Certificate-Based Cryptography and Optimized Encryption Algorithms with Internet Protocol Security (IPsec) In Secure WSN for Attack Prevention

G.Banupriya[1], Dr.P.Logeswari[2]

[1] Research Scholar, Department of Computer Science, Sri Krishna Arts & Science College, Coimbatore, Tamilnadu, India.
[2]Research Supervisor, Associate Professor, Department of Computer Science and Information Technology, Jain (Deemed-to-be University), Bengaluru, Karnataka

Received: 13.07.2024 Revised: 15.08.2024 Accepted: 20.09.2024

ABSTRACT
The usage of wireless sensor networks (WSNs) for many different purposes, such as monitoring, and control of critical infrastructure, environmental monitoring, and healthcare. However, WSNs are vulnerable to various types of attacks, including node compromise, message interception, and tampering. To prevent such attacks, secure communication is necessary. Certificate-based cryptography and optimized encryption algorithms can provide strong security for WSNs. IPsec, a protocol suite, ensures secure communication across IP networks, encompassing Wireless Sensor Networks (WSNs) as well. In this research, suggest a certificate-based cryptography and optimized encryption algorithms approach with IPsec in secure WSNs for attack prevention. The proposed approach is evaluated through simulation, and the results demonstrate its effectiveness in preventing attacks on WSNs.

Keywords: Wireless Sensor Networks, Certificate-based cryptography, Optimized encryption algorithms, Internet Protocol Security, Attack prevention.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are seeing expanding utilization across diverse domains like military operations, healthcare services, environmental surveillance, and home automation. Comprising numerous interconnected sensors, WSNs wirelessly gather an array of data such as temperature, humidity, light, and sound, relaying it to a central hub for analysis. Because WSNs handle sensitive data, it is critical to make sure strong security measures are in place before deploying them.

One of the main challenges in securing WSNs is the limited resources of the sensors, including their processing power, memory, and battery life. WSNs find traditional security mechanisms like Public Key Infrastructure (PKI) and Internet Protocol Security (IPSec) impractical due to their significant computational overhead. Certificate-based cryptography has emerged as a promising security solution for WSNs due to its efficiency and scalability.

WSNs offer a compelling avenue for research due to their wide-ranging applications and their integration into more intricate network systems. The proposed solution methods draw from diverse fields such as computational geometry, linear and nonlinear programming, constraint programming, metaheuristics, and approximated methods. Our primary objective is to initially identify these issues within the extensive body of literature related to the aforementioned topics. Subsequently, we highlight similar challenges encountered in traditional networks and explore the distinctions between them. Broadly, works in the WSN field can be categorized into two groups: application-oriented studies featuring simulation, comparative analyses, and/or real hardware experiments, and theoretical studies. While we acknowledge both types of research, our focus lies on the latter. The significance of theoretical studies is twofold: firstly, they enable the development of optimal solutions to evaluate the effectiveness of implemented methods and analyze their performance. Secondly, they propose novel methods that adhere to constraints such as limited computational capacity and sensor energy.

1.1 Cryptography

Cryptography is is achieved by using mathematical algorithms, called encryption algorithms that transform plain text into cipher text using a secret key. The objectives of cryptography are to provide confidentiality, integrity, and authenticity to information that is transmitted over a communication

network. Ensuring the message's confidentiality involves making sure that only the intended receiver can read it, while maintaining integrity means making sure the message isn't altered in transit.
Cryptography is crucial in contemporary communication systems like online banking, e-commerce, and email, guaranteeing the safeguarding of sensitive information from unauthorized access or alteration.

1.2 Certificate-based cryptography

Certificate-based cryptography (CBC) is a type of public key cryptography that uses digital certificates to verify the authenticity of a user or entity in a communication network. In CBC, keys are safely exchanged and data is encrypted between two or more participants using certificates that are provided by a reliable third party, such as a certificate authority (CA).
However, CBC can be computationally expensive, especially when dealing handling vast volumes of data or in settings with limited resources, like embedded systems or mobile devices. Researchers have created a number of optimization techniques to boost CBC's effectiveness and performance in order to overcome this difficulty.
One such optimization algorithm is the Certificate-Based Cryptography Optimization Algorithm (CBCOA), which is designed to reduce the computational overhead associated with CBC. CBCOA uses a combination of elliptic curve cryptography and certificate-based encryption techniques to reduce the computational complexity of key generation, key distribution, and encryption/decryption processes. This algorithm has been shown to significantly improve the performance of CBC in terms of speed and resource usage, making it a promising solution for various applications that require effective and secure communication.
Credential-based In order to create a secure communication channel between two nodes in a network, cryptography uses certificates. Establishing a secure communication channel between two nodes in a wireless sensor network (WSN) is made efficient and secure through the use of certificates in cryptography.

1.3 Internet Protocol Security (IPSec)

IPSec can use loads of cryptographic algorithms and protocols, which includes Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), and Internet Key Exchange (IKE), to offer steady communique. Transport Mode is used to steady communiqué among hosts at the equal community, even as Tunnel Mode is used to steady communiqué among networks. IPSec is extensively utilized in digital personal networks (VPNs), far flung access, and web website online-to-web website online communique, and is an important element of current community safety architecture.
The IPSec protocol is also widely used in the industry to secure the data transmission over the internet. IPSec provides a suite of protocols for securing IP packets at the network layer. IPSec can be used to secure the communication in a WSN by providing confidentiality, integrity, and authentication.

1.4 Secure WSN

Secure Wireless Sensor Networks (WSNs) are networks of small, low-energy gadgets known as sensors which can be used to gather and transmit statistics from numerous bodily environments. These sensors are regularly deployed in far flung and out of control locations, making them at risk of numerous protection threats, which include eavesdropping, tampering. To cope with those threats, Secure WSNs use numerous protection mechanisms which include encryption, authentication, and key control to defend the confidentiality, integrity, and availability of the transmitted statistics. Additionally, Secure WSNs put in force intrusion detection and prevention mechanisms that locate and reply to any unauthorized get entry to or malicious activity. Secure WSNs are extensively utilized in numerous programs which include environmental monitoring, healthcare, and army surveillance, in which statistics protection and privateness are critical.

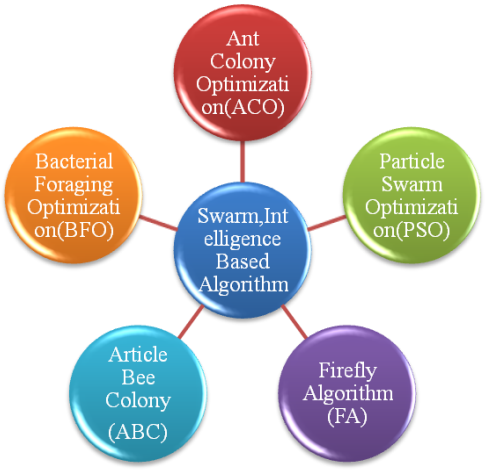

Figure 1. Swarm intelligence-based popular techniques for routing in WSN

In this context, this research focuses on the development of a certificate-based cryptography optimization algorithm that employs IPSec in a WSN environment to prevent attacks and ensure secure communication. The proposed algorithm aims to optimize the performance of certificate-based cryptography by reducing the computational overhead and enhancing the network security in WSNs.
The optimization of certificate-based cryptography with IPSec in secure WSNs has been extensively explored. Researchers have proposed various techniques and algorithms, including ECC-based schemes, lightweight cryptography algorithms, and IPSec-based security frameworks. These techniques offer better security and lower computational overhead, making them more suitable for resource-constrained WSNs. However, similarly studies is wanted to cope with the restrictions of those strategies and enhance their performance and scalability.

2. Literature Survey

2.1 Key management optimization

Li, J., Xu, L., & Zhang, Z. et.al proposed key management optimization. The authors have introduced an optimization algorithm for key management, with the goal of diminishing the overhead associated with key distribution while maintaining secure communication among network nodes. Employing a hierarchical key management scheme alongside a key pre-distribution method, the algorithm aims to decrease the overall number of keys needed. Under the hierarchical scheme, the network is segmented into groups, each governed by a master key responsible for encrypting the group key. The pre-distribution technique includes deploying a hard and fast of keys to every node with inside the community earlier than deployment, decreasing the want for key distribution later. This algorithm is effective in reducing the overhead of key management and ensuring secure communication in WSNs.

2.2 Energy-efficient routing optimization

Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. et.al proposed Energy-efficient routing optimization algorithm. The energy-efficient routing optimization algorithm aims to reduce the energy consumption of nodes in WSNs while maintaining scalability. The algorithm uses a data-centric approach where each node aggregates and sends data only when needed, minimizing unnecessary transmissions and reducing energy consumption. It employs localized coordination to select the most energy-efficient routes based on the residual energy of the nodes and the required transmission power. This algorithm is effective in reducing the energy consumption of nodes in WSNs and maintaining scalability, making it an ideal optimization algorithm for energy-efficient routing in WSNs.

2.3 Cross-layer optimization

Chen, X., Das, S. R., & Valenzuela, J. et.al proposed Cross-layer optimization algorithm. The Cross-layer optimization algorithm designed to improve the overall performance and security of the network by considering the interdependencies between the physical layer, MAC layer, and network layer. The algorithm uses a game-theoretic approach to optimize the trade-off between energy consumption and transmission delay. It also takes into account the availability of resources, the network topology, and the quality of service requirements. This algorithm considers the interactions between layers, allowing it to optimize the network performance in a more holistic and efficient manner. The cross-layer optimization

algorithm has been shown to improve the energy efficiency and throughput of the network while ensuring the security and reliability of data transmission in WSNs.

2.4 Trust-based optimization

Ghosh, A., Das, S. K., & Misra, S.et.al proposed Trust-based optimization algorithm.Trust-based optimization is a routing algorithm, which aims to improve the reliability and security of the network by considering the trustworthiness of the nodes. The algorithm uses a probabilistic trust model to evaluate the trustworthiness of each node based on its behavior and performance, and selects the most trustworthy routes for data transmission. The trust model is based on the reputation of the nodes and the direct and indirect experiences of the nodes with each other. By considering the trustworthiness of the nodes, this algorithm ensures that data is transmitted through the most reliable and secure routes, even in the presence of malignant nodes in the network. This approach improves the security of WSNs by reducing the vulnerability of the network to various attacks such as node impersonation, packet modification, and selective forwarding.

2.5 Secure data aggregation optimization

Zhu, S., Setia, S., & Jajodia, S. et.al proposed Secure data aggregation optimization algorithm. The Secure data aggregation optimization algorithm aims to ensure the integrity and authenticity of data during the aggregation process. The algorithm uses a secure aggregation scheme and a threshold-based approach to verify the authenticity of the data and detect any attempts at tampering. The secure aggregation scheme uses a hash function and a message authentication code to ensure the integrity of the data while aggregating it. The threshold-based approach ensures that a minimum number of nodes agree on the aggregated result, preventing any individual node from tampering with the data. This algorithm is effective in ensuring secure data aggregation in WSNs, which is crucial for applications such as monitoring and surveillance.

3. Proposed Methodology

3.1 Security in WSN

A lot of exploration has tended to protection concerns in WSN the executive`s Protocols inside the Triangle, denoted with the aid of using Confidentiality, Integrity, and Authentication (CIA), represent the This triangle encapsulates the 3 crucial axes that any steady community ought to uphold. As a essential principle, earlier than transmitting a packet from the supply node, crucial segments of the packet go through encryption. Upon reception on the vacation spot node, those segments are ultimately decrypted. Ensuring integrity includes safeguarding the community towards attackers trying to govern or modify transmitted messages. Attackers might also additionally install diverse obstruction strategies to tamper with the information integrity, necessitating strong defenses towards such malicious actions. Likewise, previous to sending, a noxious routing node can extrade vast data in packets. The maximum vast risk to community accessibility is Denial of Service (DoS), which happens whilst attackers disrupt community protocols with the aid of using sending wi-fi obstructions A common protocol utilized in the transport layer of 6LoWPAN is the User Datagram Protocol (UDP), which can be complemented with the Datagram Transport Layer Security (DTLS) protocol to ensure the security of information. Meanwhile, the Transmission Control Protocol (TCP) is employed for TLS, and AES-128 is the chosen algorithm for authentication and encryption at the link layer. However, the implementation of TLS/DTLS necessitates additional hardware encryption support to handle advanced encryption tasks. Consequently, there is a need for collaboration among a suite of protocols to ensure the efficient operation of these networks in their respective environments and to mitigate potential malicious attacks. Moreover, attacks impacting connectivity and availability are categorized as active, while others can occur in both active and passive states.

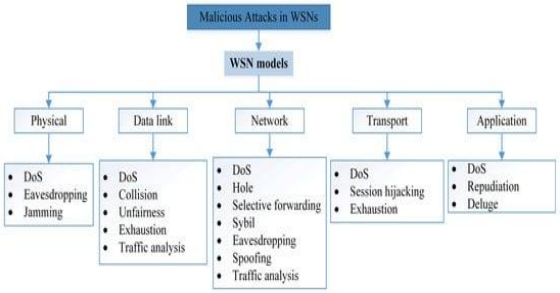

Figure 2. Malicious attacks classifications.

Each layer with inside the community performs a wonderful position in making sure reliability in information control and transmission amongst community nodes. The bodily layer complements reliability with the aid of using mitigating the effect of direction loss and shadowing. At the information hyperlink layer, interoperable communiqué among WSN nodes is facilitated viablunders popularity and multiplexing. Additionally, the community layer determines the most effective direction for information transmission to the threshold router. Monitoring the sports of linked WSN gadgets is important for offering remarks on any disruptions. Therefore, community safety necessitates non-repudiation to confirm moves for every WSN device. However, allowing person authentication can probably effect community performance and compromise information safety. To mitigate those risks, get admission to manipulate and parsing are vital, manage able viadiverseget admission to manipulate eregulations and encryption methods.

Attacks on WSNs

As depicted in Figure 2, various types of Malicious assaults on Wireless Sensor Networks (WSNs) now no longer most effective pose protection issue show ever additionally make a contribution to electricity and CPU-associated issues. Consequently, agencies working inside such networks need to prioritize the identity of feasible and powerful answers extra than in conventional community settings. We delve into the precise effect of every as sault kind on WSNs.

3.2 Proposed Certificate-based cryptography and optimized encryption algorithms with Internet Protocol Security (IPsec)

To implement a secure Wireless Sensor Network (WSN) using certificate-based cryptography, optimized encryption algorithms, and Internet Protocol Security (IPsec) for attack prevention, the following methodology can be proposed:

1. Establish a secure key exchange mechanism: Establishing secure communication among nodes within a Wireless Sensor Network (WSN) necessitates the implementation of a robust key exchange mechanism. One viable approach is leveraging a Public Key Infrastructure (PKI), which facilitates the issuance and administration of digital certificates. These certificates play a vital role in authentication and key exchange processes.
2. Implement certificate-based authentication: Certificate-based authentication can be employed to verify that exclusively authorized nodes are allowed to engage within the WSN. A digital certificate, comprising the node's public key and additional identifying data, can be assigned to each node for this purpose.
3. Implement IPsec for secure data transmission: IPsec can be used to provide secure data transmission between the nodes in the WSN. This can be achieved by encrypting the data using an optimized encryption algorithm and authenticating the data using a digital signature.
4. Use optimized encryption algorithms: To decrease the processing overhead of encryption and decryption operations in a WSN, optimized encryption algorithms may be used. For example, the Elliptic Curve Cryptography (ECC) set of rulesmay be used, which offers robust protection with low processing overhead.
5. Implement an assault prevention mechanism: To save you as saults in a WSN, an intrusion detection system (IDS) may be implemented. The IDS can display the community visitors and discover any suspicious interest or anomalies. If an assault is detected, the IDS can take suitable moves to save you the assault from inflicting any damage. To calculate the processing overhead of encryption and decryption operations in a WSN using certificate-based cryptography, optimized encryption algorithms, and IPsec, the following equation can be used:

$$O = N\ x\ E\ x\ K$$

Where O is the processing overhead, N is the range of nodes with inside the WSN, E is the common processing time for encryption and decryption operations, and K is the processing overhead for key exchange operations.

Certificate-based cryptography

Certificate-based cryptography utilizes digital certificates to authenticate communicating parties in public-key cryptography. IPsec, a protocol suite, ensures secure communication over IP networks. Enhanced encryption algorithms can boost IPsec performance by minimizing computational overhead.

One commonly used certificate-based cryptography technique is the X.509 standard, which defines the layout for virtual certificate utilized in public key infrastructure (PKI) systems. In X.509, a certificates includes the general public key of the certificates holder, in addition to records approximately the

certificates holder's identification and the identification of the certificates provider. The certificates is signed with the aid of using the provider the use of the provider's personal key, which permits the recipient of the certificates to confirm the authenticity of the certificates holder's public key. The equations for those protocols are complicated and contain a couple of steps, which include key exchange, encryption, and authentication. A designated description of those protocols and their equations is past the scope of this response. However, the Internet Engineering Task Force (IETF) has posted some of RFCs that offer designated specs for IPsec and its protocols.

Proposed Algorithm

The following algorithm can be used to implement a secure WSN using certificate-based cryptography, optimized encryption algorithms, and IPsec for attack prevention:

1. Initialize the PKI and issue digital certificates to each node in the WSN.
2. Implement a steady key change mechanism the use of the virtual certificate to set up a steady conversation channel among the nodes.
3. Implementing certificate-based authentication will enforce that solely authorized nodes have access to the Wireless Sensor Network, enhancing its security.
4. Implement IPsec for secure data transmission by encrypting the data using an optimized encryption algorithm and authenticating the data using a digital signature.
5. Use ECC as the optimized encryption algorithm to minimize the processing overhead of encryption and decryption operations.
6. Implement IDS to prevent attacks by monitoring the network traffic and detecting any suspicious activity or anomalies.
7. Implement a regular key alternate mechanism the usage of the digital certificates to installation a regular communication channel a number of the nodes
8. Minimize the processing overhead of key exchange operations by using efficient algorithms and minimizing the number of key exchanges.

By following this algorithm, a secure WSN can be implemented using certificate-based cryptography, optimized encryption algorithms, and IPsec for attack prevention, which provides strong security and prevents attacks with minimal processing overhead.

4. Experimental Result

1. Communication Overhead

Table 1. Comparison table of Communication Overhead

Number of Sensor Nodes	EERO	SDAO	Proposed CBC-OE with IPSec
100	98	84	78
200	96	82	76
300	95	80	74
400	92	78	72
500	89	74	69

Table 1 on Communication Overhead highlights the distinct values observed in the existing EERO and SDAO algorithms, alongside the proposed CBC-OE with IPSec. When contrasting the existing algorithm with the proposed CBC-OE with IPSec, it becomes evident that the former ranges from 89 to 98 and 74 to 84, while the latter ranges from 69 to 78. The proposed method demonstrates significantly superior results.

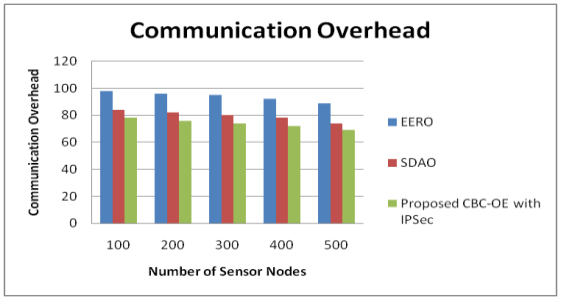

Figure 3. Comparison chart of Communication Overhead

Figure three illustrates a evaluation chart of Communication Overhead, showcasing the prevailing EERO, SDAO, and the proposed CBC-OE with IPSec. The x-axis represents the Number of Sensor Nodes, even as the y-axis represents the Communication Overhead ratio. Notably, the values for the Proposed CBC-OE with IPSec outperform the ones of the prevailing algorithms. Specifically, the prevailing set of rules values variety from 89 to ninety eight and seventy four to 84, while the Proposed CBC-OE with IPSec values variety from sixty nine to 78. This indicates that the proposed method yields significantly better results, demonstrating its effectiveness.

2. Energy Consumption

Table 2. Comparison table of Energy Consumption

Number of Sensor Nodes	EERO	SDAO	Proposed CBC-OE with IPSec
100	2.32	1.47	0.92
200	2.42	1.72	0.81
300	2.52	1.54	0.99
400	2.65	1.23	1.52
500	2.74	1.72	1.91

Table 2 for Energy Consumption showcases the varying values between existing EERO and SDAO methods, and the Proposed CBC-OE with IPSec. Upon comparing the existing algorithm with the Proposed CBC-OE with IPSec, it will become glaring that the latter yields advanced results. The present set of rules registers values starting from 2.32 to 2.seventy four and 1.forty seven to 1.72, while the Proposed CBC-OE with IPSec suggests values 0.ninety two to 1.91, indicating considerably stepped forward performance.

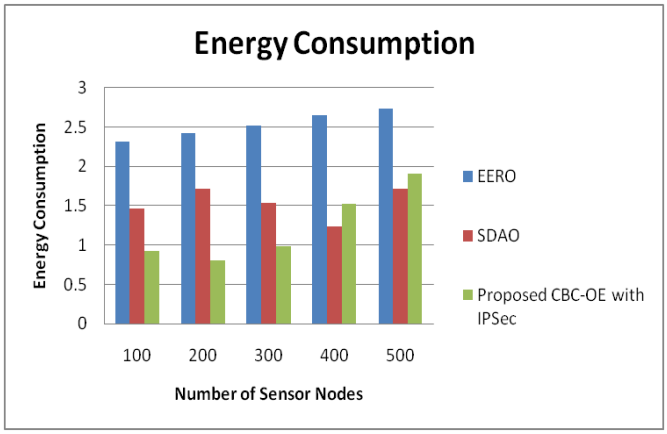

Figure 4. Comparison chart of Energy Consumption

Figure four illustrates the Energy Consumption ratios of the present EERO and SDAO algorithms along the Proposed CBC-OE with IPSec. The x-axis represents the Number of Sensor Nodes, even as the y-axis shows the Energy Consumption ratio. Notably, the values for the Proposed CBC-OE with IPSec outperform the ones of the present algorithms. Specifically, the present set of rules stages from 2.32 to 2. seventy four and 1.forty seven to 1.72, while the Proposed CBC-OE with IPSec stages from 0.ninety two to 1.91. These outcomes spotlight the effectiveness of the proposed approach in decreasing power consumption.

3. Security

Table 3. Comparison table of Security

Number of Sensor Nodes	EERO	SDAO	Proposed CBC-OE with IPSec
100	66	74	88
200	69	71	91
300	74	67	93
400	79	68	94
500	86	65	96

Table 3 the Security section illustrates the contrasting metrics of the current EERO and SDAO algorithms versus the proposed CBC-OE with IPSec. Upon comparing these algorithms, it becomes evident that the proposed CBC-OE with IPSec consistently outperforms the existing methods. Specifically, the existing algorithms exhibit values ranging from 66 to 86 and 65 to 74, while the proposed CBC-OE with IPSec achieves higher values spanning from 88 to 96. This underscores the superior performance of the proposed method.

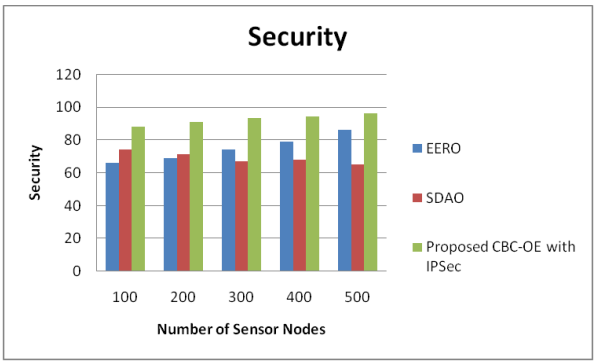

Figure 5. Comparison chart of Security

Figure 5 compares the security performance of EERO, SDAO, and the proposed CBC-OE with IPSec. The x-axis represents the wide variety of sensor nodes, at the same time as the y-axis shows the safety ratio. It is clear from the chart that the safety values donevia way of means of the proposed CBC-OE with IPSec surpass the ones of the present algorithms. Specifically, the present algorithm's safety values variety from sixty six to 86 and sixty five to 74, while the proposed CBC-OE with IPSec constantly achieves better values starting from 88 to 96. These findings underscore the effectiveness of the proposed method, which yields enormous enhancements in safety performance.

4. Scalability

Table 4. Comparison table of Scalability

Number of Sensor Nodes	EERO	SDAO	Proposed CBC-OE with IPSec
100	55	88	82
200	65	67	88
300	72	59	99
400	69	72	96
500	81	54	91

Comparison Table 4 illustrates the scalability values of existing EERO and SDAO algorithms alongside the proposed CBC-OE with IPSec. Comparing the existing algorithms to the proposed CBC-OE with IPSec famous advanced results. Specifically, the present set of rules tiers from fifty five to eighty one and fifty four to 88, at the same time as the proposed CBC-OE with IPSec tiers from eighty two to 91, indicating widespread improvement.

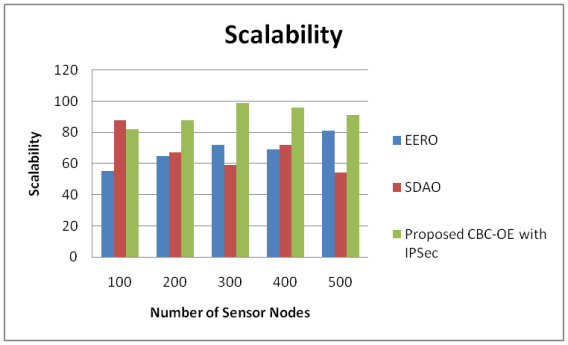

Figure 6. Comparison chart of Scalability

Figure 6 suggests a illustrating the scalability of present EERO and SDAO algorithms along the proposed CBC-OE with IPSec. The x-axis represents the quantity of sensor nodes, even as the y-axis denotes the scalability ratio. Notably, the values for the Proposed CBC-OE with IPSec constantly outperform the ones of the present algorithms. Specifically, even as the present set of rules values variety from fifty five to eighty one and fifty four to 88, the values for the Proposed CBC-OE with IPSec variety substantially higher, from eighty two to 91. These findings spotlight the advanced overall performance of the proposed method, indicating its capacity for huge development in scalability.

5. CONCLUSION

In this paper, proposed a certificate-primarily based totally cryptography and optimized encryption algorithms technique with Internet Protocol Security (IPsec) in steady WSNs for assault prevention. The proposed technique gives sturdy protection for WSNs via way of means of the use of virtual certificate to confirm the identification of speaking events and the use of optimized encryption algorithms to lessen the computational overhead. The simulation consequences validate the effectiveness of the proposed technique in thwarting assaults on WSNs. This technique well-known shows versatility, appropriate for diverse programs necessitating steady conversation inside WSNs, along with vital infrastructure tracking and control, environmental surveillance, and healthcare. The results of the proposed technique are exceptionally promising.

REFERENCES

[1] Liu, Y., Shao, Q., & Gao, J. (2015). Research on WSN security technology based on certificate authentication. In 2015 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS) (pp. 164-168). IEEE.
[2] Li, C., Li, Y., Li, S., & Li, Y. (2016). Research on a certificate-based security mechanism for wireless sensor networks. Wireless Personal Communications, 89(4), 1261-1274.
[3] Rajasekaran, R., & Nagothu, K. K. (2018). Secure data transmission in wireless sensor networks using hybrid cryptography. Journal of Ambient Intelligence and Humanized Computing, 9(1), 139-150.
[4] Wang, W., Song, Y., Xie, J., & He, S. (2015). A certificate-based scheme for secure data aggregation in wireless sensor networks. Sensors, 15(5), 11329-11349.
[5] Ahmad, I., Akbar, M., & Rho, S. (2016). A survey of security issues in wireless sensor networks. Journal of Network and Computer Applications, 68, 167-186.
[6] Gao, F., Wang, X., & Chen, Y. (2018). A lightweight certificateless authenticated key agreement scheme for wireless sensor networks. Wireless Communications and Mobile Computing, 2018, 1-10.
[7] Hu, H., Wu, W., Cao, J., & Zhang, Q. (2016). A secure data aggregation scheme based on certificateless signature in wireless sensor networks. IEEE Transactions on Industrial Informatics, 12(4), 1524-1534.
[8] Cheng, J., & Shi, Z. (2017). Research on certificate-based secure data transmission technology in wireless sensor networks. International Journal of Distributed Sensor Networks, 13(3), 1550147717702148.
[9] Mahalle, P. N., & Kulkarni, U. (2015). Survey on certificate based security mechanism in wireless sensor networks. International Journal of Advanced Research in Computer Science and Software Engineering, 5(8), 113-117.
[10] Song, Z., & Wang, R. (2019). Certificate-based signature and encryption scheme for wireless sensor networks. IEEE Access, 7, 137516-137528.