INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

DynAuthRoute: Dynamic Security for Wireless Sensor Networks

V Elamurugu[1]*, **D J Evanjaline**[2]

1 Research Scholar, Department of Computer Science, Rajah Serfoji Government College (Autonomous), Affiliated to Bharathidasan University, Tanjore, Tamil Nadu, India
2 Assistant Professor, Department of Computer Science, Government Arts College, Affiliated to Bharathidasan University, Thiruverumbur, Trichy, Tamil Nadu, India

OPEN ACCESS

Received: 06-01-2024

Accepted: 29-01-2024

Published: 22-03-2024

Citation: Elamurugu V, Evanjaline DJ (2024) DynAuthRoute: Dynamic Security for Wireless Sensor Networks. Indian Journal of Science and Technology 17(13): 1323-1330. https://doi.org/10.17485/IJST/v17i13.49

* **Corresponding author**.

rschlrelamurugu@outlook.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: The research aims to design an architecture for secure transmission of data in wireless sensor networks. **Methods:** The method involves three main pillars: authentication, data encryption, and dynamic routing. Extensive simulations have been conducted to evaluate the suggested method in terms of energy consumption, memory footprint, packet delivery ratio, end-to-end latency, execution time, encryption time, and decryption time. **Findings:** For authentication, a dynamic key is used to power an improved salt password hashing method. Data encryption is performed using format-preserving encryption (FPE) with the appended salt key. Dynamic routing is implemented using a cluster-based routing technique to enhance network efficiency in terms of power consumption and security. The execution time for MD5 ranges from 15 to 22 milliseconds, while for SHA-1 it ranges from 16 to 23 milliseconds and for the proposed salt key generation it is 1 to 5 milliseconds. Similarly, in terms of energy consumption, memory footprint, packet delivery ratio, end-to-end latency, execution time, encryption time, and decryption time the proposed method shows promising results in ensuring the integrity and security of transmitted encrypted data. **Novelty:** The presents a novel architecture with enhanced cluster head-based selection algorithm that combines dynamic key-based authentication and secure data routing to establish a safe environment for data transmission in wireless sensor networks. This research works offers a method for encrypting text with a dynamic salt key that is safe, energy-efficient, and lightweight.

Keywords: Wireless Sensor Network; Dynamic Key; Authentication; Hash function; Salt algorithm; Dynamic routing; Node clustering; Format-preserving encryption

1 Introduction

There is a growing interest in Wireless Sensor Networks (WSNs) in several fields, including those of environmental monitoring, healthcare, smart homes, and smart manufacturing[(1)].A user, gateway, and sensor node are the primary components of a WSN. Numerous industries rely on the information gathered by sensor nodes. The

proposed Hybrid Key Management Scheme for Wireless Sensor Networks (WSNs) is a promising approach to provide security in WSNs. One of the main drawbacks is that the proposed scheme requires the use of Elliptic Curve Cryptography (ECC), which is computationally intensive and requires more resources than traditional cryptographic algorithms.[2] Due to the computationally intensive nature of security measures, most WSN applications may ignore them altogether. To enhance the safe routing procedure in WSNs, the suggested Deep RPL-Software Defined Network (DRPL_SDN)[3] has great promise. One major issue is that, in contrast to more conventional routing algorithms, the suggested strategy makes use of deep reinforcement learning, which can be resource and computationally demanding. An authentication protocol[4] is a standard security approach that creates a session key for communication partners to guarantee safe data transfer. It might be difficult to devise a workable authentication technique for WSNs due to their restricted resources. While systems based on hash functions are very efficient, ensuring the safety of the session key is difficult. The motivation of the proposed work is to address the challenges in wireless sensor networks (WSNs) related to energy efficiency, secure data transmission, and network lifetime.

Several WSN authentication methods[5,6] including those based on public key cryptosystems and hash functions, include security weaknesses including replay and forgery attacks and don't guarantee user anonymity. As a result, it becomes difficult to design an economical security protocol for WSNs that relies on authentication. An effective and safe dynamic authentication technique for WSNs is advocated for in this research. Specifically, we combine the dynamic salt method with a hash-based password strategy. Many studies[7],[8]have investigated the privacy of WSNs by using a variety of security measures. However, scaling remains a key challenge because sensors' lifespans are highly dependent on their power supply. This is because it is challenging to fulfill the resource requirements of high-security standard encryption technologies. The study[9] proposes a Hybrid Key Management Scheme for WSNs linking edge devices which use Elliptic Curve Cryptography (ECC) and a hash function to generate key pre-distribution keys. However, combining ECC with a hash function for key pre-distribution might be susceptible to collusion attacks. In[10] the research study provides an extensive analysis of how the characteristics of different trust management, authentication, and key management techniques may be effectively utilised in certain applications.

The two primary goals of key management for a secure network are authentication and secrecy. Mesmoudi[11] describe a dynamic and smart method for managing keys in hierarchical WSNs. It has three different strategies for handling key generation, key updating, and node addition, all of which aim to minimize resource consumption, network traffic, and data storage needs without sacrificing security. According to the proposed SKWN scheme, vulnerabilities may be introduced if the security level is changed based on ML predictions. Fuzzy logic is used for path key generation and node insertion in the intelligent, dynamic key management system for WSN proposed by Yousef[12]. While the proposed system aims to reduce energy consumption, the introduction of fuzzy logic and dynamic key management may add computational overhead.[13]Discusses the various Security Schemes for Data Exchange in Wireless Sensor Network.

Uras[14] offer a blockchain-based multi-WSN authentication method. This mixed-model approach allows for mutual authentication of node identities over a wide range of network topologies and transport protocols. The high volume of sensed and transferred data among nodes can lead to increased vulnerability, and the method of using reserved bits in the Zigbee MAC header to choose between insecure or secure modes may not provide a robust and comprehensive security solution. While the proposed three-party password authenticated key exchange (3-PAKE)[15] protocols are efficient and designed to address security concerns in ad hoc sensor network applications. The proposed method lacks secure data transmission and does not focus on energy consumption. The proposed cryptographic based clustering structure for preserving data privacy using Optimal Privacy-Multihop Dynamic Clustering Routing Protocol (OP-MDCRP)[16] is a promising approach to improve data privacy and energy efficient routing for the heterogeneous network which uses both clustering and multi-hop communication to reduce the energy consumption of sensor node and increases the lifetime of WSN. The use of cryptographic techniques can lead to increased computational complexity and overhead. The approach[17] focuses on optimizing two primary factors: residual energy and distance to the sink node. While these are crucial, ignoring other relevant factors like node density, cluster size, and link quality might limit the overall effectiveness in balancing energy consumption. Mehra[18] developed a fuzzy logic-based CH selection method to evaluate cost, residual energy, node density, and distance to the sink during the secure transmission of data. The use of fuzzy logic in the proposed fuzzy-based balanced cost CH selection algorithm (FBECS) may lead to increased computational complexity and overhead.

Ali[19]similarly optimized energy consumption and network lifetime by creating a cluster head selection approach and a ranked-based Clustering heuristic. However, this work does not focus on secure data transmission WSN. Using the seagull K-medoid clustering method and Rider Bald Eagle, Meena[20] proposed a method for energy-efficient routing with dynamic key authentication in IoT-based WSNs. Combining two optimization algorithms (SKC and RBES) for clustering and CH selection could introduce computational overhead for resource-constrained sensor nodes. As an addition, Kumar[21] introduced a scalable and space-saving key management (SSEKMS) technique for WSNs by establishing three distinct varieties of network keys. However, the proposed SSEKMS specifically benefits secure cluster formation in terms of efficiency or resilience. In

order to increase WSNs' chances of survival, Mansour [22] suggested an Energy-Aware Fault Tolerant Clustering with a Routing strategy that chooses Cluster Heads and best pathways to the target using a fault-tolerant mechanism. Employing two swarm intelligence algorithms (MFO and SSO) simultaneously might add complexity and increase computational overhead for resource-constrained sensor nodes. In addition, this approach focuses on survivability but doesn't mention performance in terms of other important metrics like packet delivery ratio, latency, or energy consumption Khashan [23] describe a lightweight, automated cryptographic technique for WSNs. By introducing dynamic clustering and variable encryption parameters adds complexity to the overall scheme. This might increase computational overhead and memory requirements for sensor nodes, potentially impacting resource-constrained devices Mezrag [24] provide a new identity-based authentication and key agreement strategy for clustered WSNs. However, Elliptic Curve Cryptography (ECC) introduces pairing-based cryptographic operations, which can be computationally expensive for resource-constrained sensor nodes.

2 Methodology

The methodology used in the proposed model involves a combination of safe authentication, data encryption, and dynamic routing to establish secure communication in wireless sensor networks. The authentication process utilizes a dynamic key approach and an improved salt password hashing method to ensure secure user identification and password protection. Data encryption is performed using Format Preserving Encryption (FPE) algorithm, which transforms plain text data into encrypted information using a random salt key. Dynamic routing is implemented using a cluster-based approach, where the network space is partitioned into quadrants and the best node in each quarter is appointed as the cluster head (CH). Figure 1 shows the proposed model workflow. Table 1 shows the notation and description.

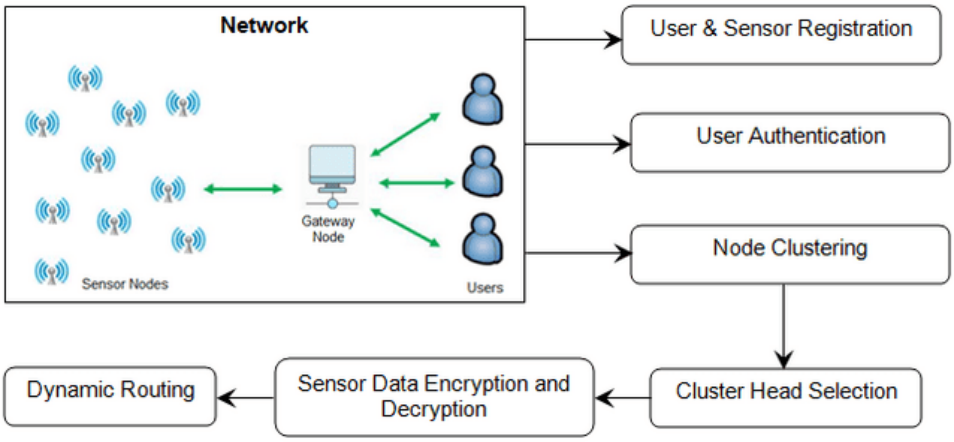

Fig 1. Proposed Work low

Table 1. Notation and Description

Entity	Notation	Meaning
User	U_i	i^{th} User
	$U^{ID}{}_i$	User Identity
	$U^{PWD}{}_i$	User Password
	$U^{PIN}{}_i$	PIN for the user
	$U^{S}{}_i$	Salt value for the user
	$U^{PWDSH}{}_i$	Hashed salted password value for the user
	$U^{PINSH}{}_i$	Hashed salted PIN value for the user
	$U^{ECP}{}_i$	Encrypted password for the user
Sensor	SN_j	The j-th sensor node
	$S^{ID}{}_j$	The identity of the j-th sensor node
	$S^{S}{}_j$	Sensor salt value
	$S^{SH}{}_j$	Hash value of the sensor salt

Continued on next page

Table 1 continued

Operator	h(.)	Cryptographic hash function
	bin(.)	Conversion of string to binary
	||	Concatenation of strings
	□	Exclusive OR (XOR) operation

2.1 Authentication and Data Routing Process in the Dynamic Key Approach for Wireless Sensor Networks

When a user interacts with a sensor network, GWN mediates the interaction. The Gateway Node is a specific piece of hardware that facilitates communication between the sensors and the user's computer devices. In order for users to access and manipulate the sensor data, the Gateway Node acts as a communication link between the sensor network and the user. The Gateway Node is an integral part of a sensor network design due to its ability to perform various crucial tasks. The user Ui must select a user id (UIDi), password (UPWDi), and PIN (UPINi) in order to register with the GateWay Node (GWN). Additionally, an 8-bit string consisting of both lowercase and uppercase letters is used to create a random salt value (USi). The authentication procedure is made more secure by using this salt value. Data from the sensor nodes is accessed, the user's credentials are validated, and a denial of service attack is prevented through the login process. The user generates authentication data and checks it against a database of known values. After a user has been authenticated, they are allowed to utilize the WSN service.

2.2 Methods of Encrypting and Decrypting Data

This section explains how to use a changing salt key to encrypt text in a way that is both lightweight and secure. The first stage in the encryption process is to transform the plain text (secret text) into a matrix. The matrix is encrypted with format-preserving encryption (FPE) once the produced salt key is appended to it. Decryption works in the opposite direction of encryption. The length of the secret message, given by msg = m1, m2, m3,... m16,> must be precisely 16 bits. Transform the encrypted message into a matrix,

$$sm1 = \begin{bmatrix} m_1 & m_2 & m_3 & m_4 \\ m_5 & m_6 & m_7 & m_8 \\ m_9 & m_{10} & m_{11} & m_{12} \\ m_{13} & m_{14} & m_{15} & m_{16} \end{bmatrix}$$

Create salt key with the length of 16-bit.

Let salt key = {k_1, k_2, k_3,…,k_{16}}. Append salt to sm,

$$sm2 = \begin{bmatrix} x_0 & k_1 & k_2 & k_3 & k_4 & x_0 \\ k_5 & m_1 & m_2 & m_3 & m_4 & k_6 \\ k_7 & m_5 & m_6 & m_7 & m_8 & k_8 \\ k_9 & m_9 & m_{10} & m_{11} & m_{12} & k_{10} \\ k_{11} & m_{13} & m_{14} & m_{15} & m_{16} & k_{12} \\ x_0 & k_{13} & k_{14} & k_{15} & k_{16} & x_0 \end{bmatrix}$$

Convert matrix sm2 into message sc = {X_0, k_1, k_2, k_3, k_4, X_0, k_5, m_1, m_2, m_3, m_4, k_6, k_7, m_5, m_6, m_7, m_8, k_8, k_9, m_9, m_{10}, m_{11}, m_{12}, k_{10}, k_{11}, m_{13}, m_{14}, m_{15}, m_{16}, k_{12}, X_0, k_{13}, k_{14}, k_{15}, k_{16}, X_0}.

The text is encrypted using format-preserving encryption after a binary string is produced from sc.

2.3 Cluster-based dynamic routing

In this section, a secure dynamic routing technique for cluster based WSNs is presented. First, the nodes are grouped together geographically, and then cluster leaders are chosen taking into account both their energy and their proximity to one another. Sensitive information is transmitted from the sensor node to the base station through a way that is dynamically determined to be the most secure. The network topology is partitioned into quadrants, and a cluster head node is chosen according to its position, proximity to other nodes, and available power. The CH's packet delivery ratio is used to update the cluster head.

Algorithm-1 Dynamic Key Approach-based Secure Authentication and Dynamic Secure Data Routing

Input: N, M (number of nodes and size of the network area), UIDi, UPWDi, UPINi, SIDj, PT (User ID, password, PIN number, sensor ID, and plain text), and h() (hash function)

Output: CHi (Cluster Head for each region), UIDi, USi, UECPi (user registration information), X3 (sensor registration information), ET (encrypted data), Dynamic routing, PT (decrypted data)

Step 1 : User Registration:

User selects User Identity UIDi, Password UPWDi, and Pin Number UPINi

Generate a random salt value (USi)

If UPINi is even, append USi with UPWDi in an even position and UPINi in an odd position. Else, append USi with UPWDi in an odd position and UPINi in an even position

Hash the resulting values to obtain UPWDSHi and UPINSHi

Compute V3 and V4 using UIDi, V1, and V2

Compute UECPi using UPWDSHi, UPINSHi, V3, and V4

Send UIDi, USi, and UECPi to GWN

If UIDi already exists in GWN, send a denial notification to Ui

Else, store Ui information [UIDi, USi, and UECPi]

Step 2 : Sensor Registration:

Sensor selects SIDj and generates a random salt value (SSi)

Compute SSHj = h(SSj)

Compute X1 using bin(SIDj) and SSHj

Send X1 and SSHj to GWN

GWN computes X2 = X1 ⊠ SSHj

Compute X3 using X2 and SSHj

Store X2 and X3 and send X3 to SNj

Step 3 : User Authentication:

The user provides their user identity (UIDi), password (UPWDi), and PIN number (UPINi) to the system.

The system generates a random salt value (USi) and computes V1 and V2 based on the PIN number.

The system computes the secure hashed passwords (UPWDSHi and UPINSHi) based on V1 and V2.

The system computes V3 and V4 based on the user identity and V1 and V2.

The system combines the hashed passwords and V3 and V4 to create a new encrypted user credential (newUECPi) and sends it to the gateway node (GWN).

The GWN retrieves the user's encrypted password (UECPi) and compares it to the new encrypted user credential (newUECPi).

If they match, the user is granted access to the sensor network and its information. If they don't match, the user is denied access.

Step 4 : Node Clustering and Cluster Head Selection:

Deploy N number of nodes in M x M area

Create a base station (BS) in the center position of the network area

Split network area into four regions (R)

For each region i = 1 to |R|

Find the optimal node based on distance, number of neighbors, and energy and select it as the Cluster Head (CHi) for that region.

Return CHi for each region

Step 5 : Data Encryption:

Check if there is any sensed message (PT)

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

Generate random salt key (SK)

Add SK into MAT1 to create MAT2

Convert MAT2 into Message (SM)

Convert SM into binary format binSM

Use Format Preserving Encryption (FPE) to encrypt binSM into ET

Return ET as the encrypted data

Step 6 : Dynamic Routing:

BS generates the salt key (SK) and distributes it to each cluster head (CH).

If a node has any sensed encrypted data (ET), it transmits the ET to its respective CH.

The CH checks the BS communication range.

If the CH is nearest to the BS, it sends the ET to the BS.
If the CH is not nearest to the BS, it sends the ET to the nearest CH and continues until the ET reaches the BS.
Step 7 : Data Decryption:
Get encrypted data (ET)
Use Format Preserving Decryption (FPD) to decrypt ET into binary format binSM
Convert binSM into Message (SM)
Convert SM into matrix (MAT2)
Remove salt key (SK) from MAT2 to get MAT1
Convert MAT1 into plain text (PT) based on (1)
Return PT as the decrypted data

3 Results and Discussion

This section explains how the proposed method's performance may be assessed. The recommended dynamic authentication and secure data routing is implemented in Java (version 1.8), and tests are done on a Windows 10 64-bit computer with a 2.30 GHz Intel Pentium (R) CPU and 4.0 GB of Memory. Multiple measures, such as memory use, energy usage, end-to-end latency, packet delivery ratio, and execution time, were used to assess the efficacy of the suggested approach. The execution time for salt key creation is shown in Table 2 revealing that the suggested technique is more efficient than the MD5 and SHA algorithms. The execution time for salt generation is consistently 1 millisecond regardless of the salt size or hashing algorithm used. For both MD5 and SHA-1, the execution time increases slightly as the salt size increases. The execution time for MD5 ranges from 15 to 22 milliseconds, while for SHA-1 it ranges from 16 to 23 milliseconds. The highest execution time is observed for a salt size of 256 bits with SHA-1, which takes 23 milliseconds.

Table 2. Execution Time

Salt Size in bits	Execution Time (ms)		
	Salt Generation	MD5	SHA-1
8	1	15	16
16	1	16	16
32	1	18	21
64	1	16	18
128	1	21	21
256	4	22	23
512	8	20	20

AES algorithm is used to compare the proposed data encryption algorithm. Table 3 shows the execution time. In comparison to AES's 1066 ms encryption time, the suggested method takes 841 ms. The suggested method's decryption time is 37 ms, whereas AES's is 45 ms. Furthermore, Table 4 show memory consumption for encryption and decryption.

Table 3. Encryption and Decryption Time Comparison

Parameters	AES	Dynamic Key Approach-based Secure Authentication (Proposed)
Encryption Time (in ms)	1066	841
Decryption Time (in ms)	45	37

Table 4. Memory consumption

Parameters	AES	Dynamic Key Approach based Secure Authentication (Proposed)
Encryption (in bytes)	13178	8307
Decryption (in bytes)	14120	8996

With a total memory consumption of 8307 bytes for encryption and 8996 bytes for decryption, the suggested approach utilizes less memory than AES by 58.63% and 56.95%, respectively. Tables 5, 6 and 7 provide the energy consumption, average delay and packet delivery ration of the proposed method with other methods. In the context of cluster-based dynamic routing, 100–300 sensor nodes, each with an initial energy of 5J, are distributed at random over the network region.

Energy consumption refers to the amount of energy used or consumed by a system or device. The values in the Table 5 represent the energy consumption of each protocol for different numbers of nodes in the WSN. For example, when there are 100 nodes in the WSN, the SKWN[11] protocol consumes 2.3 Joules of energy, while the FBECS[18] protocol consumes 2.1 Joules and the CDR protocol consumes 1.5 Joules. As the number of nodes in the WSN increases, the energy consumption of all three protocols also increases. The proposed method aims to establish a safe environment for data transmission while minimizing energy consumption.

Table 6 is a data table that provides information about the average delay in milliseconds (ms). The delay refers to the time taken for a packet of data to travel from one node to another in the wireless sensor network. The average delay is calculated by taking the sum of all the delays and dividing it by the total number of packets transmitted. The delay is an important metric in evaluating the performance of the network as it affects the overall efficiency and reliability of data transmission. A high delay can result in data loss, packet drops, and increased power consumption, which can impact the network's performance and longevity. The average delay can be affected by various factors such as the distance between nodes, the number of nodes in the network, the routing protocol used, and the quality of the wireless channel. By analyzing the average delay, researchers can identify the bottlenecks in the network and optimize the routing protocol to reduce the delay and improve the network's performance. From the table it is observed that the proposed cluster head dynamic routing (CDR) out performs the other two approaches SKWN[11] and the FBECS[18] with respect to the number of nodes.

Table 7 depict a comparison of the proposed Cluster head Dynamic Routing (CDR) performance to that of the SKWN[11] and the FBECS[18]. Packet Delivery Ratio (PDR) is a measure of the percentage of packets that are successfully delivered to their intended destination in a network. In the context of this research, PDR is being used as a way to evaluate the effectiveness of the suggested method for secure authentication and dynamic secure data routing in wireless sensor networks. The PDR values can range from 0% (no packets successfully delivered) to 100% (all packets successfully delivered). A high PDR is desirable in a network, as it indicates that a high percentage of packets are being successfully delivered to their intended destination.

Table 5. Energy Consumption (in J)

No of Nodes	SKWN	FBECS	CDR
100	2.3	2.1	1.5
150	2.5	2.2	1.8
200	3	2.5	2.1
250	3.5	3	2.3
300	3.7	3.1	2.8

Table 6. Average Delay (in ms)

No of Nodes	SKWN	FBECS	CDR
100	55	30	25
150	59	38	28
200	62	42	37
250	70	50	40
300	75	58	42

Table 7. Packet Delivery Ratio (in %)

No of Nodes	SKWN	FBECS	CDR
100	63	85	90
150	60	80	89
200	55	78	85
250	43	70	81
300	40	62	79

The energy needed to transfer data from one node to another grows in proportion to the number of nodes involved. The proposed CDR, on the other hand, consumes less power than any of the other routing strategies. Packet transmission times are reduced while using the proposed strategy. However, this delay grows when more nodes are added because of the increased

data transfer and traffic they generate. As the number of nodes expands, the proportion of successfully delivered packets falls. The proposed CDR has a better packet delivery ratio than the state-of-the-art methods.

4 Conclusion

This study proposes a novel method for secure authentication and dynamic secure data routing in wireless sensor networks using a dynamic key approach. The use of a dynamic key for improved salt password hashing in the authentication process is a unique aspect of the proposed method. The proposed method combines secure authentication, data encryption, and dynamic routing, addressing the security risks associated with carrying sensitive data in wireless sensor networks. The study also highlights the use of cluster-based routing to enhance network efficiency in terms of both power consumption and security. Further research or real-world implementation may be required to identify any weaknesses or challenges.

References

1) Lanzolla A, Spadavecchia M. Wireless Sensor Networks for Environmental Monitoring. *Sensors*. 2021;21(4):1–3. Available from: https://doi.org/10.3390/s21041172.
2) Yu S, Park Y. SLUA-WSN: Secure and Lightweight Three-Factor-Based User Authentication Protocol for Wireless Sensor Networks. *Sensors*. 2020;20(15):1–26. Available from: https://doi.org/10.3390/s20154143.
3) Qamar S. Optimal sensor network routing with secure network monitoring using deep learning architectures. *Neural Computing and Applications*. 2023;35(26):19039–19050. Available from: https://doi.org/10.1007/s00521-023-08753-0.
4) Moghadam MF, Nikooghadam M, Jabban MABA, Alishahi M, Mortazavi L, Mohajerzadeh A. An Efficient Authentication and Key Agreement Scheme Based on ECDH for Wireless Sensor Network. *IEEE Access*. 2020;8:73182–73192. Available from: https://doi.org/10.1109/ACCESS.2020.2987764.
5) Wu F, Li X, Xu L, Vijayakumar P, Kumar N. A Novel Three-Factor Authentication Protocol for Wireless Sensor Networks With IoT Notion. *IEEE Systems Journal*. 2021;15(1):1120–1129. Available from: https://doi.org/10.1109/JSYST.2020.2981049.
6) Lee J, Yu S, Kim M, Park Y, Das AK. On the Design of Secure and Efficient Three-Factor Authentication Protocol Using Honey List for Wireless Sensor Networks. *IEEE Access*. 2020;8:107046–107062. Available from: https://doi.org/10.1109/ACCESS.2020.3000790.
7) Babaeer HA, Al-Ahmadi SA. Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking. *IEEE Access*. 2020;8:92098–92109. Available from: https://doi.org/10.1109/ACCESS.2020.2994587.
8) Liu L, Chen W, Li T, Liu Y. Pseudo-Random Encryption for Security Data Transmission in Wireless Sensor Networks. *Sensors*. 2019;19(11):1–16. Available from: https://doi.org/10.3390/s19112452.
9) Sharmila, Kumar P, Bhushan S, Kumar M, Alazab M. Secure Key Management and Mutual Authentication Protocol for Wireless Sensor Network by Linking Edge Devices using Hybrid Approach. *Wireless Personal Communications*. 2023;130(4):2935–2957. Available from: https://doi.org/10.1007/s11277-023-10410-7.
10) Gautam AK, Kumar R. A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. *SN Applied Sciences*. 2021;3(1):1–27. Available from: https://doi.org/10.1007/s42452-020-04089-9.
11) Mesmoudi S, Benadda B, Mesmoudi A. SKWN: Smart and dynamic key management scheme for wireless sensor networks. *International Journal of Communication Systems*. 2019;32(7). Available from: https://doi.org/10.1002/dac.3930.
12) Yousefpoor MS, Barati H. DSKMS: a dynamic smart key management system based on fuzzy logic in wireless sensor networks. *Wireless Networks*. 2020;26(4):2515–2535. Available from: https://doi.org/10.1007/s11276-019-01980-1.
13) Ali S, Ashraf H, Ullah A, Jhanjhi NZ. Systematic Literature Review of Security Schemes for Data Exchange in Wireless Sensor Network. Institute of Electrical and Electronics Engineers (IEEE). 2024. Available from: https://d197for5662m48.cloudfront.net/documents/publicationstatus/183060/preprint_pdf/c3085aa8e0615eac2fe13645a77df19b.pdf.
14) Panahi U, Bayılmış C. Enabling secure data transmission for wireless sensor networks based IoT applications. *Ain Shams Engineering Journal*. 2023;14(2):1–11. Available from: https://doi.org/10.1016/j.asej.2022.101866.
15) Santos-González I, Rivero-García A, Burmester M, Munilla J, Caballero-Gil P. Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks. *Information Systems*. 2020;88:101423. Available from: https://doi.org/10.1016/j.is.2019.101423.
16) Loretta GI, Kavitha V. Privacy preserving using multi-hop dynamic clustering routing protocol and elliptic curve cryptosystem for WSN in IoT environment. *Peer-to-Peer Networking and Applications* . 2021;14:821–836. Available from: https://doi.org/10.1007/s12083-020-01038-6.
17) Xiuwu Y, Ying L, Yong L, Hao Y. WSN Clustering Routing Algorithm Based on Hybrid Genetic Tabu Search. *Wireless Personal Communications*. 2022;124(4):3485–3506. Available from: https://doi.org/10.1007/s11277-022-09522-3.
18) Mehra PS, Doja MN, Alam B. Fuzzy based enhanced cluster head selection (FBECS) for WSN. *Journal of King Saud University - Science*. 2020;32(1):390–401. Available from: https://doi.org/10.1016/j.jksus.2018.04.031.
19) Ali H, Tariq UU, Hussain M, Lu L, Panneerselvam J, Zhai X. ARSH-FATI: A Novel Metaheuristic for Cluster Head Selection in Wireless Sensor Networks. *IEEE Systems Journal*. 2021;15(2):2386–2397. Available from: https://doi.org/10.1109/JSYST.2020.2986811.
20) Meena U, Sharma P. Secret Dynamic Key Authentication and Decision Trust Secure Routing Framework for Internet of Things Based WSN. *Wireless Personal Communications*. 2022;125(2):1753–1781. Available from: https://doi.org/10.1007/s11277-022-09632-y.
21) Kumar V, Malik N, Dhiman G, Lohani TK. Scalable and Storage Efficient Dynamic Key Management Scheme for Wireless Sensor Network. *Wireless Communications and Mobile Computing*. 2021;2021:1–11. Available from: https://doi.org/10.1155/2021/5512879.
22) Mansour RF, Alsuhibany SA, Abdel-Khalek S, Alharbi R, Vaiyapuri T, Obaid AJ, et al. Energy aware fault tolerant clustering with routing protocol for improved survivability in wireless sensor networks. *Computer Networks*. 2022;212:109049. Available from: https://doi.org/10.1016/j.comnet.2022.109049.
23) Khashan OA, Ahmad R, Khafajah NM. An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. *Ad Hoc Networks*. 2021;115:102448. Available from: https://doi.org/10.1016/j.adhoc.2021.102448.
24) Mezrag F, Bitam S, Mellouk A. An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor networks. *Journal of Network and Computer Applications*. 2022;200:103282. Available from: https://doi.org/10.1016/j.jnca.2021.103282.