Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 489–499
DOI : 10.47974/JDMSC-1904

EAKRR : An energy-efficient key management in WSN with ECC-based cryptography

Suresh Limkar *
Department of Artificial Intelligence & Data Science
AISSMS Institute of Information Technology
Pune
Maharashtra
India

Amrik Singh †
Department of Computer Science & Engineering
M.B.S. College of Engineering and Technology
Jammu
Jammu and Kashmir
India

Wankhede Vishal Ashok §
Department of Electronics & Telecommunication Engineering
SNJBs Shri. Hiralal Hastimal (Jain Brothers, Jalgaon), Polytechnic
Chandwad
Nashik
Maharashtra
India

Rajesh Phursule ‡
Department of Information Technology
Pimpri Chinchwad College of Engineering
Pune
Maharashtra
India

* *E-mail:* **sureshlimkar@gmail.com (Corresponding Author)**
† *E-mail:* **amrik.singh@mbscet.edu.in**
§ *E-mail:* **wankhedeva@gmail.com**
‡ *E-mail:* **rphursule@gmail.com**

Vinod Wadne [@]
Department of Computer Engineering
JSPM's Imperial College of Engineering and Research
Pune
Maharashtra
India

Raju M. Sairise [#]
Department of Electronics and Telecommunication
Yadavrao Tasgaonkar College of Engineering & Management
Bardi
Maharashtra
India

Abstract

Environmental monitoring, industrial automation, and other applications require Wireless Sensor Networks (WSN). WSN must efficiently manage cryptographic keys for safe communication and energy efficiency. This study introduces "Energy-Aware Key Revocation and Rekeying" (EAKRR) to address energy efficiency and security in WSN using Elliptic Curve Cryptography (ECC). Energy-efficient key management is needed in WSN which have sensor nodes with limited resources and energy. EAKRR is designed to adapt to sensor node energy levels to make crucial key revocation and rekeying decisions while maintaining strong and resilient security. Energy profiling is used by EAKRR to assess sensor node energy consumption during cryptographic and operational operations. Energy conservation is achieved by localized key revocation when a node's energy drops below a threshold. EAKRR also optimizes security and energy efficiency with ECC-based adaptive key length modifications. EAKRR is compared to LEACH and AES to determine its efficacy. The results show that EAKRR is highly energy efficient, extending the network's lifespan and maintaining security. Cryptographic operations are careful and wise because they can adjust to energy levels in real time. The balance between security and energy usage shows that ECC-based encryption works. Energy-efficient key management in WSN is crucial. EAKRR solves WSN problems by saving energy, extending network life, and securing the network.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Energy efficiency, WSN, Internet of Things, Elliptic curve cryptography, Energy-aware key.*

1. Introduction

WSN are essential to modern data collection and surveillance systems in environmental monitoring, healthcare, industrial automation, and the

[@] *E-mail:* **vinods1111@gmail.com**
[#] *E-mail:* **rsairise566@gmail.com**

Internet of Things. WSN have many small sensor nodes with limited processing, memory, and energy. These networks must reduce energy use and ensure data security due to resource constraints. Effective cryptographic key management is crucial WSN addressing these challenges. Data confidentiality, integrity and authenticity while optimizing sensor node resources are its main duties[1], [2].

WSN are complex systems with many small, distributed sensor nodes. These nodes identify, collect, and send data from remote or hostile environments to central processing units. Key management distributes, renews, and revokes cryptographic keys for secure sensor node communication. A good key management scheme helps sensor nodes use their limited resources to securely transmit data[3], [4].

Several strategic management methods have been developed to address WSN challenges. These methods use probabilistic key distribution, pre-distributed keys, and hierarchical key management with symmetric and asymmetric key management. By optimizing cryptographic key allocation and control, they aim to balance energy efficiency and security and increase network durability[5], [6].

Elliptic Curve Cryptography (ECC) is popular in WSN because it provides strong security with shorter key lengths, making it suitable for sensor nodes' limited resources. ECC is secure because elliptic curves over finite fields use fundamental operations like point addition and scalar multiplication.

Leach's Low-Energy Adaptive Clustering Hierarchy (LEACH) algorithm reduces energy consumption in wireless sensor networks. This process involves decentralized cluster creation and leader selection. The algorithm uses sensors finite energy to extend network operation.

A famous clustering-based protocol, LEACH, was created to address Wireless Sensor Networks' energy efficiency issues. This system focuses on forming groups led by a leader and efficiently transferring data within them. Probabilistic algorithms select cluster heads and enable energy-efficient data transmission in LEACH. AES a popular cryptographic algorithm, protects data in WSN. AES manipulates data blocks using a confidential key using complex mathematical operations like substitution, permutation, and mixing.

Despite various key management methods, WSN sensor nodes' limited energy and resource capabilities remain a challenge. These challenges require energy efficiency and data security. Developing a key management scheme that addresses these limitations and maximizes network efficiency is a priority.

Our Contribution

- Create "Energy-Aware Key Revocation and Rekeying (EAKRR)" to improve key management in Wireless Sensor Networks using ECC-based cryptography.
- Assess EAKRR's energy efficiency, network longevity, security, key distribution complexity, and real-time adaptability.

2. Literature Review

The domain of WSN has undergone substantial advancements in recent times, propelled by the increasing need for instantaneous data gathering and surveillance in diverse domains, spanning from environmental sensing to precision agriculture and the Internet of Things (IoT). Effective key management is essential for addressing these challenges, as it guarantees the confidentiality and integrity of data while maximizing the utilization of scarce resources.

The purpose of this literature review is to present a comprehensive summary of important research papers and studies that enhance our understanding of energy-efficient key management, secure data transmission, and routing protocols in WSN. Through the analysis of these works, we acquire valuable understanding of the current advancements in WSN and discern significant patterns and progressions in the field.

B. A. Bakr et al.[7] conduct a comparative analysis of the LEACH protocol and its improved version, LEACH-SM. The primary objective is to assess the amount of energy used and the duration of network operation, offering valuable information on energy-efficient clustering in WSN. Gupta et al.[8] propose the "Resource Discovery Algorithm with Binary Whale Optimization" (RDA-BWO) as a method to facilitate data transfer and predict the location of mobile sinks in heterogeneous WSN. R. Hajian et al.[9] presents CHESDA, a method for ongoing combination and energy-efficient protection of data in WSN. The focus is on secure methods of combining data to improve energy efficiency.

K. Haseeb et al.[10] introduce a WSN framework for smart agriculture applications in IoT that is both energy-efficient and secure. The framework is designed to meet the unique requirements of the agricultural domain. The study conducted by K. Haseeb et al.[11] centers on a routing protocol for WSN that prioritizes energy efficiency and security. It enhances routing techniques that guarantee both energy efficiency and data security. G. Mehmood et al.[12] present a highly effective and reliable method for

managing session keys in WSN with a particular focus on ensuring secure distribution and management of the keys.

B. Marques et al.[13] focuses on energy-efficient node selection in application-driven WSN. The research contributes to the development of techniques that aim to optimize energy consumption by considering the requirements of specific applications. The authors, V. Pandiyaraju et al. [14] propose an efficient energy utilization model for precision agriculture in WSN. The main focus is on utilizing multi-objective clustering techniques to improve energy efficiency. Pavan Kumar et al.[15] present a novel routing protocol called "Secure and Energy-Efficient Position-based Routing Protocol" (SPEED-UP) designed specifically for WSN. The main emphasis is on ensuring secure and energy-efficient routing within the framework of IoT.

Preeth et al.[16] introduce an adaptive fuzzy rule-based protocol that focuses on energy-efficient clustering and immune-inspired routing in WSN-assisted IoT systems. O. Rehman et al.[17] presents "Energy Consumption Rate-based Stable Election Protocol" (SPEED-UP) for WSN which emphasizes energy-efficient strategies for selecting nodes. S. Selvaraj et al.[18] present an "Energy-Efficient Dynamic Routing Mechanism" (EEDRM) designed for WSN. The focus of their research is on dynamic routing strategies, particularly when dealing with obstacles.

This literature review encompasses an analysis of a range of research papers that together provide a comprehensive perspective on the progress and obstacles in energy-efficient key management and secure data transmission in Wireless Sensor Networks. These papers discuss different strategies and methodologies, such as clustering-based protocols like LEACH, secure data aggregation, routing protocols, and session key management schemes. Researchers are consistently working to create new solutions that improve the energy efficiency and security of WSN, thus increasing the potential and range of these networks.

3. EAKRR: Energy-Aware Key Revocation and Rekeying

Within the domain of WSN where the most important considerations are energy efficiency and data security, the suggested key management scheme, Energy-Aware Key Revocation and Rekeying (EAKRR), stands out as an innovative solution. Given the limited resources available to sensor nodes, it is crucial to have a key management approach that is dynamic, adaptive, and energy-conscious.

EAKRR is a new framework designed to optimize the balance between energy consumption and cryptographic security in WSN. EAKRR aims to tackle the complex challenges presented by the limited resources of sensor nodes by implementing innovative strategies such as localized key revocation, adaptive key length adjustment, and real-time adaptability.

Essential elements of the EAKRR:

- Energy Profiling: Energy profiling is an essential process for comprehending the energy usage patterns of sensor nodes. This entails evaluating the energy consumption during regular operation and cryptographic procedures. The utilization of mathematical models and algorithms allows for the analysis of energy consumption patterns, offering valuable information about the main factors that influence energy efficiency in the network.
- Localized Key Revocation: The EAKRR system implements a localized method for revoking keys, which involves identifying and revoking compromised or redundant keys within specific clusters or nodes in a dynamic manner. To minimize network disruption and ensure continuous and efficient operation, the impact of key revocation is confined to specific regions.
- Adaptive Key Length Adjustment: The EAKRR system incorporates a mechanism for adjusting the key length in response to the dynamic nature of WSN. This feature adjusts the length of cryptographic keys in real-time according to the current energy level of each individual node. The implementation of adaptive key length adjustment not only improves security but also optimizes energy efficiency.

$$L = \{L_{healthy} \text{ if } E_{status} = healthy \; L_{low} \text{ if } E_{status} = low$$

where, L= "key length", E_{status} = "Energy status", healthy = "longer key is used", low = "shorter key is used to reduce computational overhead".

- Real-time Adaptability: EAKRR is specifically engineered to function in real-time, promptly adjusting to fluctuating network circumstances and promptly addressing emerging security risks. EAKRR achieves real-time adaptability by employing feedback mechanisms that constantly monitor energy levels, security parameters, and network dynamics. This enables prompt adaptation and optimization of key management strategies.

Algorithm: Energy-Aware Key Revocation and Rekeying

Algorithm 1: Energy-Aware Key Revocation and Rekeying

```
Initialize:
    Energy_Threshold = a predefined threshold value
    ECC_Key_Length_Healthy = preferred key length for healthy nodes
    ECC_Key_Length_Low = shorter key length for nodes with low energy
Main Loop:
    for each Sensor_Node in Network:
    Energy_Status ☮ Measure_Energy_Consumption(Sensor_Node)
    if Energy_Status < Energy_Threshold:
    Revocation_Decision ☮Assess_Revocation_Necessity(Sensor_Node)
    if Revocation_Decision is True:
    Neighboring_Nodes = Find_Neighbors(Sensor_Node)
    Revoke_Keys(Sensor_Node, Neighboring_Nodes)
    Update_ECC_Key_Length(Sensor_Node, ECC_Key_Length_Low)
    else:
    Update_ECC_Key_Length(Sensor_Node, ECC_Key_Length_Healthy)
    event_trigger = Check_Event_Trigger()
    if event_trigger:
    Rekeying(Sensor_Node)
    Scheduling(Sensor_Node)
```

4. Simulation Tool

In the Contiki-NG framework, Cooja is the best simulation tool for testing the EAKRR method. This help to deploy sensor nodes, evaluate

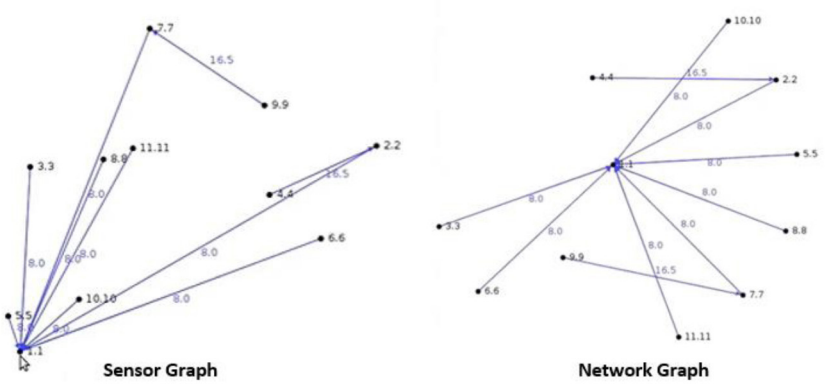

Figure 1

Cooja Simulation of Sensor graph and Network graph

energy usage and test key management protocols in Cooja flexible and authentic WSN. With its simple interface and seamless integration with Contiki-NG it the best choice for testing EAKRR efficacy and flexibility in WSN. Figure 1 Shows the Cooja simulation of Network Graph and sensor graph.

5. Results and Outputs

Evaluation Parameters

Parameter	EAKRR	Leach	AES
Energy Consumption (joule)	986	1240	1180
Key distribution Overhead	100	165	150
Key revocation Overhead	120	160	140
Communication Overhead	85	100	90
Throughput (Mbps)	3.5	4.2	2.8
Latency (ms)	10.2	15.5	12.1

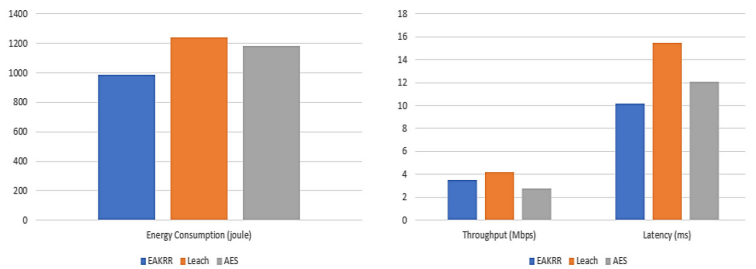

Figure 2

Energy consumption, Throughput and Latency comparison

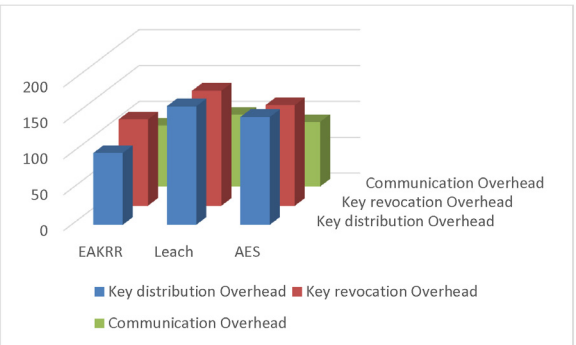

Figure 3

Overhead comparison

Among key management methods, EAKRR uses the least energy at 986 joules. This is better than LEACH and AES, which use 1240 and 1180 joules, respectively. EAKRR's minimal key distribution overhead is 100, better than LEACH's 165 and AES's 150. EAKRR key revocation overhead score beats LEACH and AES. With values of 85, 100, and 90, EAKRR has much lower communication overhead than LEACH and AES. EAKRR performance metrics show 3.5 Mbps throughput, slightly lower than LEACH=4.2 Mbps but higher than AES=2.8 Mbps. EAKRR has the lowest latency at 10.2 ms, beating LEACH (15.5 ms) and AES (12.1 ms). As a key management method, EAKRR is energy efficient, low overhead, and comparable to LEACH and AES in throughput and latency. Figure 2 and 3 shows the comparison results.

6. Conclusion and Future scope

As discussed in our previous conversations, Energy-Efficient Key Management in WSN with ECC-based Cryptography has revealed promising insights into improving WSN efficiency and security. EAKRR uses Elliptic Curve Cryptography to maximize energy efficiency, reduce overhead, and match LEACH and AES in throughput and latency. Localized key revocation, adaptive key length adjustment, and real-time adaptability help EAKRR solve resource-constrained sensor node problems. The comparison of energy consumption, key distribution overhead, key revocation overhead, and communication overhead shows EAKRR good performance. It leads in energy efficiency, reducing energy use and overhead while maintaining competitive communication. Several future research avenues are laid out by Energy-Efficient Key Management in WSN with ECC-based Cryptography. This may involve fine-tuning algorithms, exploring new cryptographic methods, and adapting the method to different network topologies. Key management methods in large WSN must also be scalable. Future research could assess EAKRR scalability and develop strategies to ensure its efficacy in large sensor networks.

References

[1] T. T. Chakavarika, S. K. Gupta, and B. K. Chaurasia, "Energy Efficient Key Distribution and Management Scheme in Wireless Sensor Networks," *Wirel. Pers. Commun.*, vol. 97, no. 1, pp. 1059–1070 (2017), doi: 10.1007/s11277-017-4551-2.

[2] A. B. Feroz Khan and G. Anandharaj, "A cognitive key management technique for energy efficiency and scalability in securing the sensor nodes in the IoT environment: CKMT," *SN Appl. Sci.*, vol. 1, no. 12, pp. 1–7 (2019), doi: 10.1007/s42452-019-1628-4.

[3] B. S. Kim and J. S. Song, "Pseudonymous mobile node reauthentication scheme for mobile wireless sensor networks," *ACM Int. Conf. Proceeding Ser.*, pp. 294–299 (2019), doi: 10.1145/3377170.3377207.

[4] L. Kaur and R. Kaur, "A survey on energy efficient routing techniques in WSNs focusing IoT applications and enhancing fog computing paradigm," *Glob. Transitions Proc.*, vol. 2, no. 2, pp. 520–529 (2021).

[5] M. Krishnapriya, G. Angeline Prasanna, and S. Anbarasu, "Rank-Based Energy-Efficient Key Management Routing For Wireless Sensor Network-Based Iot Medical Sensors," *Wirel. Pers. Commun.*, vol. 130, no. 3, pp. 2175–2196 (2023), doi: 10.1007/s11277-023-10377-5.

[6] Sharma, S.K., Kumar, A., Digital Image Transformation Using Outer Totality Cellular Automata. Machine Intelligence Techniques for Data Analysis and Signal Processing. Lecture Notes in Electrical Engineering, vol 997. Springer, Singapore (2023).

[7] Sharma, Sandeep Kumar, Kumar, Anil, Ashtagi, Rashmi & Jain, Rekha. OCA: An intelligent model for improving security breach of biometric based authentication systems, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:5, 1415–1425 (2023), DOI: 10.47974/JDMSC-1765.

[8] P. Gupta, S. Tripathi, and S. Singh, "RDA-BWO: hybrid energy efficient data transfer and mobile sink location prediction in heterogeneous WSN," *Wirel. Networks*, vol. 27, no. 7, pp. 4421–4440 (2021).

[9] R. Hajian and S. H. Erfani, CHESDA: continuous hybrid and energy-efficient secure data aggregation for WSN, vol. 77, no. 5. Springer US (2021).

[10] Anil Kumar & Sandeep Kumar Sharma. Information cryptography using cellular automata and digital image processing, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1105-1111 (2022).

[11] K. Haseeb, I. U. Din, A. Almogren, and N. Islam, "An energy efficient and secure IoT-based WSN framework: An application to smart agriculture," *Sensors (Switzerland)*, vol. 20, no. 7 (2020), doi: 10.3390/s20072081.

[12] G. Mehmood *et al.*, "An Efficient and Secure Session Key Management Scheme in Wireless Sensor Network," *Complexity*, vol. 2021 (2021), doi: 10.1155/2021/6577492.

[13] B. Marques and M. Ricardo, "Energy-efficient node selection in application-driven WSN," *Wirel. Networks*, vol. 23, no. 3, pp. 889–918 (2017), doi: 10.1007/s11276-016-1194-2.

[14] V. Pandiyaraju, S. Ganapathy, N. Mohith, and A. Kannan, "An Optimal Energy Utilization Model for Precision Agriculture in WSNs Using Multi-Objective Clustering," *J. King Saud Univ. - Comput. Inf. Sci.*, p. 101803 (2023), doi: 10.1016/j.jksuci.2023.101803.

[15] M. V. N. R. Pavan Kumar and R. Hariharan, "SPEED-UP, and energy-efficient GPSR protocol for WSNs using IOT," *Meas. Sensors*, vol. 23, no. July, p. 100411 (2022), doi: 10.1016/j.measen.2022.100411.

[16] S. K. S. L. Preeth, R. Dhanalakshmi, R. Kumar, and P. M. Shakeel, "An adaptive fuzzy rule based energy efficient clustering and immune-inspired routing protocol for WSN-assisted IoT system," *J. Ambient Intell. Humaniz. Comput.*, vol. 0, no. 0, p. 0 (2018).

[17] O. Rehman, N. Javaid, B. Manzoor, A. Hafeez, A. Iqbal, and M. Ishfaq, "Energy consumption rate based stable election protocol (ECRSEP) for WSNs," *Procedia Comput. Sci.*, vol. 19, pp. 932–937 (2013), doi: 10.1016/j.procs.2013.06.128.

[18] S. Selvaraj and S. Vasanthamani, "Energy Efficient Dynamic Routing Mechanism (EEDRM) with Obstacles in WSN," *Wirel. Pers. Commun.*, vol. 112, no. 4, pp. 2761–2776 (2020), doi: 10.1007/s11277-020-07174-9.