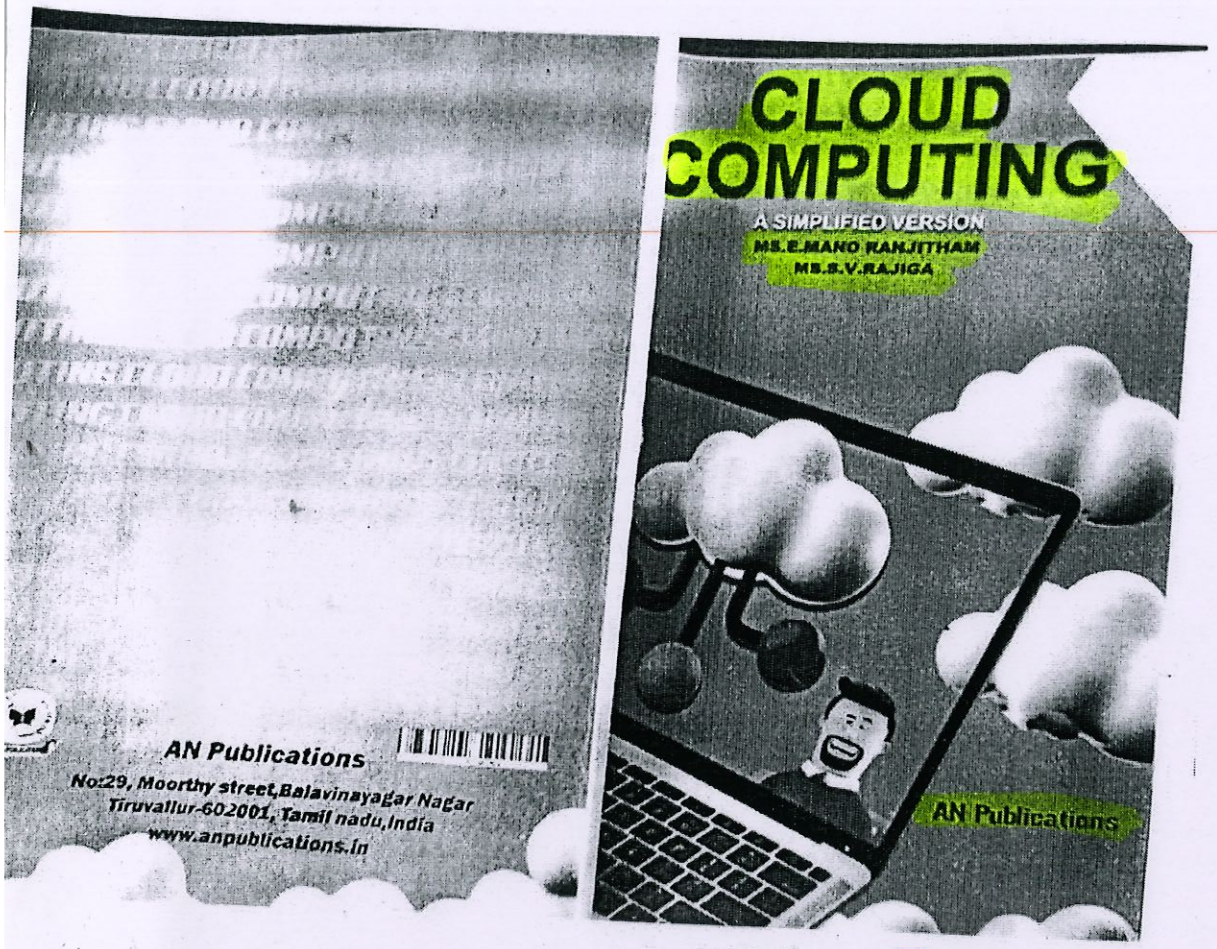
Books and Chapters 2022

S.No	Name/title of Paper	Name of the author
1.	Book - Cloud Computing	E.Mano Ranjitham
2.	Book Advancing Social work	Dr.Mary Angeline Santhosam
3.	Comprehensive analysis of energy efficient secure routing protocol over	Dr.Thyagaraj M



Title: Cloud Computing
ISBN: 978-81-960885-6-9
Authors: E.Mano Ranjitham, S.V. Rajga

AN Publications
No:29, Moorthy street, Balavinayagar Nagar,
Tiruvallur-602001,Tamilnadu, India.

ABOUT THE AUTHORS

Mrs.E.Mano Ranjitham is currently working as Vice Principal and Head department of Computer Science at Nazareth College of Arts and Science, Avadi, Chennai. She has got 15+ years of teaching and 6+ years of research experience.

She is an effective classroom practitioner with the required behavioral management skills and personal commitment needed to ensure that all students succeed and fulfill their academic potential. She is very passionate about making a real difference to young people lives through teaching. She has high-level skills and genuinely strives to satisfy each and every pupil unique learning requirement. Furthermore, she is having vast experience of working in academic settings.

She Coordinated National and International level Seminars, workshops and events. she acted as resource person for personality development classes for YWCA. She also contributed as external audit member for different colleges.

Her interested research areas are E-Learning, Cyber Security, E-waste management, Image processing and Visualization of data. She published More than 10 papers both National and International level.

Mrs.S.V.Rajga is currently working as Assistant Professor in Computer Science Department at Nazareth College Of Arts and Science, Avadi, Chennai from January 2021. Previously, She has worked as Assistant Professor in the Department of Computer Applications at Margregorios College Of Arts and Science, Mugappair West, Chennai from January 2011 to May 2019 and also worked as Assistant Professor in the Department of Computer Applications at Sri Kanyaka Parameshwari College of Arts and Science For Women, Parrys, Chennai. She has got 10+ years of Teaching and 4 years of Research experience. She was awarded Certificate of Excellence and Certificate of Honour for producing Cent Percent result so many times and enabled students to secure University Ranks. She also received Inspiring Teacher Award from Gurukul Academy.

NAZARETH COLLEGE OF ARTS & SCIENCE
CHENNAI
600 062

Principal
Nazareth College of Arts & Science
Kovilpathagai Main Road, Kannadapalayam,
Vellanoor Post, Avadi, Chennai-600062.

Cloud Computing

E.Mano Ranjitham

S.V. Rajiga

AN Publications

No: 29,Moorthy Street,Balavinayagar nagar,
Tiruvallur-602001,
Tamilnadu,India

Mary Angeline Santhosam is an accomplished academic administrator, social worker, sustainable educator, and social entrepreneur with over two decades of experience in the education sector. Currently serving as the Principal of Nazareth College of Arts & Science, she has held various significant positions. As a former Senate Member at the University of Madras, she drove educational reform, global collaborations, and community outreach at her present institution Nazareth College of Arts and Science. She is known for her pioneering teaching methodologies, with a prolific publication record, extensive research, and a deep commitment to social initiatives. Her international experience includes participation in conferences at Mauritius, Singapore, Germany, Malaysia and establishing collaboration by signing MoUs with universities from Malaysia, Thailand, Indonesia, Germany, Philippines, and Bangladesh. Dr. Mary Angeline shapes education and empowers communities through her multifaceted contributions.

Dr. Rambabu Botcha is an Assistant Professor in the Department of Social Work at RGNIYD, Sriperumbudur, under the Ministry of Youth Affairs and Sports, Government of India. He earned his Integrated M.Phil/Ph.D. from IGNOU, New Delhi, and is recognized for his contributions to improving the quality of life for individuals affected by HIV/AIDS, receiving the Young Achievement Award in Social Work. At RGNIYD, he has coordinated four national seminars/conferences, one international workshop, and several training programs on Youth Development nationwide. Dr. Botcha has made official visits to Thailand, China, and Sri Lanka, two of which were nominated by the Government of India. He has served as Placement Officer for over four years and NSS Officer for over six years at RGNIYD. He also completed a research project titled "Issues and Concerns of Youth at Risk in the metropolitan City of Chennai," funded by RGNIYD.

NATIONAL ACADEMIC PRESS
NAPI93

ISBN : 978-81-19671-14-4

Advancing Social Work : Evidence-Based Methods and Core Values

Edited By : Mary, Rambabu

ADVANCING SOCIAL WORK

EVIDENCE-BASED METHODS AND CORE VALUES

Edited By :

Dr Mary Angeline, Dr Rambabu Botcha

ADVANCING SOCIAL WORK :

EVIDENCE-BASED METHODS AND CORE VALUES

Edited by

Dr. MARY ANGELINE

Dr. RAMBABU BOTCHA

NATIONAL ACADEMIC PRESS

CHENNAI (INDIA)

Advancing Social Work:
Evidence-Based Methods and Core Values

by **Dr. Mary Angeline, Dr. Rambabu Botcha**

ISBN : 978-81-19671-14-4

Published in 2022 by

NATIONAL ACADEMIC PRESS

#25/57, Mohammed Hussain Street,
Royapettah, Chennai- 600 014.
Email : nationalacademicpress@gmail.com
Ph : 044-48677341, Mobile : 087544 32818

Printed and bound in India

TABLE OF CONTENTS

Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

Journal homepage: www.elsevier.com/locate/matpr

Comprehensive analysis of energy efficient secure routing protocol over sensor network

Mohit Chandra Saxena [a], Firdouse Banu [b], Anurag Shrivastava [c,*], M. Thyagaraj [d], Shrikant Upadhyay [e]

[a] SCSE, Galgotias University, Greater Noida, India
[b] Department of Applied Information System, Applied College, King Khalid University, Mahala, Saudi Arabia
[c] Sushila Devi Bansal College of Engineering, Indore, India
[d] Department of Computer Applications, Nazareth College of Arts and Science, Avadi, Chennai, India
[e] Department of ECE, Cambridge Institute of Technology, Ranchi, Jharkhand, India

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Anonymity
Wireless network
Sensor network
Man in middle attack
Dos attack
DDOS attack

ABSTRACT

To make hierarchical wireless sensor network transmission more secure, node life longer, and network operation efficiency higher, a WSN shared vital management scheme based on LEACH protocol is proposed. The program has good integrity and timeliness, dynamic critical security, node security independence, and critical survival effectiveness. It also can resist risks such as man-in-the-middle attacks and DDoS attacks, and it is expensive to distribute shared keys. The energy is lower, and the network operation efficiency is higher.

Selection and peer-review under responsibility of the scientific committee of the International Conference on Innovative Technology for Sustainable Development.

1. Introduction

With the rapid increase in the application demand of the Internet of things (IOT), wireless sensor networks (WSN, wireless sensor networks) have also been developed rapidly. They are widely used in environmental monitoring, forest fire prevention, homeland security, military, Aviation control, smart home and many other fields [1]. The wireless sensor network is different from other networks, It comprises many low-cost data processing and transmission, specific storage and computing capabilities, and wireless sensor intelligent nodes that communicate in ad hoc mode. These nodes are employed as sensing devices in the Internet of Things' sensing layer, which is comprised of a network of sensors. As a result, they are frequently stationed in hostile areas where they are left unattended and vulnerable to attack and destruction. As a result, the security challenges associated with wireless sensor networks are of critical relevance. Because wireless sensors have features such as limited computational power, limited storage capacity, and limited energy, as well as the ability to fail easily, the security of wireless sensor networks differs from the security of traditional networks. The physical safety of the network nodes themselves, as well as the security of communication between nodes, are critical components of the protection provided by wireless sensor networks. The security of communication is embodied in the protection of the secure communication mechanism as well as the safety of the keys used in communication. The solution to the important management problem of the network, after the communication method has been defined, may be recognised to be the key to overcoming the problem of network transmission security [2–5]. As a result, it is critical to investigate the fundamental management difficulties that arise in wireless sensor networks.

2. Routing protocol over sensor network

Wireless sensor networks differ from wired networks in that their nodes are spread and their energy, processing power, and storage capacity are typically constrained, whereas traditional networks have no such constraints. A consequence of this is that the routing scenario must be modified as a result of changes in node conditions. The routing protocol establishes the network structure, and the routing mechanism governs how data is transmitted between nodes in a wireless sensor network. A large number of routing protocols have been researched in light of the characteristics of diverse applications. Routing protocols are classified into five types: flooding routing protocols, hierarchical routing protocols, data-centric routing protocols, location-based routing protocols, and QoS-based routing protocols [6]. The standard protocols

* Corresponding author.
E-mail address: anurag.sh1768@gmail.com (A. Shrivastava).

https://doi.org/10.1016/j.matpr.2022.04.857
2214-7853/
Selection and peer-review under responsibility of the scientific committee of the International Conference on Innovative Technology for Sustainable Development.

that are utilised in various wireless sensor network routing protocols are listed in Table 1.

Table 2 shows the life cycle, scalability, path selection (single-hop or multi-hop), energy perception, data aggregation, location information (if the node's geographic location information is required), information storage, mobile nodes, real-time, and reliability. The comparison results of the performance and characteristics of wireless sensor network routing protocols [7–9] are based on performance (fault tolerance) and other elements.

Table 2 shows that the performance of key indicators of different routing protocols varies, and each has its own set of benefits and drawbacks. A single routing protocol cannot suit the needs of many applications because the design of the wireless sensor network routing protocol is intimately tied to the application [10–12]. In practical applications, the best routing protocol to use depends on the individual application and the characteristics of each routing protocol, as well as the accompanying security protocol, to ensure secure and reliable data transmission between each sensor node and sink node [13–15]. This paper proposes a WSN shared key based on the LEACH (low-energy adaptive clustering hierarchy) protocol Management plan to provide data information in hierarchical wireless sensor networks and improve data transmission security in a manner suitable for the characteristics of wireless sensor network nodes. Researchers are proposing various protocols [16–20] for providing data integrity, Confidentiality on the information shared among many users and servers in wireless network communication.

3. LEACH protocol

In wireless sensor networks, the LEACH protocol is a hierarchical routing mechanism. It is a cluster hierarchical protocol that consumes very little power. Each sensor node sends data to a randomly chosen cluster head node according to the protocol, which separates the sensor nodes into clusters. Sending data to the sink node is done by the cluster head node, which conducts data fusion processing. Wireless router networks may be extended 15 percent longer using the LEACH routing protocol than with other multi-hop routing protocols and static clustering methods since the energy consumption of network nodes is balanced.

When the energy levels of wireless sensor nodes fluctuate, LEACH performs a cluster rebuilding procedure in a predetermined cycle. There are two rounds to a cluster reconstruction process known as around, and each round is broken down into the cluster formation and transmission stages.

Node selection, node broadcasting, node establishment, and the construction of a cluster-scheduling system may all be considered steps in the setup process. The total number of cluster head nodes needed in the network and the number of times each node has been a cluster head node so far should guide the selection of cluster head nodes. Using a random number generator, each sensor node picks a value from 0 to 1. This node becomes the cluster head node if the selected value falls below a certain threshold. The cluster head node broadcasts the selection of the cluster head node to the whole network. Using the signal intensity of the received information, other network nodes select which cluster they should join and notify the head node of the appropriate cluster to finish the group formation. A last step involves using TDMA on the cluster head node to determine when data should be sent across clusters. As illustrated in Fig. 1, the LEACH routing protocol establishes a hierarchical wireless sensor network.

After the cluster has been created, it moves onto the phase of steady data transmission. At the heart of every network is a cluster head node, which receives the data collected and transmitted by each member node and performs the necessary data fusion; each cluster head node communicates with one another using the CSMA protocol in order to compete for a channel, with the data being sent to the sink node if it is able to obtain the channel (Sink).

Until the cluster is complete, the network cycles back to the cluster creation stage and repeats the cluster head selection cycle. [21–23] Each cluster communicates using a unique CDMA code, preventing other groups' nodes from interfering with the cluster's transmission. The stable phase lasts longer than the setup phase to save resources and time. During its operation, the LEACH protocol must address three critical areas: The hierarchical routing system must be built periodically, and each cycle's function may vary. During the node establishment procedure, the cluster head node will broadcast that it has been selected as a member. When the cluster head node is selected, the sink node will listen for this broadcast. They will choose which cluster to join based on the strength of the broadcast signal received, and they will communicate with that cluster. The head node informs the remainder of the cluster that it has joined. As stated previously, the basic criteria given above are required for implementing the WSN shared vital management scheme based on the LEACH protocol. They are also used to assess the system's overall success.

The cluster enters the steady data transmission phase after formation. Each cluster head node talks with and competes for the channel via the CSMA protocol, and the cluster head node that receives the channel distributes the data to the sink node (Sink). After a while, the network returns to the cluster building stage, where a new cycle of cluster head selection begins. Each cluster uses its own CDMA code [24] to avoid interfering with the transmission of other clusters. To save resources, the stable phase lasts longer than the setup phase. The LEACH procedure has three important points:

a. The hierarchical routing system should be rebuilt on a regular basis, with each node performing a distinct function in each cycle.
b. As soon as the cluster head node is selected during the node establishment process, the cluster head node broadcasts the fact that it has been selected as the cluster head node, and the sink node waits for this broadcast. c.
c. The member nodes of the cluster will pick which cluster to join depending on the strength of the received broadcast signal and will submit their findings to that particular cluster. The head node of the cluster tells the rest of the cluster that it has joined the group. The above-mentioned critical features are also the fundamental process of the system's functioning, and they help to generate the conditions necessary for implementing the WSN shared vital management scheme based on the LEACH protocol and its associated protocols.

Table 1
Common routing protocol for wireless sensor networks.

Agreement type	Agreement name
Hierarchical routing protocol	LEACH TEEN PEGASIS
Data-centric routing protocol	SPIN DD (directed diffusion) Rumor
Flooding routing protocol	Flooding, Gossiping
Routing protocol based on location information	GPSR GEAR
QoS-based routing protocol	SAR SPEED

Table 2
Comparison of performance and characteristics of wireless sensor routing protocols.

Protocol	Life Cycle	Scalability	Energy Perception	Data Aggregation	Movable Node	Real-Time	Reliability
Flooding	Short	Poor	None	None	Sensor node Sink node	Difference	better
Gossiping	Longer	Poor	None	None	Sensor node Sink node	Difference	better
LEACH	Longer	Poor	have	have	None	Difference	better
TEEN	Long	good	have	have	good	Difference	Difference
PEGASIS	Long	good	have	have	good	Difference	Difference
SPIN	Long	good	have	have	Sensor node Sink node	Difference	Difference

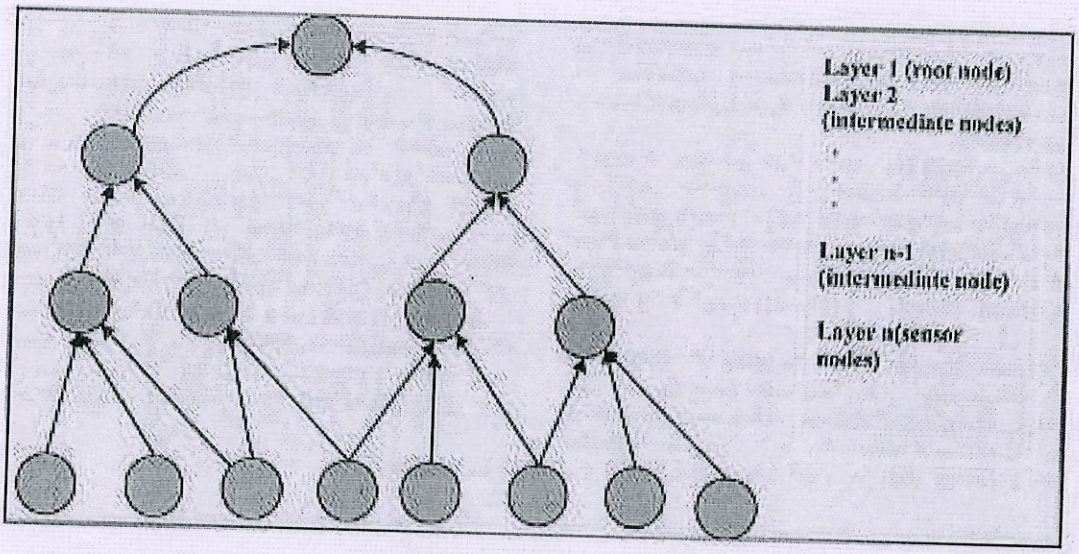


Fig 1. Hierarchical wireless sensor network.

4. Key management scheme

Given the soft computing and storage capabilities of wireless sensor nodes and limited energy, it is the apparent practical significance for nodes to provide security of data transmission between nodes through symmetric key algorithms. According to the working principle of LEACH protocol, while establishing a cluster, it can realize the distribution of shared keys between cluster member nodes and cluster head nodes and between cluster head nodes and sink nodes.

4.1. System model

Next, take the established hierarchical model consisting of a sink node Sink, a cluster head node C1 and its member nodes {N11, . . , N1i, . . , N1m} as an example to illustrate the LEACH-based WSN shared vital management scheme. The working principle of the model is shown in the left branch part of Fig. 1.

4.2. Description of model nodes

a. Each node is preset with the initial key mkey, which is well protected.
b. Each node has an ID number.
c. Each node can store data similar to the database table structure {recID, nodeID, key, isHeader}. Among them, recID represents the record number, and the record number increases from 1 to natural numbers as the number of records increases; nodeID represents the node number; key represents the shared key used to encrypt and decrypt data when transmitting data; header represents whether it is the node The corresponding node that communicates with the upper layer has a value of 0 or 1. 1 means yes, and 0 means no.
d. Each node has an encryption function F (Plaintext, key) and a decryption function F-1 (Ciphertext, key), which are respectively used to encrypt and decrypt the transmitted data. Plaintext represents a plain text string, Ciphertext represents a ciphertext string, and key represents a shared encryption and decryption key.
e. Each node has a data fusion function P (datas[ ]), which is used to fuse the data in the elements of the datas array.
f. Each node can perform XOR operation (operator is "⊕") and hash function operation (function Hash()).
g. Each node can generate a pseudo-random number $s \in S[0,1]$ RL, where RL is the length of the security key. s serves as the session key shared between the pair of nodes.
h. The implementation of the solution in this article does not change the original LEACH protocol process but only increases the content transmitted in the corresponding phase of the LEACH protocol.

5. Performance analysis of key management scheme

5.1. Security analysis of the scheme

a. Plan completeness: The solution is based on the LEACH wireless routing protocol and does not destroy the working mechanism of the original protocol; at the same time, the solution ensures that a new round of shared key regeneration and distribution is completed with each game of network structure re-establishment, achieving the LEACH protocol The operation and the distribution key of this program are correct.
b. Timeliness of the plan: The goal of the plan's implementation is to use an asymmetrical cryptosystem that saves energy, saves time, and occupies less operating space during the data transmission session between each pair of interactive nodes because the shared key is issued simultaneously hierarchical network structure is generated. Therefore, the timeliness of the scheme in the network constructed in each round is guaranteed.
c. Dynamic essential security: During the program's implementation, the content exchanged between nodes is encrypted when the key is released, and the keys are generated randomly, which significantly increases the difficulty of the adversary to obtain the key by analyzing the intercepted information and guarantees dynamic security of the key is improved.
d. Node security independence: After the hierarchical network structure is established, the session keys used by any two pairs of session nodes are different. Therefore, the loss of any session key will not affect the secure session between other nodes, ensuring the security independence of the nodes.
e. Key survival validity: Except for the initial key mkey of the wireless sensor node itself, all other keys are randomly generated during each cluster reconstruction round, any keys used in different games, sessions between different nodes, and various encryption and decryption processes. Therefore, they are not the same, and the lifetime of the same key does not exceed the lifetime of the hierarchical network structure, ensuring the validity of the key during the lifetime.
f. Resistance to attack: Because the session key of each pair of nodes is different, and they are all randomly generated. Therefore, it can resist attacks such as man-in-the-middle attacks and DDoS attacks. However, because the mkey and other keys exist in the wireless sensor node, the static security of the key has certain risks.

5.2. Scheme efficiency analysis

During the working period of the LEACH routing protocol, each wireless sensor node must send relevant information to ensure the establishment of a hierarchical network, and at the same time to ensure the implementation of the WSN shared vital management scheme based on the LEACH protocol. To make each key safely distributed to each related node, each node must pay the communication and calculation cost. The specific communication volume and calculation cost are shown in Tables 3 and 4, respectively. Among them, i represents the operation cost of the hash function, d represents the connection operation cost, q represents the exclusive OR operation cost, b represents the AND operation, and M represents the required length.

Table 3
Communication cost of each node in the scheme of this paper.

Node	Traffic
Cluster Member Node	4L
Cluster Head Node	4L
Convergence Node	4L

Table 4
Computational cost of each node of the scheme in this paper.

Node	Computing overhead
Cluster Member Node	6i + 6d + 6 s + 3b
Cluster Head Node	6i + 6d + 6 s + 3b
Convergence Node	3i + 3d + 4 s

The amount of communication generated by each node is the same, as seen in Table 3. Table 4 further shows that the calculation amount of each cluster head node is the same as the calculation amount of the cluster member nodes while transmitting data from the cluster member nodes to the sink node. The sink node's calculation amount is smaller, indicating that the energy spent by the cluster head node and cluster member nodes during the program's implementation is the same. Concatenation operations, exclusive-or operations, and activities, in addition to hash function operations, are processes that take up little time and space, showing that the scheme's implementation uses less energy.

In addition, each node must hold the connected node's number ID and key, with a maximum of 2 M bytes of data per related node. As a result, if a node (such as a cluster head node) contains n nodes that hold related news, the needed storage space is 2 nM.

6. Conclusion

With the increasing growth of Internet of Things applications, experts have turned their attention to studies on the security of wireless sensor networks. Wireless sensor network research is focused on extending the life of wireless sensors, increasing the efficiency of wireless sensor networks, and assuring network security. The adoption of the WSN shared vital management system based on the LEACH protocol has no effect on the original routing protocol's operation. The system has good scheme integrity, scheme timeliness, dynamic critical security, node security independence, and encryption at the same time. The vital survival effectiveness can withstand threats such as man-in-the-middle and DDoS attacks, while the energy consumption of distributing shared keys is minimal and network operation efficiency is good. This is extremely important for boosting wireless sensor network performance.

CRediT authorship contribution statement

Mohit Chandra Saxena: Data curation, Formal analysis, Conceptualization, Investigation, Methodology. **Firdouse Banu:** Data curation, Investigation, Methodology, Validation, Software, Software. **Anurag Shrivastava:** Data curation, Visualization, Investigation, Validation, Software, Software. **M. Thyagaraj:** Data curation, Visualization, Methodology, Validation, Software, Software. **Shrikant Upadhyay:** Visualization, Investigation, Methodology, Validation, Software, Software.

Declaration of Competing Interest

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

References

[1] J. Barad, H. Kathiwala, "DIST-LEACH: A deterministic key management scheme for securing cluster-based sensor networks," in: 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), 2014, pp. 1–5, doi: 10.1109/ICAETR.2014.7012949.

[2] D. Ramanand, D.S. Jayalakshmi, U. Ghosh, A. Balasundaram, P. Vijayakumar, P. K. Sharma, Enabling Sustainable Energy for Smart Environment Using 5G Wireless Communication and Internet of Things, IEEE Wirel. Commun. 28 (6) (2021) 50–61.

[3] A. Singh, S. Rathkanthiwar, S. Kakde, Energy efficient routing of WSN using particle swarm optimization and V-LEACH protocol, in: 2016 International Conference on Communication and Signal Processing (ICCSP), 2016, pp. 2078–2082, doi: 10.1109/ICCSP.2016.7754544.

[4] B. Seenalatha et al., FPGA Implementation of Protected Compact AES S-Box Using CQCC for Embedded Applications, in: Advances in Parallel Computing (Smart Intelligent Computing and Communication Technology), IOS Press, vol. 38, 2021, pp. 396–401.

[5] M. Kaddi, K. Benahmed, M. Omari, LEACH-KANGA: A new routing protocol for WSN based on leach protocol and Kangaroo method, in: 2017 International Conference on Mathematics and Information Technology (ICMIT), 2017, pp. 273–278, doi: 10.1109/MATHIT.2017.8259729.

[6] Wei Zhang, Liang Zhao, Analysis and research of improved LEACH routing protocol for pressure sensor based on WSN, in: International Conference on Cyberspace Technology (CCT 2014), 2014, pp. 1–6, doi: 10.1049/cp.2014.1133.

[7] A. Rajesh et al., A routing optimization algorithm via Fuzzy Logic towards security in wireless ad hoc networks, in: International Conference on Circuits, Power and Computing Technologies, IEEE Xplore, pp. 1321–1323, 2014.

[8] K. Singh, WSN LEACH based protocols: A structural analysis, in: 2015 International Conference and Workshop on Computing and Communication (IEMCON), 2015, pp. 1–7, doi: 10.1109/IEMCON.2015.7344478.

[9] T. Al-khdour, M. Baroudi, An Entropy-Based Throughput Metric for Fairly Evaluating WSN Routing Protocols, in: 2007 IEEE International Conference on Network Protocols, 2007, pp. 342–343, doi: 10.1109/ICNP.2007.4375872.

[10] M.B.M. Taj, M.A. Khir, ICH-LEACH: An enhanced LEACH protocol for wireless sensor network, in: 2016 International Conference on Advanced Communication Systems and Information Security (ACOSIS), 2016, pp. 1–5, doi: 10.1109/ACOSIS.2016.7843949.

[11] K. Kalpana et al., Design and Performance Analysis of Low Power High Speed Adder and Multiplier Using ATTCMOS in 90nm, 45nm and 18nm Regime, in: Advances in Parallel Computing (Smart Intelligent Computing and Communication Technology), IOS Press, vol.38, pp. 409–416, 2021.

[12] Mukesh Soni, Dileep Kumar Singh, Privacy Preserving Authentication and Key management protocol for health information System, in: Data Protection and Privacy in Healthcare: Research and Innovations, Page-37, CRC Publication, 2021

[13] D. Kothandaraman et al., Energy and Bandwidth Based Link Stability Routing Algorithm for IoT, Comput., Mater. Continua 70 (2) (2021) 3875–3890.

[14] M. Soni, YashKumar Bansal, S. Gomathi, A review on Privacy-Preserving Data Preprocessing, JCIM (2020) 16–30, https://doi.org/10.54216/JCIM.010202, JCIM.010202.

[15] M. Ganga et al., Survey of Texture Based Image Processing and Analysis with Differential Fractional Calculus Methods, in: International Conference on System, Computation, Automation and Networking, IEEE Xplore, pp. 1–6, 2021.

[16] M. Soni, D.K. Singh, Blockchain Implementation for Privacy preserving and securing the Healthcare data, in: 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), 2021, pp. 729–734, https://doi.org/10.1109/CSNT51715.2021.9509722.

[17] A. Shashank et al., Power Analysis of Household Appliances using IoT, in: International Conference on System, Computation, Automation and Networking, IEEE Xplore, pp. 1–5, 2021.

[18] S. Gomathi, M. Soni, G. Dhiman, B. Govindaraj, P. Kumar, A survey on applications and security issues of blockchain technology in business sectors, Mater. Today: Proc. (2021), https://doi.org/10.1016/j.matpr.2021.02.088.

[19] M. Soni, S. Gomathi, P. Kumar, P.P. Churi, M.A. Muhammed, A.O. Salman, Hybridizing Convolutional Neural Network for Classification of Lung Diseases, Int. J. Swarm Intell. Res. (IJSIR), 13(2) (2022) 1–15, https://doi.org/10.4018/IJSIR.287544.

[20] A. Shrivastava, A Study on the effects of forced air- cooling enhancements on a 150 W solar photovoltaic thermal collector for green cities, sustain. Energy Technol. Assess., 2022,Volume 49 Feb, number 101702.

[21] A. Shrivastava, G.S. Tomar, A.K. Singh, Performance comparison of AMBA bus-based system-on-chip communication protocol, in: Proceedings - 2011 International Conference on Communication Systems and Network Technologies, CSNT 2011, pp. 449–454, 5958687.

[22] A. Shrivastava, A. Rizwan, M.S. Kumar, B. Saravanakumar, I.S. Dhanoa, P. Bhambri, B.K. Singh, S.K. Sar, VLSI implementation of Green Computing Control Unit on Zynq FPGA for Green Communication, Wirel. Commun. Mobile Comput. 2021 (2021) 1–10.

[23] A. Shrivastava, S.K. Sharma, Various arbitration algorithm for on-chip(AMBA) shared bus multi-processor SoC, in: 2016 IEEE Students' Conference on Electrical, Electronics and Computer Science, SCEECS 2016, 508330.

[24] A. Shrivastava, S.K. Sharma, Efficient bus based router for NOC architecture, World J. Eng. 13 (4) (2016) 370–375.