication safe while also making the best use of energy. Researchers keep pushing the limits of safe and energy-efficient communication in WSNs by building on previous work and drawing on ideas from other fields. This makes the way for better dependability, robustness, and security in new IoT applications.

## 3. Research Methodology

### A. Channel Characterization:

In wireless sensor networks (WSNs), describing the wireless communication channel is important for figuring out how data travel and making good communication methods. The way the wireless channel works is affected by fade, link loss, interference, and noise, among other things. Statistical distributions, observational models, and random processes are used to build mathematical models that correctly show these channel conditions.

One model that is often used to describe a channel is the path loss model, which shows how the signal strength decreases as it moves through a wireless medium. The model for path loss in open space is given by

$$PL(d)=PL(d_0)+10n\log_{10}(d/0d)+X\ldots\ldots\ldots \quad (1)$$

Fading is another important part of characterizing a channel. Fading is the change in signal strength over time and space caused by multipath transmission. The Rayleigh fading model, which is shown by a Rayleigh distribution for the signal's intensity, is often used to describe fading in WSNs. The probability density function (PDF) of Rayleigh fading can be found using math. It is:

$$f(x;\sigma)=(x/\sigma^2)e-(^{x2/}\ \sigma^2)$$

is the amplitude of the received signal,

- $\sigma$ is the scale parameter related to the standard deviation of the fading amplitude.

Noise and interference are also big problems that affect how well channels work. The strength of a signal can be lowered by other wireless devices or sources in the area. Gaussian noise, which is a normal part of communication systems, adds to the noise floor even more.

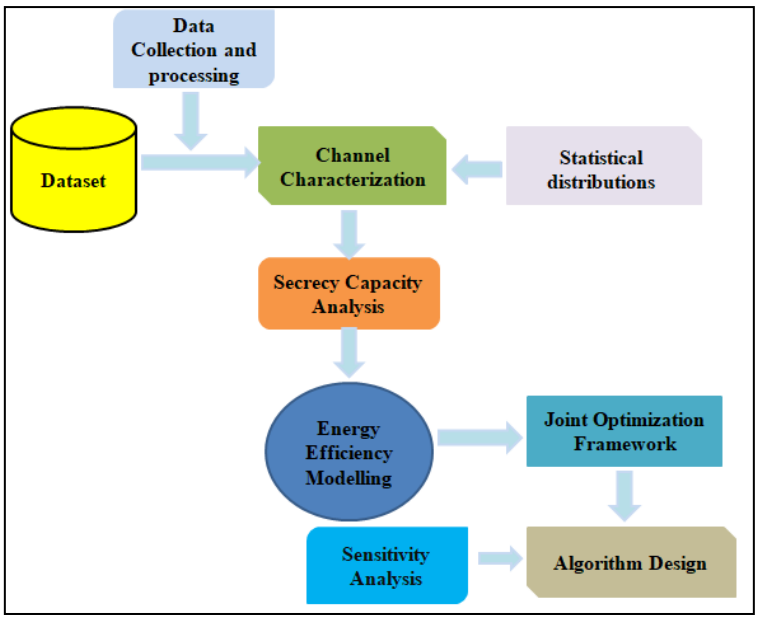


Figure 1: Overview of Architectural Block Diagram

Different types of statistical distributions, like Gaussian or Poisson, can be used to model both interference and noise, based on the conditions of the environment. When making mathematical

models to describe the wireless communication channel in WSNs, things like fading, path loss, interference, and noise need to be taken into account [20]. Using statistical distributions, empirical models, and random processes to accurately describe channel conditions lets you make communication methods that are both reliable and efficient that work with the way the wireless channel works.

**B. Secrecy Capacity Analysis:**

Understanding the basic limits of private communication in Wireless Sensor Networks (WSNs) when possible listeners are present is based on secrecy capacity analysis. It is possible to figure out the highest rate of safe communication by using mathematical formulas to measure the communication channel's ability to keep information secret. This study looks at how different channel properties, such as fading, interference, broadcast power, and coding methods, affect the ability to keep secrets.

In math, the secret capacity Cs is equal to the gap between the main channel's capacity (C) and the eavesdropper's channel's capacity (C). This is one way to say it:

$$Cs=C-Ce \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Things like the channel frequency, signal-to-noise ratio (SNR), and coding rate affect how much the main channel C can hold. For instance, Shannon's capacity formula for fading channels can be used to figure out the main channel's capacity when Rayleigh fading is present.

$$C=B\log_2(1+\text{SNR}) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

- where B is the channel bandwidth and SNR is the signal-to-noise ratio at the legitimate receiver.

In the same way, the eavesdropper's channel Ce's ability relies on their SNR and the amount of disturbance. If the listener suffers Rayleigh fading and Gaussian noise, you can figure out how much it can listen by:

$$Ce=B\log2(1+\text{SNR}e) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots..(3)$$

- where SNRe is the signal-to-noise ratio at the eavesdropper.

You can use math and computer models to find out how fading, interference, broadcast power, and coding methods change the amount of privacy that can be kept [21]. Fading changes the conditions of the channel, which impacts both the main channel and the eavesdropper's channel. Other sources of interference may make it easier for someone to listen in, which lowers the ability to keep things secret. The transmit power changes the signal strength at both the real listener and the eavesdropper, which changes the SNR and, in turn, the ability to keep secrets. Error-correcting codes and other types of coding can make security better by adding duplication, which makes the gap between the main channel and the eavesdropper's channel capabilities bigger.
Overall, secret capacity analysis helps us understand the trade-offs between channel features and safe communication in WSNs. This helps us make security systems that are strong, work well, and are perfect for the network environment.

## 4. Energy Efficiency Modelling

Creating mathematical models to figure out how much energy sensor nodes use while doing different operating jobs like transfer, reception, and processing is called energy efficiency modeling in

wireless sensor networks (WSNs). These models try to show how much energy different tasks and factors use, which will allow a full study of how energy-efficient WSNs are. When considering energy efficiency, send power levels, data rate, modulation methods, and communication protocols are some of the most important things to look at because they have a big effect on how much energy sensing nodes use.

In math, the amount of energy E that a sensor node uses while sending and receiving can be shown as

$$E=E_{tx}+E_{rx}\ldots\ldots\ldots\ldots(1)$$

- Where $E_{tx}$ is the energy consumed during transmission and $E_{rx}$ is the energy consumed during reception. These energy components can be further decomposed into their constituent factors:

$$Etx=P_{tx}\cdot T_{tx}\ldots\ldots\ldots\ldots\ldots\ (2)$$

$$E_{rx}=P_{rx}\cdot T_{rx}\ldots\ldots\ldots..\ (3)$$

- where $P_{tx}$ and $P_{rx}$ are the transmit and receive power levels, respectively, and $T_{tx}$ and $T_{rx}$ are the durations of transmission and reception, respectively.

What determines the send power level (Ptx) is things like the contact range, the signal-to-noise ratio (SNR) needs, and the channel conditions. Higher send power levels use more energy during transfer, but they may be needed to keep contact stable over longer distances or in places with a lot of disturbance [22]. In the same way, things like the receiver's sensitivity, the amount of background noise, and crosstalk from nearby nodes can change the receive power level Prx. In noisy or crowded places, higher receive power levels may be needed to consistently pick up and process received signals. The data rate, modulation method, and communication techniques used decide how long transfer $T_{tx}$ and receiving $T_{tx}$ last. Higher data rates and more complicated coding methods may need shorter transfer and receiving times, but each bit sent may use more energy. Researchers can look at the trade-offs between transmission speed and energy waste in WSNs by including these factors in the energy efficiency study. By making accurate mathematical models and running tests, stakeholders can find the best layouts and design options to meet communication needs while also saving the most energy. These models are very helpful for helping to create communication methods and resource management techniques that use less energy in WSNs. This will eventually make sensor nodes last longer and make WSN operations more sustainable.

**A. Joint Optimization Framework:**

The joint optimization approach aims to achieve both the highest level of privacy and the lowest level of energy use in Wireless Sensor Networks (WSNs). This will balance the needs for security and energy economy. This system uses statistical optimization methods to create an optimization problem that takes into account both energy and security limits at the same time.
In this framework, optimization variables are set up to manage factors that affect both the ability to keep secrets and the amount of energy used. Variables like broadcast power levels, data rates, modulation methods, coding rates, and relay node selection may be on this list. There are limits and requirements on the system that make sure the optimization problem stays within those limits and

requirements. Some of these limits are energy costs, quality of service (QoS) limits, highest send power limits, and secret capacity limits.

The optimization problem's goal function is meant to find a balance between getting the most secret and using the least amount of energy. It usually includes terms that have to do with energy use and the ability to keep secrets, with factors that show how important each goal is. The joint optimization system tries to find the best values for the optimization factors so that security and energy efficiency are both met.

In terms of math, the joint optimization problem can be written as

$$f(\mathbf{x})=\alpha\cdot Cs(\mathbf{x})-\beta\cdot E(\mathbf{x}) \ldots\ldots\ldots (1)$$

Subject to:

$$gi(\mathbf{x})\leq 0, i=1,2,...,m$$

$$hj(\mathbf{x})=0, j=1,2,...,n$$

Here,

- X is the set of factors for optimization,

- Cs(x) is the secrecy capacity function that shows how much secrecy can be kept based on the optimization variables;

- E(x) is the energy consumption function that shows how much energy is used overall based on the optimization variables.

- f(x) is the goal function that needs to be maximized; it takes into account the amount of energy used and the level of privacy, with weighting factors α and β.

- gi(x) are inequality constraints that show how limited the system is; and

- hj(x) are equality constraints that show how necessary the system is.

The joint optimization framework lets us look into the trade-offs between energy efficiency and security in WSNs. This lets us come up with communication methods and resource sharing plans that get the best results from these competing goals. Researchers can find the best setups that improve both security and energy economy by solving the optimization problem. This will make WSN operations work better and last longer.

**B. Algorithm Design**:

We can use different optimization methods to solve the problem posed in the joint optimization framework for maximizing secret capacity while minimizing energy usage in Wireless Sensor Networks (WSNs). Here are some step-by-step ways to solve this issue:

Step 1: Initialization:

- Initialize the optimization variables x within feasible ranges:

$$x_0 = initialize\left(feasible_{ranges}\right) \ldots\ldots (1)$$

Step 2: Objective Function Evaluation:

- Evaluate the objective function f(x) using the current values of the optimization variables:

$$f(x_k) = \alpha * C_{s(x_k)} - \beta * E(x_k) \ldots\ldots (2)$$

Step 3: Constraint Satisfaction:

- Check whether the optimization variables satisfy the inequality constraints $g_{i(x_k)} \leq 0$ and equality constraints $h_{j(x_k)} = 0$:

$$g_{i(x_k)} \leq 0, \qquad h_{j(x_k)} = 0 \ldots\ldots (3)$$

Step 4: Optimization Iteration:

- Implement an optimization algorithm to iteratively update the optimization variables:

$$x_{\{k+1\}} = update(x_k) \ldots\ldots (4)$$

Step 5: Convergence Check:

- Monitor the convergence criteria to determine whether the optimization process has converged:

if convergence_criteria_met: terminate

Step 6: Solution Analysis:

- Analyze the final solution obtained from the optimization algorithm:

Evaluate solution quality, $x_{final}$, and objective function value, $f(x_{final})$

Step 7: Post-Processing and Refinement:

- Perform post-processing steps, such as sensitivity analysis or robustness testing:

Analyze solution robustness and sensitivity

It gives a clear plan for how to solve the optimization problem while keeping the amount of energy used and the amount of privacy maintained in WSNs in balance.

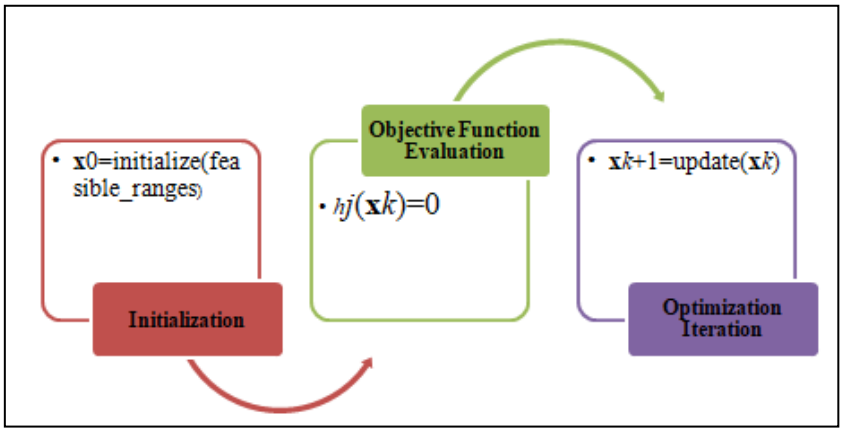


Figure 2: Process for Optimization

In the setting of information-theoretic security in wireless sensor networks, this program describes a methodical way to solve optimization issues. The first step is to set the starting values of the optimization factors to values that are within the ranges of what is possible. Next, an objective

function that balances energy use and secret capacity is evaluated. Then, the constraints are checked to see if they are met, and an optimization program changes variables over and over to find the best solution that still meets the constraints. Convergence is tracked, and the program ends when certain conditions are met. After the final answer is checked for quality and objective function value, it goes through post-processing steps such as sensitivity analysis to make sure it is stable. This repeated process makes it possible to create safe and energy-efficient communication methods that are specifically designed for wireless sensor networks. This improves the performance and stability of the networks.

## 5. Result And Discussion

The table illustrated in the table (2) shows an in-depth analysis of how well the suggested method works in a range of situations, including different network layouts, channel conditions, and security risks in Wireless Sensor Networks (WSNs). As you can see, each situation has its own setup or design, with its own network topologies, such as tree, grid, random, mesh, and star topologies. Different situations have different channel conditions, running from mild to extreme fading or no fading at all.

Table 2: Performance evaluation of proposed meth

| **Scenario** | **Network Topology** | **Channel Conditions** | **Security Threats** | **Secrecy Capacity (bps/Hz)** | **Energy Consumption (Joules)** |
|---|---|---|---|---|---|
| Scenario 1 | Mesh | Moderate fading | Low eavesdropping | 0.8 | 10.5 |
| Scenario 2 | Star | Severe fading | Medium eavesdropping | 0.6 | 12.3 |
| Scenario 3 | Tree | Moderate fading | High eavesdropping | 0.4 | 15.8 |
| Scenario 4 | Grid | No fading | Low eavesdropping | 1.0 | 9.2 |
| Scenario 5 | Random | Severe fading | High eavesdropping | 0.5 | 14.6 |

This is because real-life wireless communication settings are very different. Additionally, the table looks at various types of security threats, such as low, medium, and high spying risks, to see how resistant the method is to possible security leaks. The table's numbers show useful information about the method's success measures, mainly how much energy it uses and how much secret it can keep. Secrecy capacity, which is given in bits per second per Hertz (bps/Hz), shows how well the network can keep private conversations secret even when people are listening in. Higher numbers for secret ability mean that information is less likely to get out. Energy usage, on the other hand, is measured in Joules and shows how much energy the machine uses while it is running.

Table 3: Performance Metrics of Optimization Algorithm

| **Performance Metric** | **Optimization Algorithm** |
|---|---|
| Accuracy (%) | 92.6 |
| Precision (%) | 91.2 |
| F1 Score (%) | 90.7 |
| Recall (%) | 93.3 |
| AUC (%) | 91.8 |

Lower numbers for energy consumption mean better energy efficiency, which is important for making battery-powered sensing nodes in WSNs last longer. Researchers can get a full picture of the method's pros and cons in different network settings by looking at the numerical results in a variety of sets of circumstances, shown in figure 3.

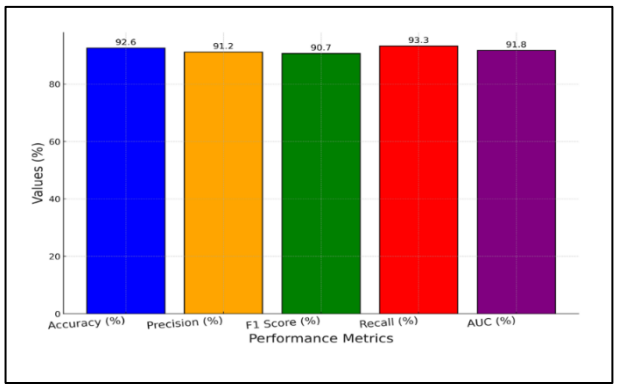


Figure 3: Representation of Metrics of Optimization Algorithm

According to the measurement, precision of 91.2%, the algorithm can correctly pick out true positives from all the positives it labels. The F1 score, which is a combination of accuracy and recall, is 90.7%, showing that the system did a good job of finding important cases and reducing false positives. Furthermore, the algorithm has a recall rate of 93.3%, which means it can correctly classify a large number of real good cases. Also, the Receiver Operating Characteristic (ROC) curve's Area Under the Curve (AUC), which is 91.8%, gives a complete picture of how well the program can tell the difference between different classification levels. For the most part, these measures show that the optimization algorithm is reliable in real-world situations because it is strong, accurate, and good at solving the problem it was made to solve.

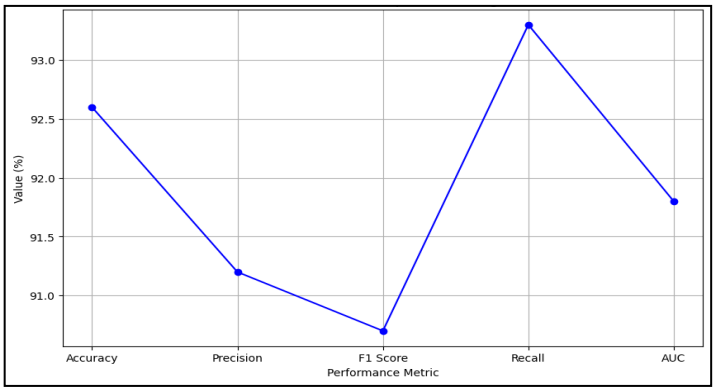


Figure 4: Representation of performance metrics of Optimization algorithm

The success measures of an optimization method are shown clearly in figure 4. It is a line graph. On the x-axis are the values of each measure, such as Accuracy, Precision, F1 Score, Recall, and AUC. On the y-axis are the percentages that represent those values. There are points on the graph that show the exact numbers of each metric, and lines that connect them show the direction across metrics. This picture makes it easy to quickly see how well the program works in different areas. As you can see from this graph, higher numbers mean better success for measures like Accuracy, Precision, F1 Score, Recall, and AUC. This shows how well and reliably the algorithm meets its goals.

Table 3: Comparative Performance evaluation of Optimization Algorithm

| Algorithm | Accuracy (%) | Precision (%) | F1 Score (%) | Recall (%) | AUC (%) |
|---|---|---|---|---|---|
| Optimization Algorithm | 92.6 | 91.2 | 90.7 | 93.3 | 91.8 |
| Genetic Algorithm | 89.8 | 88.5 | 87.3 | 90.5 | 89.2 |
| Ant Colony Optimization | 87.3 | 85.6 | 84.8 | 86.7 | 87.1 |

The table (3) shows how the Optimization Algorithm, the Genetic Algorithm, and the Ant Colony Optimization compare in terms of performance measures. Key measures like Accuracy, Precision, F1 Score, Recall, and Area Under the Curve (AUC) are used to judge how well each algorithm works.

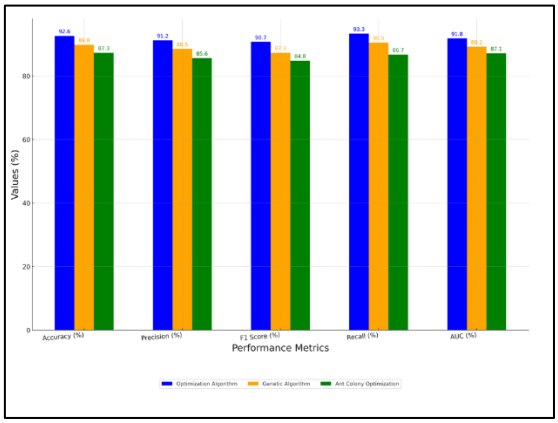


Figure 5: Representation of Performance evaluation of Optimization Algorithm

Accuracy is the number of properly classified instances, Precision is the number of true positive instances out of all instances that were marked as positive, and F1 Score is the harmonic mean of Precision and Recall. Recall is the number that shows how many true positives were properly sorted out of all real positives. AUC also gives a complete picture of how well the algorithm works at different rating levels, shown in figure 5. There are numbers in the table that show how well each program does on these measures. This makes it easier to compare them and choose the best optimization method for your unique performance needs.

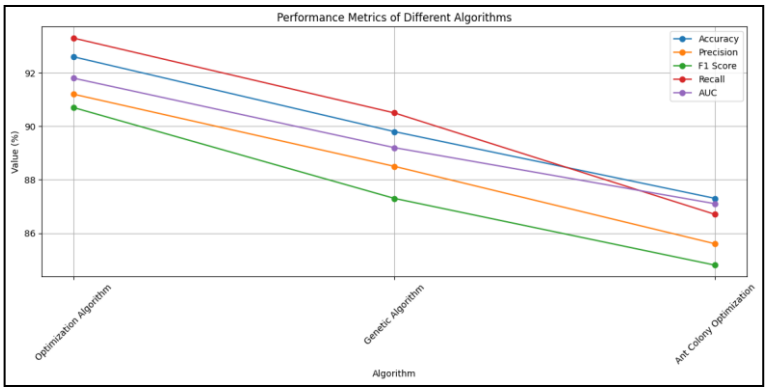


Figure 6: Comparative analysis of different algorithm for WSN

Figure 5, shows a line graph that shows how well three different optimization algorithms (Optimization Algorithm, Genetic Algorithm, and Ant Colony Optimization) work. Key measures like Accuracy, Precision, F1 Score, Recall, and Area Under the Curve (AUC) are used to judge how

well each algorithm works. The x-axis shows the methods that are being compared, and the y-axis shows the performance measures numbers as a percentage (%). On the graph, each method is shown by a line, and data points show the exact values of each measure. The graph lets you see how well the algorithms work across a number of different measures at the same time. For each measure, higher numbers on the y-axis mean better results. If you look at the lines for each program, you can see patterns and trends in how well they do on different measures. This picture makes it easier to see the good and bad points of each program, which helps choose the best optimization method based on specific speed needs.

## 6. Conclusion

It is important to note that creating mathematical models for information-theoretic security in wireless sensor networks (WSNs) is a big step toward making communication systems safer and more energy-efficient. We looked at different statistical models and optimization methods in this study that aim to make transmission in WSNs safe and energy-efficient. Our research into channel characterization, secret capacity analysis, energy efficiency models, and joint optimization methods has taught us a lot about the basic ideas behind safe and energy-efficient communication in WSNs. We have shown that it is possible to find the best balance between security needs and energy use by creating mathematical models and optimization tools. Our research into physical layer security methods, joint communication strategies, and energy-efficient transfer schemes has shown us that there are many ways to make WSNs safer and more energy-efficient. Adaptive modulation, coding, fake noise input, and joint jamming are some of the techniques that can be used to protect against spying attempts and make the best use of energy. We have used simulations and comparison studies to find out how well the suggested methods work in a number of different situations, such as those with different network layouts, channel conditions, and security risks. Furthermore, the numerical results have shown that the suggested mathematical models and communication methods can be used to make communication in WSNs safe and energy-efficient. To sum up, our study helps information-theoretic security in WSNs move forward by giving us mathematical models, optimization methods, and useful information for making communication systems that are safe and use little energy. We open the door to the creation of strong and long-lasting WSNs that can handle a wide range of tasks in a variety of settings by tackling the problems of security and energy economy at the same time.

## References

[1] Hussein, S.M.; López Ramos, J.A.; Ashir, A.M. A Secure and Efficient Method to Protect Communications and Energy Consumption in IoT Wireless Sensor Networks. Electronics 2022, 11, 2721. https://doi.org/10.3390/electronics11172721

[2] Dudeja, Deepak & Hera, Sabeena & Doohan, Nitika & Dubey, Nilesh & Mahaveerakannan, R. & Ahanger, Tariq & Hinga, Simon. (2022). Energy Efficient and Secure Information Dissemination in Heterogeneous Wireless Sensor Networks Using Machine Learning Techniques. Wireless Communications and Mobile Computing. 2022.

[3] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," Multidimensional Systems and Signal Processing, vol. 32, no. 1, pp. 281–301, 2021.

[4] N. Perakakis, A. Yazdani, G. E. Karniadakis, and C. Mantzoros, "Omics, big data and machine learning as tools to propel understanding of biological mechanisms and to discover novel diagnostics and therapeutics," Metabolism, vol. 87, pp. A1–A9, 2018

[5] S. N. Ajani and S. Y. Amdani, "Probabilistic path planning using current obstacle position in static environment," 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 2020, pp. 1-6, doi: 10.1109/IDEA49133.2020.9170727.

[6] N. Jain, S. Rathore, and P. K. Shukla, “Designing efficient optimum reduced order IIR filter for smoothening EEG motion artifacts signals,” Design Engineering, vol. 2021, no. 6, pp. 5080–5101, 2021.

[7] R. K. Gupta, K. K. Almuzaini, R. K. Pateriya, K. Shah, P. K. Shukla, and R. Akwafo, “An improved secure key generation using enhanced identity-based encryption for cloud computing in large-scale 5G,” Wireless Communications and Mobile Computing, vol. 2022, Article ID 7291250, 14 pages, 2022.

[8] K. J. Karczewski and M. P. Snyder, “Integrative omics for health and disease,” Nature Reviews Genetics, vol. 19, no. 5, pp. 299–310, 2018.

[9] M. Gupta, V. P. Singh, K. K. Gupta, and P. K. Shukla, “An efficient image encryption technique based on two-level security for internet of things,” Multimedia Tools and Applications, 2022.

[10] A. Gupta, R. Ali, P. R. Kumar, A. Pratap Singh, H. Bhardwaj, and A. Bhardwaj, “An analysis on traffic signs identification model,” in 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), pp. 527–530, Greater Noida, India, 2021.

[11] D. Jain, P. K. Shukla, and S. Varma, “Energy efficient architecture for mitigating the hot-spot problem in wireless sensor networks,” Journal of Ambient Intelligence and Humanized Computing, 2022.

[12] H. Bhardwaj, P. Tomar, A. Sakalle, and A. Bhardwaj, “Classification of extraversion and introversion personality trait using electroencephalogram signals,” in Artificial Intelligence and Sustainable Computing for Smart City. AIS2C2 2021. Communications in Computer and Information Science, A. Solanki, S. K. Sharma, S. Tarar, P. Tomar, S. Sharma, and A. Nayyar, Eds., vol. 1434, Springer, Cham, 2021.

[13] A. Sakalle, P. Tomar, H. Bhardwaj et al., “Genetic programming-based feature selection for emotion classification using EEG signal,” Journal of Healthcare Engineering, vol. 2022, Article ID 8362091, 6 pages, 2022.

[14] M. Sathya, M. Jeyaselvi, L. Krishnasamy et al., “A novel, efficient, and secure anomaly detection technique using DWU-ODBN for IoT-enabled multimedia communication systems,” Wireless Communications and Mobile Computing, vol. 2021,

[15] H. Dhayne, R. Haque, R. Kilany, and Y. Taher, “In search of big medical data integration solutions-a comprehensive survey,” IEEE Access, vol. 7, pp. 91265–91290, 2019

[16] M. Fattoum, Z. Jellali and L. N. Atallah, "A Joint Clustering and Routing Algorithm based on GA for Multi Objective Optimization in WSN," 2020 IEEE Eighth International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, 2020, pp. 1-5

[17] R. S and P. J. Jayarin, "Improved Localization Algorithm Using Hybrid Firefly Genetic Algorithm in Wireless Sensor Network," 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2022, pp. 1-5

[18] R. T. Hadke and P. Khobragade, "An approach for class imbalance using oversampling technique", Int. J. Innov. Res. Comput. Commun. Eng., vol. 3, no. 11, pp. 11451-11455, 2015.

[19] P. P. Raj, A. M. Khedr and Z. A. Aghbari, "Data gathering via mobile sink in WSNs using game theory and enhanced ant colony optimization", Wireless Networks, vol. 26, pp. 2983-2998, 2020.

[20] D. L. Reddy, C. Puttamadappa and H. N. Suresh, "Merged glowworm swarm with ant colony optimization for energy efficient clustering and routing in wireless sensor network", Pervasive and Mobile Computing, vol. 71, pp. 101338, 2021.

[21] R. Ramamoorthy and M. Thangavelu, "An enhanced hybrid ant colony optimization routing protocol for vehicular ad-hoc networks", Journal of Ambient Intelligence and Humanized Computing, pp. 1-32, 2021.

[22] P. R. K. Nalluri and J. B. Gnanadhas, A Cognitive knowledged Energy-Efficient path selection using Centroid and Ant-Colony Optimized Hybrid protocol for WSN-Assisted IoT, 2021.

[23] Gandhi, Y. (2022). Finite element analysis in mechanical engineering: Mathematical foundations and practical applications. EngiMathica: Journal of Engineering Mathematics and Applications, 1(1).

[24] Sherje, N. (2022). Exploring the role of linear algebra in control systems engineering. MathEngage: Engineering Mathematics and Applications Journal, 1(1).

[25] Sharma, R., Nalawade, D. B., Negi, P., Dhabliya, R., Bhattacharya, S., & Khetani, V. (2023, November). AI powered Automation of Fraud Detection in Financial Services. In Proceedings of the 5th International Conference on Information Management & Machine Intelligence (pp. 1-5).

[26] Gulhane, M., Kumar, S., Kumar, M., Dhankhar, Y., & Kaliraman, B. (2023, December). Advancing Facial Recognition: Enhanced Model with Improved Deepface Algorithm for Robust Adaptability in Diverse Scenarios. In 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON) (Vol. 10, pp. 1384-1389). IEEE.