Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 28 No. 7s (2025)

Crswsn-Based Framework for Secure Routing in Wireless Sensor Networks

Dr.K.Akila[1], Dr.S.Padmapriya[2], Mrs.P.Anitha[3], Mrs.C.Merlyne Sandra Christina [4], Mrs.N.Radha[5] ,Mrs.S.Gowthami[6]

[1]Assistant Professor

Department of Computer Science & Engineering,

School of Engineering & Technology,

Dhanalakshmi Srinivasan University, Trichy

[2]Assistant Professor

Department of Computer Science & Engineering,

School of Engineering & Technology,

Dhanalakshmi Srinivasan University, Trichy

[3]Assistant Professor

Department of Computer Science & Engineering,

School of Engineering & Technology,

Dhanalakshmi Srinivasan University, Trichy

[4]Assistant Professor

Department of Computer Science & Engineering,

School of Engineering & Technology,

Dhanalakshmi Srinivasan University, Trichy

[5]Assistant Professor

Department of Computer Science & Engineering,

School of Engineering & Technology,

Dhanalakshmi Srinivasan University, Trichy

[6]Assistant Professor

Department of Computer Science & Engineering,

School of Engineering & Technology,

Dhanalakshmi Srinivasan University, Trichy

Article History:

Received: 25-05-2025

Revised: 19-06-2025

Accepted: 02-07-2025

Abstract: The collection of sensor nodes is termed as wireless sensor network. The back bone of WSN is sensor. The sensors are used to sense the environment and transfer the data by the use of network infrastructure and to meet the user's requirements. The sensor node has the limitations in terms of storage, communication and computational capabilities. The application which may utilize WSN can be of susceptible and necessitate superior secured environment. As sensors are used to monitor the environment, security and energy efficiency is most essential considerations when designing wireless sensor networks. The security of WSN must be remunerated concentration to because it is supported by lofty content and multifarious structure. The framework suggested three algorithms such as contribution 1 proposed secure dynamic authentication for WSN using Salt key approach and contribution II suggested secure text encryption scheme for WSN using Dynamic Key approach, contribution III introduced energy efficient secured dynamic routing for cluster based WSN.

Introduction: Wireless Sensor Network has several nodes where each node is connected to one or more sensors. Achieving Security along with Energy sustainable is not a easy task. The typical sensor node has four main blocks which are power unit, communication unit, processing and sensing unit. Sensor nodes are used to monitor static and dynamic events where as monitoring static events are easy, on the other hand the dynamic events are typically needs efficient protocol performance. Protocols are in the form of specific functionality. In the field of WSN have many challenges.

Objectives: Increase the network parameters performance such as Latency, Throughput and **Security.**

Methods: Hash based Algorithm and Dynamic Key approach, Salt key Approach and Secure Dynamic routing protocol structure

Results: Security

Security is important in any area, but it is especially important in network security, which resembles the strength of the network architecture The proposed method's average security value is 98.3 percent, which is higher than that of other current methods; the lowest security level is 97 percent, and the highest security level is 98 percent.

Conclusions: The contribution methods proposed three different algorithms for achieving better results in security. The proposed method of ESDSA suggested the algorithm for achieving user registration and sensor node

registration and the method of ESEDK provides the methodology for creating the salt key to achieve the security and the method of ESDRC provides the algorithm for forming the clusters along with cluster head based on the distance and energy and to achieve the security. The methodology is used to reduce energy consumption and secure data delivery. It uses energy, distance to the base station and the number of neighbors based parameters for cluster head selection. The cluster head is used to transmit data packets from the sensor node to the base station. The simulation results proved that the CRSWSN algorithms provided the better lifetime, security and less energy consumption.

1. Introduction

Wireless Sensor Network has several nodes where each node is connected to one or more sensors. Achieving Security along with Energy sustainable is not a easy task. The typical sensor node has four main blocks which are power unit, communication unit, processing and sensing unit. Sensor nodes are used to monitor static and dynamic events where as monitoring static events are easy, on the other hand the dynamic events are typically needs efficient protocol performance. Protocols are in the form of specific functionality. In the field of WSN have many challenges.

Challenges in WSN

1. **Deployment of Node:** The deployments of nodes are categorized into deterministic or randomly scattered.
2. **Consumption of Energy without losing Accuracy:** Performance of the sensors based on the ebattery lifetime. In WSN, Sensor nodes can use up their limited supply of energy performing computations and transmission of information through a wireless environment.
3. **Data Sensing and Reporting:** Sensing and reporting of data in WSN is based on query-driven, time-driven or event-driven.
4. **Fault Tolerance:** Due to the lack of power, physical damage and interference of physical surroundings, the sensor nodes may fail or block.
5. **Security:** In the applications of military, medical field, the communication among nodes is required to be secured.

A wireless sensor network (WSN) contains sensor nodes that collect data from their surroundings in real-time. WSNs offer a trustworthy and competent data assortment mechanism. On the other hand, WSN comprises limited power, memory, computing capability, transmission length, and lifespan resources [13]. Sensor nodes are capable of sensing and communicating with other nodes through the bus. It encompasses clusters of sensor nodes scattered at random to communicate through the wireless channel to trail environmental constraints such as sound, friction, strain, weather, and so on. The WSN is self-acquired of three main components [1]: a gateway node (GW), a sensor node (SN), and a

user (U). The sensor node monitors the physical environment, and GW facilitates communication between the user and the sensor node. Sensor nodes collect useful data, which are capable of computation but have limited storage space. Sensor nodes are battery-powered. WSN architecture uses protocol and standards that are modulated and uses energy to extend their lifetime. Privacy of data ,authentication and integrity of data are the necessities for wireless sensor network [11]. The following diagram Figure 1 represents the communication between the nodes and gateway.

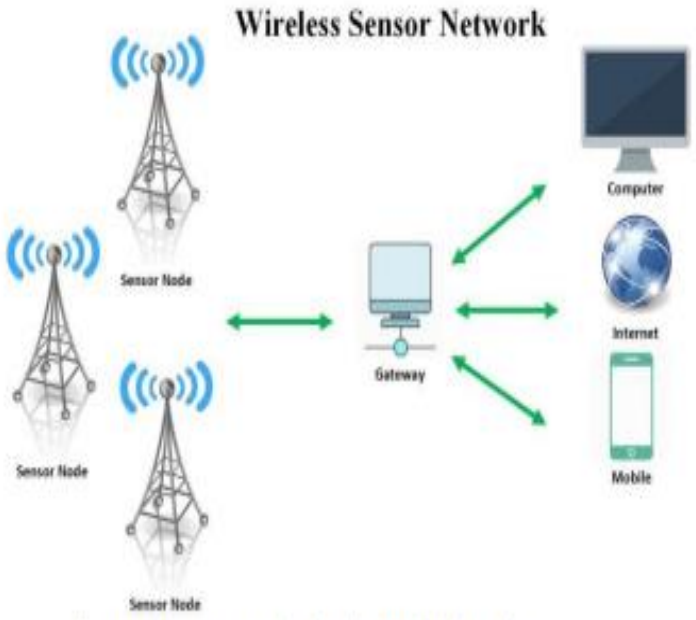


Figure .1 data communication in a WSN through gateway

The following are the proposed works for secured sensing, monitoring and controlling using energy efficient architecture. [2] It proposed a well-organized dynamic authentication and key management scheme. Although maximizing the protection level, this approach offers a single lightweight protocol for authentication and key establishment. The key distribution method creates dynamic keys using pre-existing information and does not need a secure channel or sharing process, which improves protection, energy efficiency, and memory usage. WSNs can have security, verification, trust and safety to data without internet connectivity, depending on the complexity of the programme. ESEAAK [3] suggested three –factor authentication and key agreement protocol based on light weight authentication scheme. An XOR and hash function based on elliptic curve Diffie-Hellman algorithm is used to resolve the security concern. EDAK [4] proposed an efficient dynamic authentication and key management scheme offers a single lightweight protocol for authentication and key establishment. The key distribution method generated dynamic keys using pre-existing information and does not need a secure channel or sharing process, which improves protection, energy efficiency, and memory usage. SIAEM [9] proposed two modules of customized clustering of IoT-WSN nodes (CCIN) and energy-aware state change routing protocol (EASCRP). The method of CCIN and EASCRP suggested the algorithm for classifying the wireless sensor nodes based on their energy. It categorized the nodes of low-power, medium-power and high-power nodes and the algorithm EASCRP provides the alternate paths. SIAEM-II [10] suggested the method of dynamic security scheme manager (DSSM). The method of DSSM shuffles the data

according the algorithm. Yousefpoor [12] suggested an intelligent dynamic key management system that uses fuzzy logic for path key generation and adding new nodes to the network.

An Efficient Secure Dynamic Authentication for WSN Using Dynamic Salt Approach

The proposed method [5][8] suggested simple hash algorithm with lowest time complexity for achieving more security. Sensor nodes are equipped with limited power consumption and lowest storage communication possibilities. The remote sensors authentication is major security problem. The proposed method contains three phases: Registration, Authentication and Password change.

A. Registration Phase

To access WSNs service, a user U_i and a sensor S_j have to register with gateway GWN.

User Registration

User U_i selects unique identity U^{ID}_i, password U^{PWD}_i, PIN U^{PIN}_i and generate a random salt value (U^{S}_i), then compute the following values to register with the GWN. The creation of a salt value based on the combination of random numbers and characters (alphabets lowercase and uppercase) with 8-bit length. The detailed steps involved in a user registration process as follows:

User Registration with GWN
1: User U_i select User Identity U^{ID}_i , Password U^{PWD}_i and Pin Number U^{PIN}_i
2: Generate random salt value (U^{S}_i)
3: If U^{PIN}_i % 2 ==0
4: V1=append (U^{S}_i) with U^{PWD}_i in even position
5: V2 = append (U^{S}_i) with U^{PIN}_i in odd position
6: Else
7: V1= append (U^{S}_i) with U^{PWD}_i in odd position
8: V2 = append (U^{S}_i) with U^{PIN}_i in even position
9: EndIF
10: U^{PWDSH}_i = h(V1) and U^{PINSH}_i = h(V2)
11: V3 = h(U^{ID}_i || V1) and V4 = h(U^{ID}_i || V2)
12: U^{ECP}_i = h(U^{PWDSH}_i || U^{PINSH}_i) h(V3 || V4)
13: User U_i send U^{ID}_i , U^{S}_i and U^{ECP}_i to GWN
14: If U^{ID}_i already exists in GWN then
15: Send a denial notification to U_i
16: Else
17: GWN store U_i information [U^{ID}_i , U^{S}_i and U^{ECP}_i]
18: End If

Sensor Registration

This subsection explains sensor registration with the gateway node. Each sensor node is configured with unique S^{ID}_j when the time of node deployment. The following step describes the sensor registration.

Sensor Registration with GWN
1: Sensor SN_j select S^{ID}_j
2: Generate random salt value (S^{S}_i)
3: Compute $S^{SH}_j = h(S^{S}_j)$
4: $X1 = bin(S^{ID}_j) \oplus S^{SH}_j$
5: Sensor Node SN_j send X1 and S^{SH}_j to GWN
6: GWN Compute $X2 = X1 \oplus S^{SH}_j$
7: $X3 = h(X2 \parallel S^{SH}_j)$
8. GWN store X2 and X3 and send X3 to SN_j

A. Authentication Phase

In the phase of Authentication, User's credentials are verified by login process. The login process, prevent the sensors from denial-of-service attack. The user computes the authentication information and then compares it to the previously stored data. After authentication, the legitimate user is granted access. The following steps are used to authenticate user U_i

User Authentication
1: User U_i provide U^{ID}_i, U^{PWD}_i, U^{PIN}_i and get U^{S}_i
2: Compute V1 and V2 based on U^{PIN}_i
3: Compute $U^{PWDSH}_i = h(V1)$ and $U^{PINSH}_i = h(V2)$
4: $V3 = h(U^{ID}_i \parallel V1)$ and $V4 = h(U^{ID}_i \parallel V2)$
5: $newU^{ECP}_i = h(U^{PWDSH}_i \parallel U^{PINSH}_i) \oplus h(V3 \parallel V4)$
6: User U_i send $newU^{ECP}_i$ to GWN
7: GWN retrieve U_i encrypted password U^{ECP}_i
8: If $newU^{ECP}_i == U^{ECP}_i$ then
9: Legitimate User access sensor information
10: Else
11: Illegal User request
12: End If

B. Password Change Phase

The following steps are used to modify the password U^{PWD}_i or PIN U^{PIN}_i of the User U_i.

Change Password

1: User U_i perform authentication process for User legitimate verification

2: User U_i retrieve salt value U^S_i

3: U_i input new password $newU^{PWD}_i$ and/or new pin number $newU^{PIN}_i$

4: Compute newV1 and newV2 based on $newU^{PIN}_i$

5: Recompute $newU^{PWDSH}_i$ and $newU^{PINSH}_i$

6: Recompute newV3 and newV4

7: Compute $newU^{ECP}_i = h(newU^{PWDSH}_i \,||\, newU^{PINSH}_i) \oplus h(newV3 \,||\, newV4)$

8: User U_i send $newU^{ECP}_i$ to GWN

9: GWN update U_i new password $newU^{ECP}_i$

An Efficient and Secure Text Encryption Scheme For Wireless Sensor Network Using Dynamic Key Approach

The proposed methods [6] recommended a lightweight, energy-efficient secure text encryption using dynamic salt key. There are three primary processes in the suggested paradigm. The first is salt generation. The next step is to encrypt secret text using format-preserving encryption based on the salt key, and the final step is to decrypt the data. The encryption process is more secure, and the hackers cannot capture key values. The proposed approach created a protected environment for sensors for protecting the data quickly, efficiently, and low-computation before sending it across a wireless network to the sink node. The proposed method simulation provides a high level of security while requiring minimal communication and computational resources. The sophisticated encryption/decryption procedure enhances the cryptographic approach's security, but it uses many computational resources. Sensor nodes in a WSN are typically resource-restricted, meaning they have limited energy, processing power, and memory. In addition, lightweight batteries, which cannot be replaced or recharged, are expected to power sensor nodes. In this instance, a data encryption mechanism that is both secure and low-power is required.

This section explains the proposed lightweight, energy-efficient, secure text encryption using the dynamic salt key. The proposed method contains three phases: Salt Key Generation, Data Encryption and Data Decryption.

A. Salt Key Generation

Algorithm-1 explains the salt key generation

Algorithm-1: Salt Key Generation

Step1: Assign base= 0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

Step2: s1 = randomly select 8 characters in base

Step3: For i = 1 to length(s1)

Step4: a1 = ascii(s1[i])

Step5: a2 = hex(a1)

Step6: salt[i] = a2;

Step7: End For

Step8: Return salt

In this algorithm, the combination of numbers and alphabets are assigned to the base string (step1). Then, the initial salt value is generated based on the base string, which contains an 8-bit length (step2). Then, for each character in the initial salt value, get the ASCII value (step4) and convert it to hexadecimal (step5). Finally, the generated salt value is used for data encryption.

B. Data Encryption

This section explains the proposed data encryption process. Algorithm-2 explain the data encryption process. Initially, the plain text (secret text) is converted into matrix format. Then, the generated salt key is appended with the matrix. Finally, using format-preserving encryption, the generated matrix is encrypted. The decryption process is the reverse of the encryption scheme.

Algorithm-2 Data Encryption

Input: Plain Text (PT)

Output: Encrypted Text (ET)

Step1: Get the secret plain text (PT) of 16-bit length

Step2: Convert PT into matrix (MAT1) format based on (1)

Step3:Generate salt key (SK) using Algorithm-1

Step4: MAT2 = Add SK into MAT based on (2)

Step5: Convert MAT2 into Message (SM)

Step6: binSM = binary format(SM)

Step7: ET = FPE(binSM)

Step8: Return ET

An Energy-Efficient Secure Dynamic Routing For Cluster-Based Wireless Sensor Network

The proposed method [7] suggested the method of node clustering and the cluster head selection process. Initially, the N number of nodes are randomly distributed in a (W * H) area with one base station located at the centre point of the area. Thus, all sensor nodes have the same initial energy, and the base station has unlimited energy and computing power. Algorithm-1 shows the node clustering and cluster head selection.

Algorithm1: Node Clustering and Cluster head selection

Step1: Deploy N number of nodes in MxM area

Step2: Create base station (BS) in the centre position of the network area

Step3: Split network area into four regions (R)

Step4: For i = 1 to |R|

Step5: NC_i = Count no of nodes in R_i

Step6: For j = 1 to $|NC_i|$

Step7: D = Compute the distance between NC_{ij} and BS

Step8: NR= Count no of neighbours nearest NC_{ij}

Step9: Engr = Get Current energy of Node

Step10: End For

Step11: C = Find optimal Node based on (D, NR, Engr)

Step12: Select C as Cluster Head (CH_i)

Step13: End For

In this algorithm, the network area is divided into four regions. First, the cluster head node is selected based on the distance, neighbors and energy level. Then, the cluster head is updated based on the packet delivery ratio of the CH.

Dynamic Routing:

This section explains the proposed dynamic routing for improving network performance. This routing is used to find the optimal best path, which leads to the extended lifetime of the network. Algorithm-2 shows the dynamic routing

Algorithm-2 Dynamic Routing

Step1: BS generate the salt key (SK)

Step2: BS distribute SK to each cluster head (CH)

Step3: If Node has any sensed message

Step4: Transmit the message to CH

Step5: CH checks the BS communication range

Step6: If CH is nearest to BS, then

Step7: CH send message to BS

Step8: Else
Step9: Send a message to the nearest CH
Step10: Continue until BS reaches.
Step11: End IF
Step12: End IF

Dynamic Encryption and Decryption

This section explains the proposed dynamic encryption and decryption algorithm for secure message transmission. Initially the salt key is randomly generated based on the combination of numbers and alphabets. The size of the salt key is based on the length of plain text. Algorithm-3 explains the encryption process.

Algorithm-3 Data Encryption

Input: Plain Text (PT)
Output: Encrypted Text (ET)
Step1: n=Length(PT)
Step2: Set base= 0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
Step3: salt= randomly select n characters from base
Step4: v1 = 0
Step5: for i = 0 to n
Step6: v2=(ascii(salt(i))+ascii(PT(i))+v1)%256;
Step7: ET=ET+(char(v2))
Step8: v1=v2;
Step9: end for
Step10:Return ET, salt

COMPARISON OF THE PERFORMANCE OF PROPOSED METHODS

The following table shows the comparison of the proposed methods.

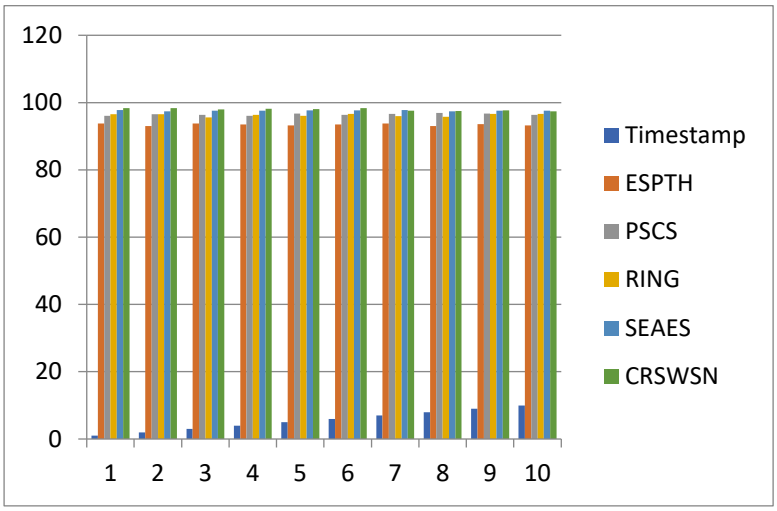
Contribution	Methodology	Advantages	Disadvantage
Hash based Algorithm and Dynamic Key approach	1. User registration with GWN 2. Sensor registration with GWN 3. User Authentication	1. The method improves the security based on dynamic hash key function 2. Security improved	Concentrated on security alone.

	4. Change of Password	based on the credentials of Change of Password and Pin	Network parameters are not achieved
Salt key Approach	1. Salt key Generation 2. Data Encryption 3. Data Decryption	1. Achieves Security based on Salt Key Generation	Network parameters are not concentrated
Secure Dynamic routing protocol structure	1. Node Clustering and Cluster head Selection 2. Dynamic Routing 3. Data Encryption and Decryption	1. Formed the cluster head based on the distance and energy level 2. Based on the algorithm of Dynamic Routing, Calculated the path between the nodes and cluster head 3. Security achieved by data encryption and decryption	Other network parameters are not concentrated

Experimental Results

1. **Security**

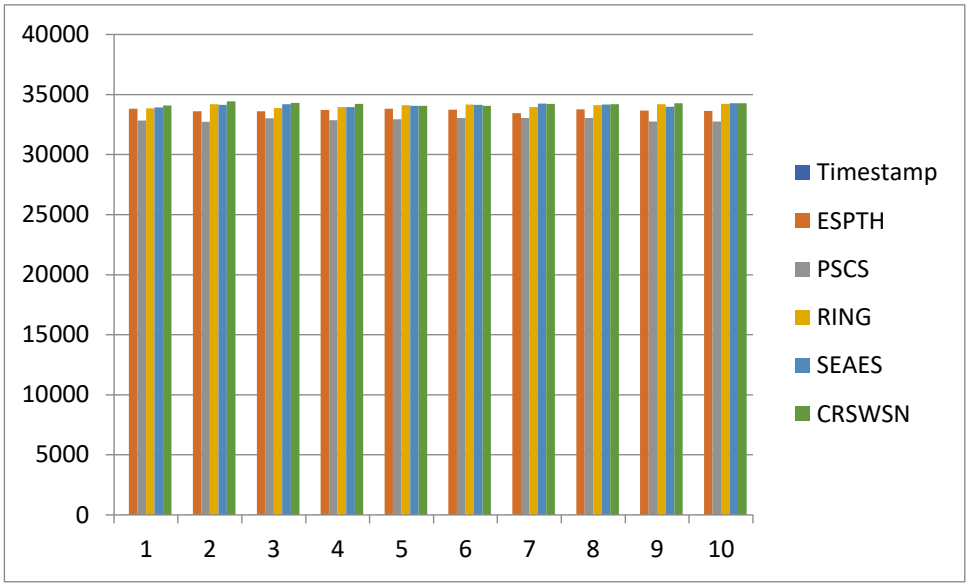
Security is important in any area, but it is especially important in network security, which resembles the strength of the network architecture The proposed method's average security value is 98.3 percent, which is higher than that of other current methods; the lowest security level is 97 percent, and the highest security level is 98 percent.



Security(%)					
Timestamp	**ESPTH**	**PSCS**	**RING**	**SEAES**	**CRSWSN**
1	93.8	96.1	96.5	97.8	98.3
2	93.0	96.5	96.5	97.4	98.3
3	93.8	96.3	95.6	97.6	98.0
4	93.5	96.1	96.3	97.6	98.2
5	93.2	96.7	96.1	97.7	98.1
6	93.5	96.3	96.6	97.7	98.3
7	93.8	96.6	96.0	97.8	97.6
8	93.0	96.9	95.8	97.4	97.5
9	93.6	96.7	96.6	97.6	97.7
10	93.2	96.3	96.6	97.6	97.4

2. Throughput (Kbps)

The content flow rate of a communication channel is referred to as throughput.

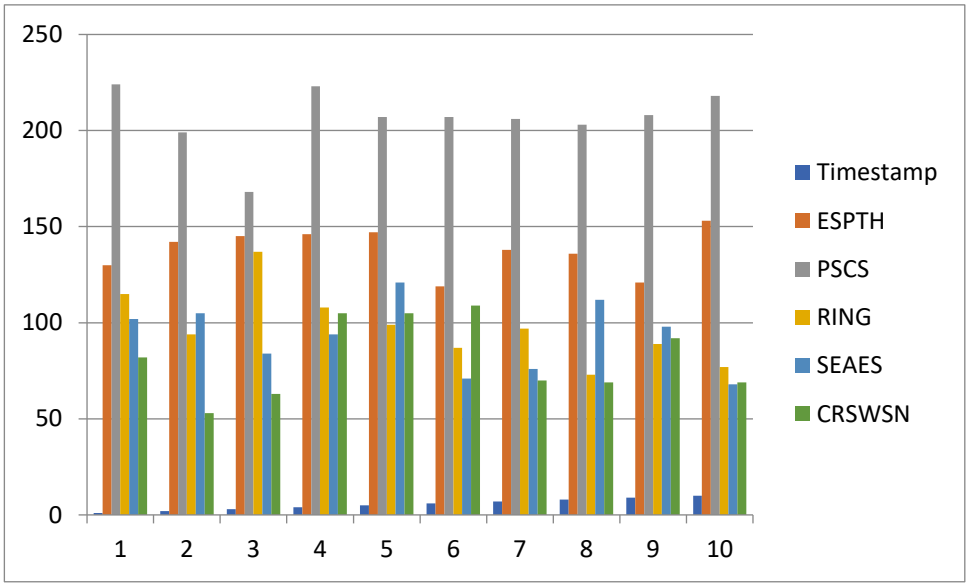


Throughput (Kbps)					
Timestamp	**ESPTH**	**PSCS**	**RING**	**SEAES**	**CRSWSN**
1	33813	32836	33845	33930	34086
2	33612	32736	34194	34130	34429
3	33596	33012	33880	34194	34306
4	33724	32870	33953	33963	34232
5	33820	32928	34115	34055	34050
6	33739	33041	34170	34145	34064
7	33436	33051	33959	34260	34227
8	33755	33059	34116	34160	34181
9	33662	32755	34191	33981	34265
10	33646	32749	34231	34275	34266

Based on the analysis, existing methods ESPTH and CRSWSN were used to provide a provision throughput values in a network with 100 nodes. With an increment in the number of nodes, the rate of dwindling rapidly increases. The proposed CRSWSN achieves the maximum average throughput of 34210 kbps.

3. End-to-End Delay (mS)

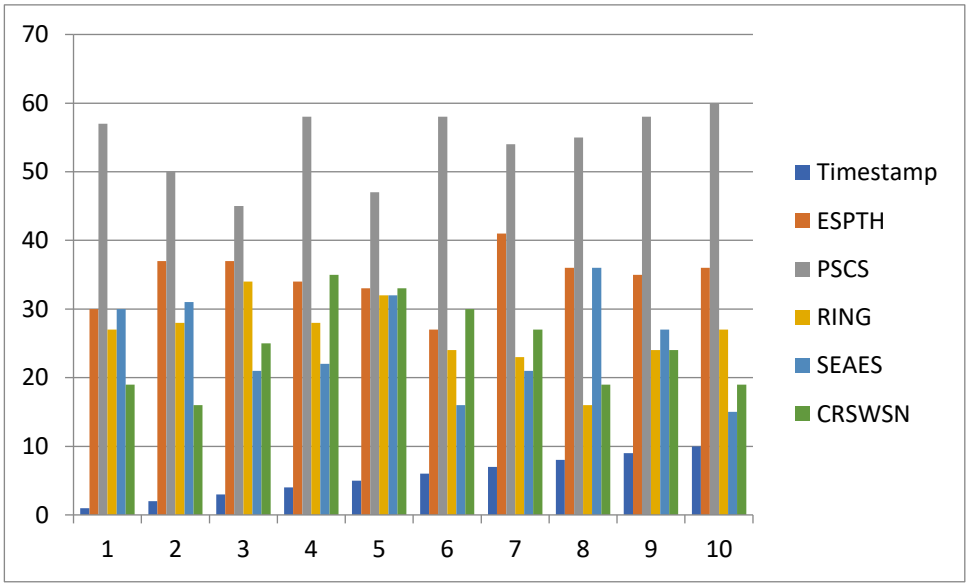
The combined amount of all communications delays, such as jitter, IP-delay, and system delay, is called end-to-end delay. It refers to the total time taken for a data packet to travel from its origin to the destination.



End-to-End Delay (ms)					
Timestamp	**ESPTH**	**PSCS**	**RING**	**SEAES**	**CRSWSN**
1	130	224	115	102	82
2	142	199	94	105	53
3	145	168	137	84	63
4	146	223	108	94	105
5	147	207	99	121	105
6	119	207	87	71	109
7	138	206	97	76	70
8	136	203	73	112	69
9	121	208	89	98	92
10	153	218	77	68	69

4. Latency (mS)

Latency refers to an expression of how much time it takes for a data packet to travel from one designated point to another. Latency is measured by milliseconds.



Latency (ms)					
Timestamp	**ESPTH**	**PSCS**	**RING**	**SEAES**	**CRSWSN**
1	30	57	27	30	19
2	37	50	28	31	16
3	37	45	34	21	25
4	34	58	28	22	35
5	33	47	32	32	33
6	27	58	24	16	30
7	41	54	23	21	27
8	36	55	16	36	19
9	35	58	24	27	24
10	36	60	27	15	19

The interval between the triggering of data transmission and the start of data transmission is known as latency. Higher quality channels would have lower latency, as latency is approximately equal to a network's performance. In milliseconds, latency is calculated.

Experimental Setup

S.No	Entity	Details
1	Simulation Area	10000 Square meters
2	Number of Nodes	100 to 1000 in step 100
3	IoT-Node types	ESP-32, ESP-8 266, LoRa (Uniform Distribution)
4	Number of Routers	Automatic Selection
5	Node Placement	Random distribution
6	Network density	Default
7	RF Range of IoT-WSN Nodes	Based on the type from 100 meters to 1000 meters
8	Frequency bands	Auto-select
9	Simulation Time	168 real-world hours

Conclusion

The contribution methods proposed three different algorithms for achieving better results in security. The proposed method of ESDSA suggested the algorithm for achieving user registration and sensor node registration and the method of ESEDK provides the methodology for creating the salt key to achieve the security and the method of ESDRC provides the algorithm for forming the clusters along with cluster head based on the distance and energy and to achieve the security. The methodology is used to reduce energy consumption and secure data delivery. It uses energy, distance to the base station and the number of neighbors based parameters for cluster head selection. The cluster head is used to transmit data packets from the sensor node to the base station. The simulation results proved that the CRSWSN algorithms provided the better lifetime, security and less energy consumption.

References

[1] M.F. Moghadam, M. Nikooghadam, MABA Jabban, M. Alishahi, L. Mortazavi and A. Mohajerzadeh, "An Efficient Authentication and Key Agreement Scheme Based on ECDH for Wireless Sensor Network," in IEEE Access, vol. 8, pp. 73182-73192, 2020

[2] M.Lavanya, V. Natarajan, "LWDSA: lightweight digital signature algorithm for wireless sensor networks", Sādhanā, Indian Academy of Sciences, vol. 42, no. 10, pp. 1629–1643 2017

[3] J. Jung, J. Moon, D. Lee, and D. Won, "Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks," Sensors, vol. 17, no. 3, p. 644, 2017

[4] S. Athmani, A. Bilami, and D. E. Boubiche, "EDAK: An efficient dynamic authentication and key management mechanism for heterogeneous WSNs", Future Gener. Comput. Syst., vol. 92, pp. 789–799, Mar. 2019

[5] V.Elamurugu, Dr.D.J.Evanjaline, “An Efficient Secure Dynamic Authentication for WSN Using Dynamic Salt Approach”, International Journal of Innovative Research in Science, Engineering and Technology, ISSN-No: 2319-8753, Vol.10, December 2021

[6] V.Elamurugu, Dr.D.J.Evanjaline, “An Efficient and Secure Text Encryption Scheme for Wireless Sensor Dynamic Key Approach”, International Journal of Computer Networks and Applications, ISSN-No: 2395-0455, Vol.8,Issue.6, December 2021

[7] V.Elamurugu, Dr.D.J.Evanjaline, “An Energy-Efficient Secure Dynamic Routing for Cluster-Based Wireless Sensor Network ”, International Journal of Mechanical Engineering, ISSN-No:0974-5823, Vol.7,Issue.6, December 2021

[8] V.Elamurugu, Dr.D.J.Evanjaline, “A Review on Dynamic Key-based Cryptographic Techniques”, International Journal of Innovative Research in Science, Engineering and Technology, ISSN-No: 2319-8753, Vol.10, September 2021

[9] K.Akila, Dr.D.J.Evanjaline, “Strengthening IoT-WSN Architecture for Environmental Monitoring”, International Journal of Innovative Technology and Exploring Engineering, ISSN-No: 2278-3075, Vol.8, Issue-11, September 2019

[10] K.Akila, Dr.D.J.Evanjaline, “Secured IoT-WSN Architecture for Monitoring Environmental Pollution”, International Journal of Scientific and Technology Research, ISSN-No: 2277-8616, Vol.8, Issue-12, December 2019

[11] M.Lavanya, V. Natarajan, "LWDSA: Lightweight Digital Signature Algorithm for Wireless Sensor Networks", Sādhanā, Indian Academy of Sciences, vol. 42, no. 10, pp. 1629–1643 2017

[12] M.S. Yousefpoor, H. Barati, "DSKMS: a dynamic smart key management system based on fuzzy logic in wireless sensor networks", Wireless Networks, vol. 26, pp. 2515–2535, 2020

[13] H. Hayouni, M.A. Hamdi, "A novel energy-efficient encryption algorithm for secure data in WSNs", Journal of Supercomputing, vol. 77, pp. 4754–4777, 2021