Fayoum University Faculty of Engineering, 2024, Vol: 7(1), 63-81
https://fuje.journals.ekb.eg/
ISSN Online: 2537-0634
ISSN Print: 2537-0626

A Novel Secured and Efficient Clustering Approach for Wireless Sensor Networks Using Cluster-Head Handover Mechanism

Mai S. Mousa[1,*], Ayman Al-Ahwal[2], Tamer M. Barakat[1]

[1] Electrical Engineering Department, Faculty of Engineering, Fayoum University, Egypt
[2] Communication and electronics Department, Pyramid-institute for Engineering and Technology, Egypt

* Corresponding Author: Mai S. Mousa (ms3574@fayoum.edu.eg)

How to cite this paper: Moussa, M.S., Al-Ahwal, A. & Barakat, T.M. (2024). A Novel Secured and Efficient Clustering Approach for Wireless Sensor Networks Using Cluster-Head Handover Mechanism, *Fayoum University Journal of Engineering*, *Vol: 7(1), 63-81*
https://dx.doi.org/10.21608/FUJE.2023.193797.1042

Abstract

Wireless sensor networks (WSNs) face significant challenges in terms of energy efficiency and security due to the limited energy capacity of sensor nodes and the sensitivity of the data they collect. This paper proposes an energy-efficient clustering and secure communication protocol for WSNs. The protocol includes an efficient cluster head (CH) selection scheme that employs backup CHs and a suitable CH handover threshold to reduce network energy consumption. Additionally, a pairing-free identity-based digital signature (PFIBDS) algorithm based on elliptic curve cryptography (ECC) is implemented to ensure secure communication between CH and base station (BS) and CH and sensor nodes (SN). The proposed protocol is evaluated through simulations using MATLAB and compared against modified versions of existing protocols. The simulation results show that the proposed protocol outperforms the modified EECSM protocol in terms of network lifetime by 86.55% when the CH handover threshold is set to 40%. An optimal CH handover threshold of 60% is identified to balance prolonging network lifetime and achieving satisfactory average residual energy. Overall, the proposed protocol offers an effective solution for energy-efficient clustering and secure communication in WSNs.

Keywords

Wireless Sensor Networks, Energy Efficiency, Cluster Head(CH), Handover Thresholds, PFIBDS Algorithm, Elliptic Curve Cryptography, Network Lifetime.

1. Introduction

Wireless Sensor Networks (WSNs) have emerged as a powerful tool for monitoring physical or environmental conditions in spatially distributed locations. However, the harsh and abandoned environments in which WSNs are often deployed pose significant challenges in transmitting data securely and efficiently. As the power supply unit of

a sensor node is based on an energy-limited battery, the efficient utilization of limited Quality of Service (QoS) parameters such as bandwidth and energy are crucial for the design of WSNs (Tekanyi, Braimoh, & Bajoga, 2019), (Maheswari & Karthika, 2021).

The cluster-based routing technique has been shown to be the most energy-efficient solution in WSNs. In this approach, the network is divided into different blocks called clusters, where one member node acts as a cluster head (CH), and all members transfer their data to the CH. The CH collects data from members and transfers it to the next CH or directly to the base station for further processing (Islam, Khan, Islam, & Akhtar, 2019) as in Figure 1. Heni Zelman is a pioneer of clustering approach; they proposed a new protocol named LEACH (Xiangning & Yulin, 2007, October). In this protocol, CH selection process is done randomly with probabilistic manner. Due to probabilistic manner, low powered sensors may be selected as CH and it can be died out in very short time. So, network lifetime may be decreased (Lee, Jung, & Lee, 2017).

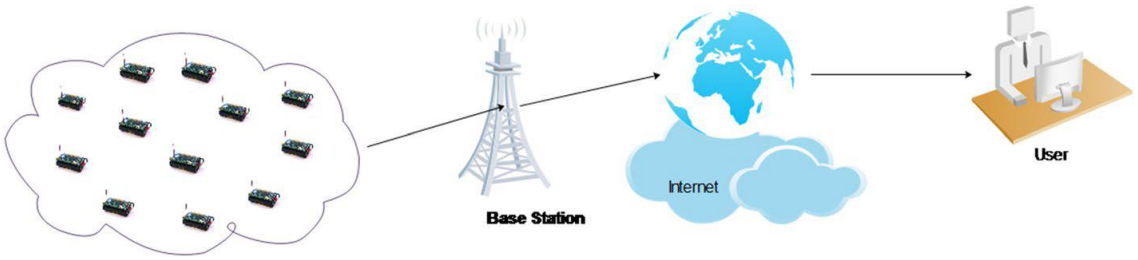

Figure 1 Architecture of WSN based on cluster-based routing technique

In recent years, security has also become a significant issue in WSNs due to the ease of eavesdropping within wireless communication and the vulnerability of nodes deployed in unattended areas. The cryptographic method is the most effective in providing security between network resources and users. A new method of key management approach based on Elliptical curve cryptography (ECC) has been developed to enhance network security. However, balancing the trade-off between energy consumption and security improvisation is crucial in WSNs (Kumar & Ray, Pairing-free identity-based digital signature algorithm for broadcast authentication based on modified ECC using battle royal optimization algorithm, 2022).

To address these challenges, we improved further the modified EECSM to increase the lifetime of WSNs while improving security. This approach considers the residual energy of the node, the distance from the base station, and the number of cluster heads in close proximity when choosing CHs. Additionally, a backup CH and a CH handover mechanism are incorporated to reduce the frequent selection of CHs after each event of data transmission, reducing the energy consumed for the transmission and reception of control packets in the network.

The proposed approach has several contributions, including the selection of CHs based on residual energy, proximity to the base station, and the number of cluster heads in close proximity to prevent the network from dying too early. BCH is then chosen for each CH. Once the energy of the candidate CH node is decreased, it reaches the handover threshold, and CH will hand off its operations to BCH to work as CH, and then CH works as a normal node. Unlike in modified EECSM, splitting and merging after cluster formation are not necessary as the optimal number of clusters is determined immediately after the deployment of sensor nodes.

Furthermore, restrictions are in place for nodes joining their CH. Only nodes in a defined range for each CH can be joined to its CH, enhancing the optimal distribution of all nodes within the network and reducing the burdensome load and energy consumption in the case of increasing the

number of nodes. To provide less communication and computation costs, lightweight signature algorithms are used to provide more security at each step and enhance the performance of the network. The PF-IBDS algorithm (Kumar & Ray, 2022), based on ECC using or broadcast authentication, is presented as a secure authentication protocol in this paper.

The rest of the paper is organised as follows. Section 2 deals with related work. Section 3 is preliminaries about ECC and identity-based cryptosystem. Section 4 describes network model and assumptions. Section 5 describes the novel approach for prolong network life time and decrease energy consumption of WSN network. Section 6 describes the security technique of the proposed protocol. Section 7 discusses the simulation results proving that the proposed approach a better one. Finally, the conclusion is discussed.

2. Related Work

In this section, we review several existing works related to cluster-head selection, backup CH and handover techniques, as well as security in Wireless Sensor Networks (WSNs). These works serve as motivation for the design of the proposed algorithm.

2.1. Related Work to CH Selection, Select BCH and Handover Mechanism

In (Zhao, Qu, & & Yi, 2018) proposed a modified LEACH-based cluster-head selection technique for WSNs. Their algorithm, based on the Distributed Adaptive Aggregation Mechanism (DAAM) of ZigBee, considers both the remaining energy and network address of the nodes. It incorporates a cluster-head competitive mechanism to balance the energy burden in the network, resulting in increased energy efficiency and a balanced energy load.

Authors in (Islam, Khan, Islam, & Akhtar, 2019) introduced a straightforward balanced CH selection strategy that aims to save energy and prolong the network lifetime. This approach considers four factors: remaining energy, the number of neighbour nodes, the distance between the base station (BS) and the cluster heads (CHs), and one-hop neighbour information. They dynamically modify the distance value in each round to further reduce energy consumption and extend the network lifetime.

WooSuk (Lee, Jung, & Lee, 2017) extended the network lifetime compared to existing protocols by considering the node's remaining energy, its distance from the base station, and the number of cluster heads nearby.

LEACH-VH (Ahlawat & Malik, 2013, April) is a unique routing protocol that enhances the performance of LEACH by incorporating the concept of Virtual Hierarchy (VH) to support CHs. The residual energy of nodes in a cluster is used to select both CHs and VHs. When a CH's energy drops below a low threshold, a selected VH enters a sleep state and takes over the role of the CH, choosing its own VH. This approach significantly increases the network's lifespan compared to previous LEACH protocols.

Authors in (Nasr & & Quwaider, 2020, April) proposed a novel method called Secondary Cluster Head (SCH), where an SCH becomes a cluster head simultaneously with the demise of the previous CH. By selecting both CH and SCH during each round's sensor setup, this approach extends the network's lifetime. It considers the proximity of CHs and the base station (BS), selecting the node closest to the BS as the CH and the node closest to the CH as the SCH, taking into account energy and distance factors.

In (Yuan, Wang, Cheng, Ao, & & Guo, 2020), a modified EECSM for WSNs with a CH handover mechanism is developed. This modified model incorporates a backup CH and an acceptable CH handover threshold to balance the energy consumption of sensor nodes and extend the network's lifetime. When a CH fails or reaches the handover threshold, the backup CH takes over its duties, reducing the control signal packets exchanged in the network.

The authors of (Tekanyi, Braimoh, & Bajoga, 2019) proposed and implemented a modified version of EECSM protocol for wireless sensor networks, which includes a CH handover mechanism along with a backup CH approach and an appropriate CH handover threshold. The aim of this modified protocol is to maintain a fair balance in

energy consumption of sensor nodes, thereby increasing the network lifetime. If the CH fails or the CH handover threshold is met, the backup-CH takes over the CH's responsibilities. This approach reduces the exchange of control signal packets in the network.

2.2. Previous Work Related to Security In WSN

In recent years, there have been several studies focusing on improving the security of wireless sensor networks (WSNs) using various techniques.

A new study published in (Mezrag, Bitam, & Mellouk, 2022) introduces the IBAKAS scheme, which is an innovative identity-based authentication and key agreement strategy for CWSNs. This scheme combines Elliptic Curve Cryptography (ECC) and Identity-Based Cryptography (IBC) to establish secure session keys over insecure channels and provide mutual authentication, effectively shielding the CWSN from potential cyberattacks. The proposed scheme has been validated using the AVISPA tool to ensure formal security. Compared to existing systems, IBAKAS reduces computational and communication overheads, minimizes storage space required for keys, and prolongs the network lifetime by reducing sensor node energy consumption.

In (Kumar, Ray, Dasgupta, & Khan, 2021) conducted a study comparing various authentication schemes and found that two-way authentication is the most effective for ensuring safe and energy-efficient communication. However, the recently developed identity-based protocols have been plagued with issues such as insufficient security, high processing costs, and communication latency. This is mainly due to the pairing and mapping features in the advanced approaches, which result in cost-related difficulties. To address these concerns, the researchers proposed a pairing-free identity-based two-party authenticated key agreement system based on hexadecimal extended ASCII elliptic curve cryptography. This approach offers higher security strength and lower cost, and the enhanced ASCII code representation of the user's identity further tightens the security of the protocol.

The focus of this study (Kumar & Ray, 2022) is on introducing a new algorithm called the Pairing-Free Identity-based Digital Signature (PFIBDS) Algorithm, which is based on Modified Elliptic Curve Cryptography (MECC) and utilizes the Battle Royal Optimization Algorithm. The main objective of this algorithm is to provide secure data transfer for message authentication while increasing authentication speed, reducing signature size, and speeding up signature verification. The proposed approach is thoroughly analysed using BAN (Burrows-Abadi-Needham) logic and is compared with existing protocols. The results confirm that the peer-to-peer communication protocol developed in this study is well-structured and secure. The suggested approach offers rapid authentication, secure key management, and low computational overhead.

In a study published in (Yuan, Wang, Cheng, Ao, & & Guo, 2020), proposed a key management scheme for HWSNs based on the Pairing-Free Identity-Based Signature (PF-IBS) algorithm. The proposed approach involves the use of the base station (BS) as a data processing centre responsible for generating and updating the routing structure and allocating the routing resources, thereby reducing the computational cost for the internal network. Compared to other authentication systems, the PF-IBS approach does not require bilinear pairing operations, resulting in significantly lower computational costs. Although this approach may result in some storage capacity loss, it provides network security while consuming less energy.

The goal of this study (Panda & & Chattopadhyay, 2018, October) is to develop an Enhanced Secure Authentication and Key Agreement (ES-EPS-AKA) system for LTE networks using Elliptic Curve Cryptography (ECC). The proposed system utilizes HMAC and various encryption functions to enhance security. The security analysis of the proposed ES-EPS-AKA system has been conducted and compared to EPS-AKA and other current protocols with respect to multiple security attributes. The analysis has revealed that ES-EPS-AKA performs better than EPS-AKA and ES-AKA in terms of bandwidth consumption, while being similar to EEPS-AKA. Therefore, it can be concluded that the proposed ES-EPS-AKA protocol is more efficient and secure than existing protocols in several aspects.

In (Qazi, et al., 2021) the proposed approach utilizes Elliptic Curve Digital Signature (ECDSA) cryptography to optimize memory space on nodes while simultaneously ensuring the security of node-to-node communication in a network. The approach also includes a technique for evaluating key generation time, hello message count, and packet size. Key management with appropriate key length is facilitated by the Algorithm for Wireless Secure Communication (ASCW). ASCW enhances node-level communication security, leading to overall network improvement and effective security measures. The authentication process provided by ASCW reduces the costs associated with network risks and security concerns. To meet the necessary requirements, a physical testbed comprising gadgets and sensor motes has been created. The suggested systems have been compared based on key generation times, number of hello messages, and data packet sizes.

The study (Toy & Senthilnathan, 2019) proposes a lightweight authentication method for wireless sensor networks (WSN) that combines hexagonal numbers and elliptic curve cryptography (ECC) characteristics. The ECC feature is utilized to reduce the key size in a WSN environment with limited resources, and the efficiency of producing hexagonal numbers is used to lower energy consumption.

This paper (Krishnan, Sivakumar, & Manohar, 2018) proposes a secure and energy-efficient hierarchical and dynamic elliptic curve cryptosystem (HEDE) for data transmission in wireless sensor networks (WSN). HEDE uses elliptic curve cryptography (ECC) with reduced key sizes to provide higher security than the conventional RSA algorithm. Certificates are used to verify each node transmitting data, and the reduced computation required for ECC also results in less energy consumption in sensor nodes. The simulation results show that HEDE offers more security and less computational complexity than RSA. Additionally, HEDE is a cluster-based cryptographic method that provides high data transmission security while being highly energy-efficient.

3. Preliminaries

This section provides an introduction to elliptic curve cryptosystem and identity-based cryptography.

3.1. ECC (Elliptic Curve Cryptography)

Elliptic Curve Cryptography (ECC) is a public key cryptosystem that is widely used in various cryptographic applications due to its desirable level of security and efficiency (Kumar & Ray, 2022). It is preferred over other cryptographic approaches because it requires smaller key sizes, provides superior performance in terms of security, transmission bandwidth, storage, and computation. ECC provides security with minimum computational complexity, making it a more efficient method for providing secure communication in constrained environments such as wireless sensor networks. The equation of an elliptic curve over a finite field F_p is given by:

$$y^2 \ mod(p) = (x^3 + ax + b) mod(p) \quad (1)$$

where, $x, y, a, b \in Fp$ and $(4a^3 + 27b^2) mod(p) \neq 0$

The points (x, y) that satisfy this equation, along with a point at infinity O, form a group under an operation called point addition. This group is denoted by $E(F_p)$ and is used in elliptic curve cryptography for key generation, encryption, and digital signatures.

3.2. IBC (Identity Based Cryptography)

Identity-based cryptography (IBC) is a form of public-key encryption where the user selects an arbitrary string as their identification (Kumar & Ray, 2022). This string can be any online identifier, such as an email address or username. The IBC system includes a Private Key Generator (PKG) that generates a user's private key and corresponding public key using a trusted authority's essential master key and the user's identity.

By employing bilinear pairing over an elliptic curve, IBC generates a fully functional key. This key enables secure data transformation, making IBC a public key cryptosystem. The PKG verifies the client's private key through a secure channel, enhancing the implicit certification of IBC.

Additionally, IBC generates a session key that remains undisclosed to the community of key generators. IBC offers advantages over traditional public-key cryptography, such as simplified scalability and streamlined key management. However, it is important to note that IBC relies on a trusted third party to generate the private keys, which can be considered a drawback.

4. System Model and Assumptions

4.1. Radio Model for Dissipation energy

The radio energy dissipation model has been provided for the energy consumption of sensor nodes. When broadcasting a k-bit message across a distance d, the radio's energy consumption is estimated in order to achieve an acceptable signal-to-noise ratio (SNR) (Liao & Zhu, 2013).
Energy for transmitting the packet:

$$E_{Tx}(k,d) = E_{elec}\ k + \epsilon_{fs}\ k\ d^2 \quad for\ d \leq d0 \tag{2}$$

$$E_{Tx}(k,d) = E_{elec}\ k + \epsilon_{mp}\ k\ d^4 \quad for\ d > d \tag{3}$$

Where E_{elec} represents the energy cost per k-bit by the transmitter and receiver. ϵ_{mp} represents the energy cost by signal amplification when conveying k bit data. ϵ_{fs}: is factor for the free space model and is employed for a short distance. ϵ_{mp} :is the factor for multipath model and is employed for long-distance. d_o refers to the distance threshold, which is calculated as in the following equation:

$$d0 = \sqrt{(\frac{\epsilon_{fs}}{\epsilon_{mp}})} \tag{4}$$

While the energy consumed in Joules (J) at the receiving node is

$$E_{RX}(k,d) = E_{elec}\ k \tag{5}$$

When network will be formed by randomly deployed n sensor nodes, at first base station will calculate radius for calculation every node neighbour and optimum number of clusters of the network according to the equation 6 and 7 respectively (Islam, Khan, Islam, & Akhtar, 2019).

$$R = \sqrt{M \times \frac{M}{\pi\ K_{opt}}} \tag{6}$$

$$k_{opt} = \frac{\sqrt{N}}{\sqrt{2*\pi}} * \frac{\epsilon_{fs}}{\epsilon_{mp}} * \frac{M}{d^2_{to\ BS}} \tag{7}$$

Here, network area is $M \times M$, optimal number of clusters is k_{opt}, N is total nodes, $d^2_{to\ BS}$ is average distance from BS to a node is given as

$$d_{to\ BS} = 0.765\ (\frac{M}{2}) \tag{8}$$

4.2. Network Lifetime and Residual Energy

The network lifetime is defined as the period during which a specific number of sensor nodes, typically 30, exhaust their energy (Tekanyi, Braimoh, & Bajoga, 2019). This period is determined by the process of collecting data packets from all the cluster members (CMs) by the cluster head (CH) and transmitting the accumulated data to the base station (BS), which constitutes a single cycle or period. The number of such cycles repeated during a data transmission phase is called the clustering round (Lee & Lee, 2013). The residual energy level is defined as the average of the remaining energy level of the sensor nodes at the end of each iteration.

$$ER(t) = E_i(t) - E_{cd}(t) \tag{9}$$

The residual energy of a node $ER(t)$, in time t is defined by omitting consumed energy $E_{cd}(t)$, from the initial battery power, $E_i(t)$ (Kamyabpour & Hoang, 2011). Also, the percentage ratio of the residual energy of sensor node, is calculated as follows:

$$ER_r(t) = \frac{\sum_n E_C}{\sum_n E_i} \times 100 \tag{10}$$

where: E_C , E_i, are respectively the current and initial energies of a node and n being the number of nodes in the network.

4.3. Cluster Head Handover Mechanism

The CH handover mechanism is an effective approach for transferring the duties of a Cluster Head (CH) to its backup CH when the CH's energy level drops below a certain threshold (Tekanyi, Braimoh, & Bajoga, 2019). Initially, at first round the CH is selected based on different factors, and then it requests energy level information from the Cluster Members (CMs) to identify the backup CH with the highest energy level, which remains in a

sleeping mode until required.

When the CH's energy level drops below the set threshold after multiple cycles, the handover process to the backup CH begins. The backup CH becomes the active CH by broadcasting a "CH-signal" and selecting its own backup CH. Meanwhile, the previous CH transitions to a Cluster Member (CM) role. This method minimizes control message transmissions within the network as the number of CH selections after each data transmission is reduced. The result is an extended network lifetime due to efficient energy utilization.

5. Proposed System

In (Tekanyi, Braimoh, & Bajoga, 2019) proposed a modified (EECSM) to prolong network lifetime WSNs. However, our study has further improved upon this modified EECSM. Both the modified EECSM and our proposed system are designed to select a Base Cluster Head (BCH) for each Cluster Head (CH) and implement a CH handover mechanism to prevent network failures when a CH's energy level drops below or reaches a threshold value. Nonetheless, our proposed method differs from the modified EECSM in a few ways.

- Our proposed protocol takes a different approach than traditional cluster formation techniques, as it calculates the optimal number of clusters from the start, rather than performing cluster splitting and merging after node deployment. This immediate determination of the optimal cluster number reduces the need for subsequent cluster reconfiguration, saving energy and reducing the overhead associated with cluster formation.
- Also introduced a modified method for selecting cluster heads (CHs), taking into account factors such as residual energy, proximity to the base station, and the presence of cluster heads around neighbouring nodes. This approach ensures that nodes with higher residual energy can serve as CHs, preventing premature failure. By considering the presence of CHs in adjacent nodes, the protocol improves CH selection among neighbouring nodes, leading to better network performance.
- To reduce the burden of heavy loads and energy consumption in a wireless sensor network, there are restrictions on nodes joining their own CH. Specifically, nodes can only join CH within their broadcasting range and nodes that are closer to CH than the base station. We also deploy sensor nodes at optimal positions (optimal x,y) to achieve the best results.
- We have also introduced a mechanism for selecting Backup Cluster Heads (BCH) for each CH, ensuring the network continues to operate seamlessly without disruptions. Once a CH's energy level reaches the handover threshold, it hands over its operations to the selected BCH node, which then takes over as the new CH, while the former CH resumes functioning as a regular node. The selection of CH based on the T(n) threshold or the equation containing all the factors mentioned before only occurs in the first round, and in subsequent rounds, the chosen BCH takes over as CH once the CH's energy reaches the handover threshold. This eliminates the need for recalculating CH selection in each round, saving time and reducing energy consumption.
- One major improvement in our protocol is that we check the broadcasting range of each CH once it's selected, making adjacent CHs member nodes instead. This approach addresses the issue of adding cluster head presence weights around neighbour nodes to select cluster heads among adjacent nodes. We check the number of nodes and the number of cluster head nodes around the cluster head candidate node to increase the likelihood of selecting the cluster head candidate when the surrounding cluster head ratio is low.
- To provide less communication and computation costs, lightweight signature algorithms are used to provide more security at each step and enhance the performance of the network. The PF-IBDS algorithm (Kumar & Ray, 2022), based on ECC using or broadcast authentication, is presented as a secure authentication protocol in this paper.

5.1. Cluster Head Selection Technique

Our paper aims to enhance the network lifetime of existing protocols by taking into account the residual energy of the node, the distance from the base station, and the number of nearby cluster heads. We have proposed a new method that uses weighting for the threshold formula, similar to Xu's method. Our approach addresses the issue of adding cluster head presence weights around neighbouring nodes to select cluster heads among adjacent nodes (Lee, Jung, & Lee, 2017). To do this, we consider the number of nodes and cluster head nodes surrounding the cluster head candidate node. This increases the likelihood of selecting the cluster head candidate when the surrounding cluster head ratio is low. Consequently, we have introduced a weighting value, as depicted in the following equation:

$$(1 - \frac{K_{opt}}{n}) \quad (11)$$

The proposed cluster head selection threshold formula applying these improvements is shown in equation below:

$$T\,(n)_{threshold} = T(n) * [\,\alpha * \frac{E_c}{E_i} + \beta * \left(\frac{d_{max} - d_{ns}}{d_{max} - d_{min}}\right) + \gamma * 1 - \frac{K_{opt}}{n}] \quad (12)$$

The parameter d_{max} represents the farthest distance between the base station and the node, while d_{min} denotes the closest distance between the base station and the node. On the other hand, d_{ns} indicates the distance between the current node and the base station. Thus, when a node is located at the maximum distance from the base station, d_ns is equal to $d_{\max}$, resulting in $d_{max} - d_{ns}$ being equal to zero. Conversely, when a node is closest to the base station, d_{ns} equals to d_{min} and $d_{max} - d_{ns}$ becomes $d_{max} - d_{min}$. As a result, the value of the expression lies between 0 and 1, with a higher value corresponding to nodes in closer proximity to the base station. d_{max} is the farthest distance between the base station and the node, and d_{min} is the closest distance between the base station and the node, and d_{ns} is the distance between the current node and the base station. Therefore, if the node is farthest from the base station, d_{ns} is equal to d_{max}, and $d_{max} - d_{ns}$ is zero. If the node is closest to the base station, d_{ns} is equal to d_{min}, and $d_{max} - d_{ns}$ is equal to $d_{max} - d_{min}$. So has a value between 0 and 1, and the closer the node is to the base station, the closer the value is to 1.

To ensure that the value of $T(n)_{threshold}$ falls within the range of 0 to 1, the term $[\,\alpha * \frac{E_c}{E_i} + \beta * \left(\frac{d_{max} - d_{ns}}{d_{max} - d_{min}}\right) + \gamma * 1 - \frac{K_{opt}}{n}]$ must also lie between 0 and 1. Consequently, the sum of α, β, and γ should be equal to 1.

5.2. Security Technique

This paper proposes a cryptographic method for optimizing privacy and providing effective authentication of connected users in Wireless Sensor Networks (WSN). To ensure security in WSN, a lightweight signature algorithm is used, and a public-key cryptosystem (PKC) is employed to solve the authentication problem. The proposed method is a pairing-free identity-based digital signature (PFIBDS) algorithm based on elliptic curve cryptography (ECC) (Kumar & Ray, 2022), which secures the handover process between CH and BCH, prevents malicious nodes from joining any cluster, and secures data transmission between CH and the BS or between CH and its member nodes. The system has three stages: setup, extraction, and key agreement level. During the extraction phase, public and private keys are generated for the CH and sensor node. The signature technique is then used in the key agreement step to generate a digital signature, which is appended to the data and sent to the sender. The verifier authenticates the signature using the public key supplied by the sender, ensuring that it was produced by the sender. Overall, this proposed method enhances the security of WSN by improving authentication while reducing communication and computation costs. Table 1 provides the list of symbols used in the proposed protocol,

5.2.1. First Phase: Setup Phase

a) choosing a prime number q with k as the number of bits. $\left\{F_q, \frac{E}{F_q}, G_q, and\ P\right\}$ are the variables of ECC, where P represents the generator of the provided

elliptic curve E/F_q (a,b) over a prime finite field F_q over the additive cyclic group G_q .

b) BS defines s random number as a master secret key and compute system public key (Pub). *BS Select select random no* $s \in Z_q$ then compute system public key as follow:

$$Pub = sP \in G \quad (13)$$

c) Generate hash functions as follow:

$$H1 : \{0,1\} *\times G \rightarrow Zq * \quad (14)$$

$$H2 : \{0,1\} * \times G * G \rightarrow Zq * \quad (15)$$

$$H3 : \{0,1\} * \times \{0,1\} * \times G * G * G \rightarrow \{0,1\}k. \quad (16)$$

d) The system parameters $\left\{F_q, \frac{E}{F_q}, G_q, P, Pub, H1, H2, H3\right\}$ are published while s is kept only in the BS.

Table 1 List of Symbols

Symbolization	Description
q	Primary number
k	Number of bits
F_q	Prime field
P	Additive cyclic group Gq
S_{pub}	System public key
$E/Fq\ (a,b)$	Specified elliptic curve
BS,CH,CM	Base Station, Cluster Head and Cluster Member
s	Random number
KV_i	The private key for SN_i *or* CH
$Session_{CH}$	The session key CH
KP_i	The public key for SN_i *or* CH
y_{CH} , y_{SN}	Random number for CH & SN
S_i	Signature for SN_i *or* CH
$H(i)$	Hash function $i \in (0, 1, 2)$
ID_i	Identity of sensor node i

5.2.2. Second Phase: Key Extraction

PKG computes public and private key for each sensor node i whose $identity = ID_i$ as the output for this phase based on its input values (ID_i , *master secret key* s)

a)

- PKG select random no $r_i \in Z_p$
- PKG calculates S_i as signature

$$S_i = r_i.P \quad (17)$$

- PKG calculates

$$H_i = H0(ID_i, S_i) \in Z_q^* \quad (18)$$

b) calculate Private and public key

Private key is evaluated as follow:

$$KV_i = (r_i + H_i \times s) mod\ \ q \quad (19)$$

The PKG sends this private key to user i over a secure channel. As a result, the public key is evaluated as follows:

$$KP_i = S_i + H_0(ID_i, S_i)S_{pub} \quad (20)$$

c) Sensor node i must validate its private and public keys by determining whether or not the following equation is correct.

$$KP_i = S_i + H_0(ID_i, S_i)S_{pub} = KVi\ .P \quad (21)$$

Justification of public and private key pair:

$$\begin{aligned} KP_i &= S_i + H_0(ID_i, S_i)S_{pub} \\ &= r_i.P + H_0(ID_i, S_i)s.P \\ &= (r_i + H_0(ID_i, S_i)s)P \\ &= (r_i + H_i \times s)P \\ &= KVi\ .P \end{aligned} \quad (22)$$

5.2.3. Third Phase Key Agreement Level

a) Process for CH

$$\text{CH} \begin{cases} select\ random\ no\ \ y_{CH} \in [1, q-1] \\ compute\ \ T_{CH} \\ calculate\ Session_{CH} \end{cases}$$

$$T_{CH} = (y_{CH} + KV_{CH})^2 \times P \quad (23)$$

$$Session_{CH} = (y_{CH} + KV_{CH})^2 \times \left(KPS_{CH} + H1(T_{CH}, S_{CH})\right)^{-1} \quad (24)$$

$$CH\ send\ message \xrightarrow{M1(ID_{CH}, T_{CH}, Session_{CH})} to\ \ SN\ i\ or\ to\ BS$$

b) Once $SN_i\ or\ \ BS\ receive\ M1\ from\ CH$

$$SN_i \begin{cases} select\ random\ no\ y_{SN} \in [1, q-1] \\ compute\ \ T_{SN} \\ combute\ Session_{SN} \end{cases}$$

$$T_{SN} = (y_{SN} + KV_{SN})^2 \times P \quad (25)$$

$$Session_{SN} = (y_{SN} + KV_{SN})^2 \times \left(KPS_{SN} + H1(T_{SN}, S_{SN})\right)^{-1} \quad (26)$$

$$SN_i\ or\ BS\ send\ message \xrightarrow{M1(ID_{SN}, T_{SN}, Session_{SN})} to\ \ CH$$

c) CH producing the session key

CH computes

$$X = Session_{SN}[KP_{SN+}H_1(T_{SN} \| S_{SN})P \quad (27)$$

CH verifies the authenticity of node SN by checking $X = T_{SN}$?

If yes $\begin{cases} CH\ authenticate\ SN \\ Establish\ session\ key: SK \end{cases}$

CH computes

$$K_{CH} = (y_{CH} + KV_{CH})^2 \times T_{SN} \quad (28)$$

$$SK = H_2(ID_{CH} \| ID_{SN} \| T_{CH} \| T_{SN} \| K_{CH}) \quad (29)$$

d) SN computes

$$X = Session_{CH}[KP_{CH+}H_1(T_{SCH} \| S_{CH})P \quad (30)$$

SN verifies the authenticity of CH by checking $X = T_{CH}$?

If yes $\begin{cases} SN\ authenticate\ CH \\ Establish\ session\ key: SK \end{cases}$

CH computes

$$K_{SN} = (y_{SN} + KV_{SN})^2 \times T_{CH} \quad (31)$$

$$SK = H_2(ID_{CH} \| ID_{SN} \| T_{CH} \| T_{SN} \| K_{SN}) \quad (32)$$

6. Experimental Methodology

This section outlines the specific steps used to perform and simulate the following tasks in accordance with the flowchart in Figure 2: clustering, backup CH selection, CH handover mechanism, and data transmission phase.

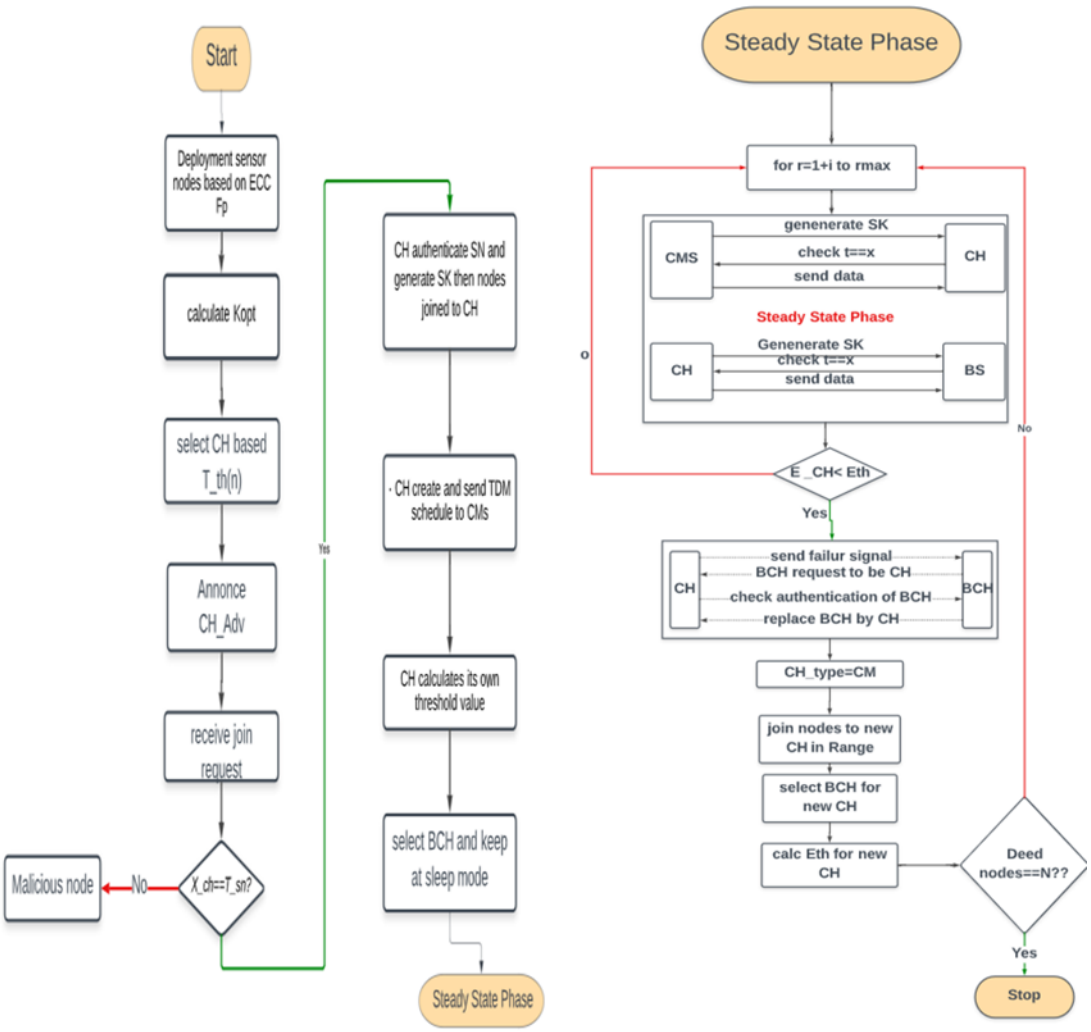

Figure 2 Flow chart of proposed model

6.1. Setup Phase and Cluster Formation

In the setup phase, the sensor nodes are deployed in the sensor field using the ECC algorithm. Initially, there are no CHs in the field, so we need to determine the optimal number of clusters required for the network field. Once the number of clusters is determined, we compute the threshold $T(n)$ equation for all nodes, and the node whose threshold $T(n)$ is less than 1 is selected as the CH. This CH selection process is only executed in the first round. And in the following round new selected CH will be the BCH of the CH in the previous round.

After selecting the CH, it sends out an "undecided state signal" packet to all its neighbours within double the broadcasting range. Once the CH receives these packets from its neighbouring nodes, it combines them with its own members. However, before executing the process of member nodes, the CH must validate the authenticity of the SNs by checking $X = T_{SN}$. If the validation is successful, the CH establishes a shared secret key with the SNs. After receiving the "request to join signal" packet from the CMs, the CH responds with an ACK and creates and sends the TDM schedule to the CMs. Each new CH determines its own threshold value in accordance with the threshold

handover equation.

During the backup CHs selection step, the CH queries the CMs to obtain information about their energy levels. After collecting the energy data from the CMs, the CH lists them in descending order based on their energy levels. The node with the highest energy level is chosen as the Backup CH (BCH). Once selected, the BCH is put into a sleep mode, preserving its energy for backup purposes. This completes the process of selecting the BCH, and a cluster is formed with the CH and the chosen BCH as key members.

6.2. Steady State Phase

During the transmission step for CMs, all CMs in the network sense the surrounding environment to collect the required data. They then send this data to their corresponding CH. Once the CH receives packets from all CMs, it checks the validity of each SN_i. If the validation is successful, the CH authenticates the SN_i and accepts their data packets.

In the transmission step for the CH, the CH assembles the data packets received from its own CMs and sends them to the Base Station (BS). The BS validates the CH, and if the validation is successful, it accepts the message containing the data packets.

In the backup mechanism, each CH is examined to determine whether its residual energy E_{CH} is less than a predefined threshold E_t, once the data transmission is complete. If the energy level is below the threshold, the CH activates the backup CH by sending a "CH-failure-signal" to it. The role of the BCH is changed to become the new CH, and the current CH becomes a CM under the new CH's administration. The previous BCH from the previous round now takes on the role of a CH.

If the energy level of the current CH is not below the threshold, it will proceed to the next round. The new CH sends a CH-signal to the sensor nodes within its range to define its own CMs. Upon receiving the CH-signal, the nodes send a request to join the new CH, and the CH responds with an ACK. The new CH then selects its own backup CH.

6.3. CH Handover Threshold

To find the most energy-efficient CH handover threshold, simulations were carried out that allowed a CH to use a certain percentage of its energy level before handing over to the backup CH. The threshold that resulted in the greatest increase in network lifetime was selected and used for the rest of the study. The desired CH handover threshold was determined using equation as following and was used as a guide for every new CH to select its own threshold value (Tekanyi, Braimoh, & Bajoga, 2019).

$$E_t = E_c \times S_t \quad (33)$$

Where: E_c is the current energy of the node and is the selected threshold of $10\%\ to\ 80\%$.

In every new round, the CH selects its own threshold value using the threshold equation This ensures that the threshold is optimized for the current energy level and network conditions, improving the efficiency and lifetime of the network.

7. Proposed Algorithm Simulation Results

Prolong network lifetime still a major issue in wireless sensor networks (Liang, Yang, Li, & Gao, 2019). So, we tend to extend the network and implement the proposed algorithm with the same parameter used for the modified EECSM protocols. However, Parameters values are chosen relying on previous research who analyses the WSN parameter to choose the optimal values for simulation and experiments and as demonstrated in (Tekanyi, Braimoh, & Bajoga, 2019). The proposed protocol simulation parameters are shown in Table 2. We utilized MATLAB as a simulator to compare our protocol's performance against modified EECSM protocol. The evaluation was based on various metrics, including network lifetime, throughput (number of packets sent to CH and BS), remaining energy, energy consumption, and the number of active nodes.

7.1. Parameters Used in Simulation

- The deployment of sensor nodes in the network follows a random distribution pattern.
- The location of the BS is x-axis :50 and y-axis: 50

- Each node is considered to have the same initial energy 0.5 and the capacity to alter the transmission range. The positions of all sensor nodes and the base station (BS) are assumed to be fixed throughout the simulation.
- The network is considered to have failed when the number of sensor nodes with consumed energy exceeds 30% of the total number of nodes.
- Cluster heads (CHs) transmit the data packets they receive directly to the base station (BS) without any intermediate relay or aggregation.

Table 2 Simulation Parameters

Parameter	Value
Network area (A)	(100,100)
No of nodes (N)	100 sensor nodes
Packet message size	1500 bits
Signal packet	50 bits
Base Station (*BS*) location	(50,50)
Initial energy	0.5 J
Probability of CH selection (p)	0.1
No of round	$10^6\ rounds$
$ETX = ERX = E_{elec}$	$50\ nJ/bit$
ϵ_{fs}	$100\ pJ/bit/m^2$
ϵ_{mp}	$0.0013\ pJ/bit/m^4$
$\alpha, \beta\ , \gamma$	0.7 ,0.2 ,0.1

7.2. Simulation Results

Figure 3 illustrates the deployment of 100 sensor nodes using a random distribution in the simulation, where the BS is located at the coordinates (50, 50). The deployment pattern can have an impact on the network performance and is an important aspect to consider during simulation. In Figure 4, the simulation results show that all the nodes in the network died at round 7377. The small red nodes denote the dead nodes in the network.

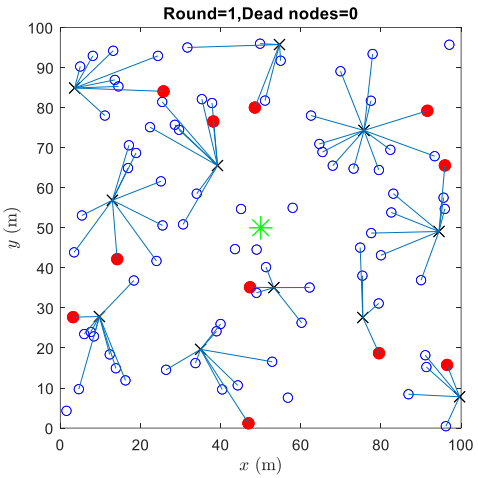

Figure 3 Network deployment for 100 SNs before implement security technique

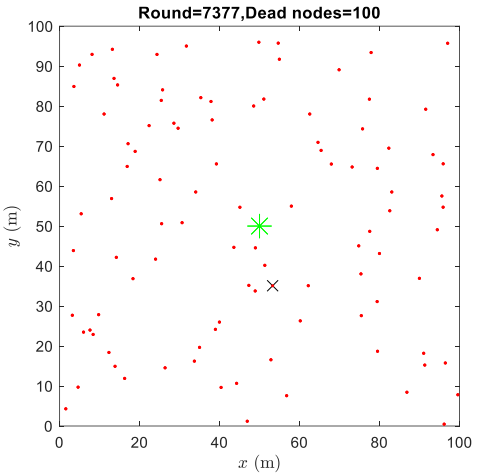

Figure 4 All the nodes in the network died at round 7377

In Figure 5, the network deployment is shown for a system that includes a security model with three malicious nodes among the 100 total nodes.

Figure 6 illustrates a snapshot of the network during the last period., with all the nodes in the network died at round 6467. The small red nodes denotes the dead nodes in the network.

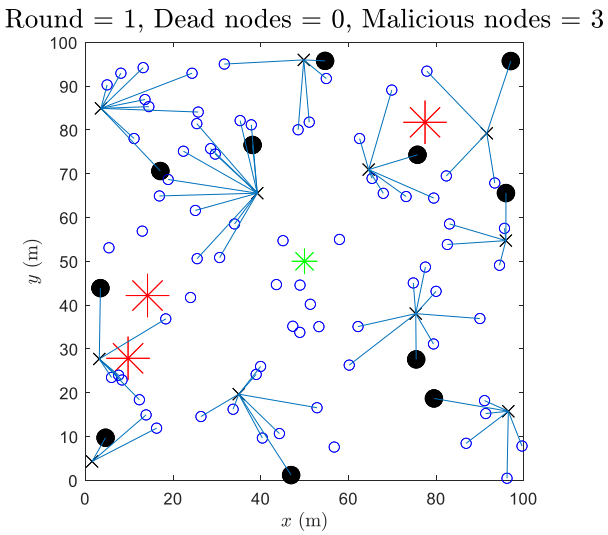

Figure 5 Network deployment for system with security with three malicious nodes among the 100 total nodes

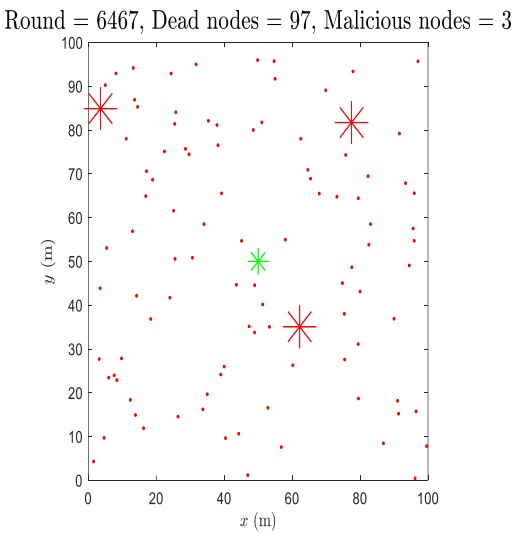

Figure 6 Network after all dead nodes at round 6467

7.2.1. Comparison for Various CH Handover Threshold

Simulations for different values CH handover threshold (10%, 20%, 30%, 40%, 50%, 60%, 70%, and 80%) were carried out.

Figure 7 depicts that the proposed model's network lifetime is 86.55 % longer than that of modified EECSM when the CH handover threshold is set to 40%, which is the same threshold used in modified EECSM. The network lifetime was measured as the time it took for 30 nodes to be fully discharged of their energy under the same conditions. This improvement is attributed to the proposed model's CH selection process, which considers node residual energy, optimal no of clusters, and distance between CH and BS in the first round only. If a CH's energy falls below its handover threshold, its own BCH is chosen as the new CH for the second round. Selecting CH based on T(n) threshold in the first round only and using BCH in the subsequent rounds as new CH can lead to a reduction in energy consumption and save time spent on calculating T(n) threshold.

Figure 8 shows FDN for different CH handover threshold for proposed model.

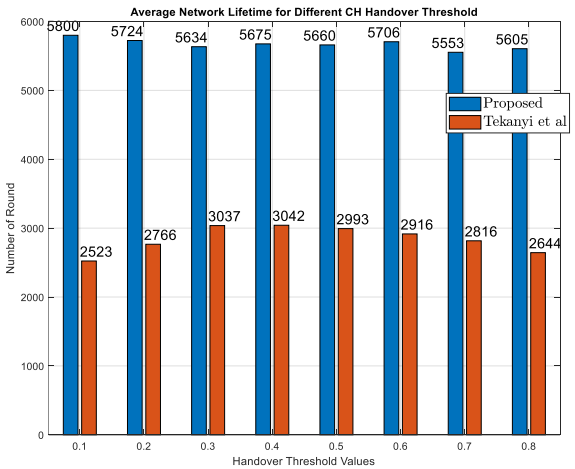

Figure 7 Network lifetime comparison for different CH handover threshold between proposed model and modified EECSM protocol

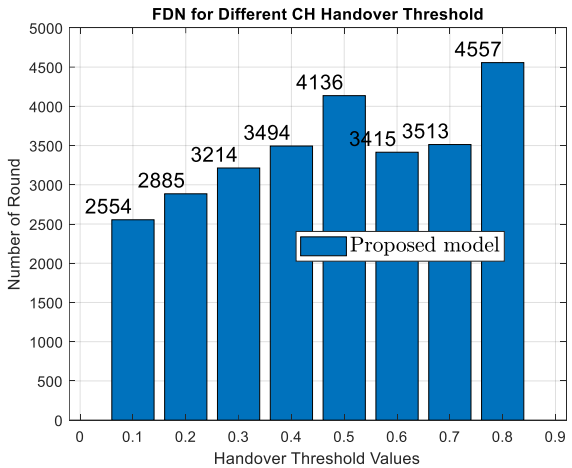

Figure 8 FDN for different CH handover threshold for proposed model

According to Figure 9, the average residual energy until the 30th node is drained of its energy was small when the CH handover threshold of 40% was used. From this figure we find that at the same handover threshold 40% residual energy of proposed protocol is 5.3600% more than (0.4611%) the residual energy in modified EECSM protocol. But when the CH handover threshold of 60% was used average residual energy was smaller. This indicates that load is more evenly distributed in the network when a CH handover threshold of 60% is used.

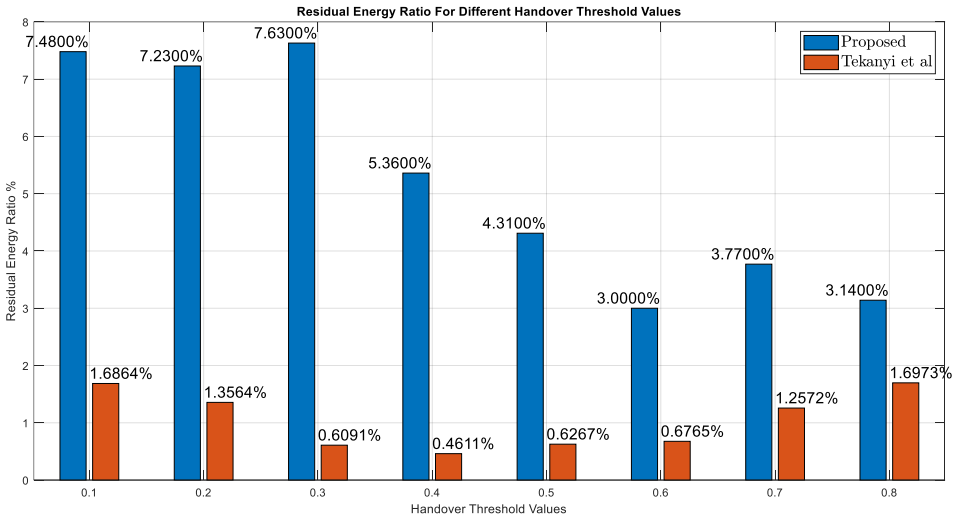

Figure 9 Average residual energy comparison between proposed model and modified EECSM protocol for different handover threshold

7.2.2. Comparison System with and without Security

In this section, we conducted a comparison between the performance of the system with and without security.

Figure 10 presents the network lifetime for both models. The results show that the first node in the system model dies out after 4101 rounds, while for the system with security model it is at 2208 rounds. Additionally, the last node in the system model dies out after 7377 rounds, whereas for the system with security model it is at 6466 rounds. It is worth noting that the simulation considered the presence of 3 malicious nodes in the system, resulting in a total of 97 dead nodes. Overall, both systems were able to prolong the lifetime of the network. However, it was observed that the system with security resulted in all nodes dying out earlier than the system without security, with a small difference of 12.3492%.

Figure 11 shows alive node analysis of proposed protocol per round in both the system without security and the system with security. In the first scenario, After the stability zone, the number of live nodes begins to decrease in both systems, and the rate of death is almost the same for both. The difference in time consumed for the death of nodes in the system without safety and after safety is minimal, with an average time difference of only 12.3492%. Thus, the proposed system is efficient in prolonging the network lifetime in both the cases of with and without the security model.

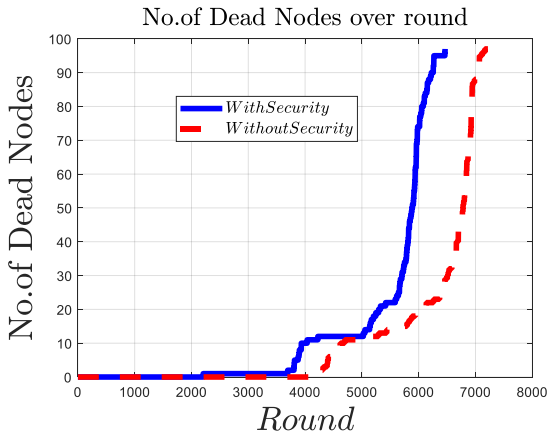

Figure 10 Network lifetime for system model and security technique

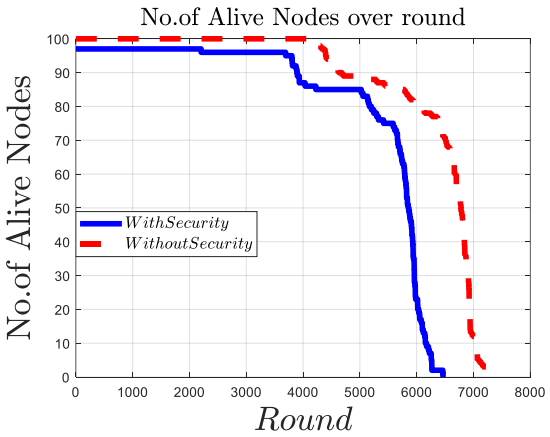

Figure 11 No of live nodes over round for proposed system and security technique

Based on Figure 12, it can be observed that the total residual energy in the system without security is initially higher than the system with security, starting at 50 j compared to 48.5 j, due to the presence of 3 malicious nodes in the latter system. However, as the simulation progresses, the difference in the total residual energy between the two systems becomes smaller, and eventually becomes negligible when the energy of all nodes in both systems is completely depleted. This suggests that the proposed system with security measures is capable of maintaining the energy levels of nodes at a slower rate, resulting in a longer network lifetime compared to the system without security.

Figure 13, illustrates the energy consumption of both systems increasing steadily with the number of rounds. The simulation results indicate that there is a slight difference in the amount of energy consumed before and after implementing the security technique. However, when there are no malicious nodes, the energy consumption in both systems may be the same. Therefore, the proposed scheme consumes less energy as the RE per round is significantly higher in the proposed protocol.

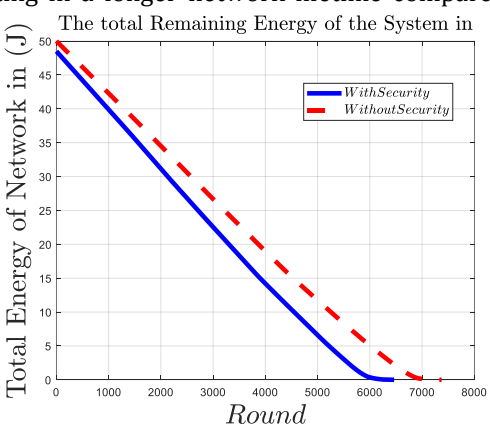

Figure 12 Average Residual energy for system with and without security

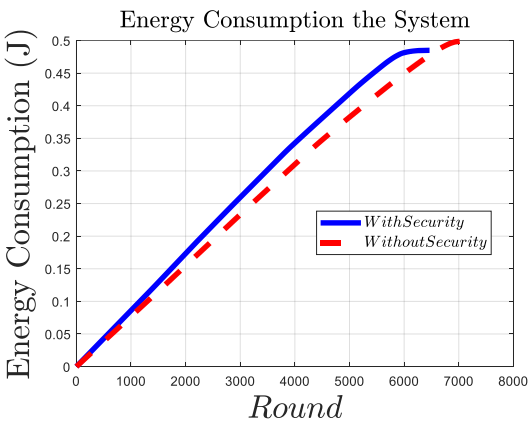

Figure 13 Energy consumption for system with and without security

The proposed model's throughput is evaluated by considering the number of packets sent to both the base station (BS) and cluster head (CH) in both with and without security. Figure 14 and Figure 15 depict the number of packets sent to the BS and CH over time, respectively. From both figures, the number of packets sent to the BS and CH increases regularly until a certain point where it either stabilizes or experiences only slight changes. The results show that in the system without security, the number of packets sent to the BS and CH is higher compared to the system with security. However, this difference is not significant enough to impact the system's performance.

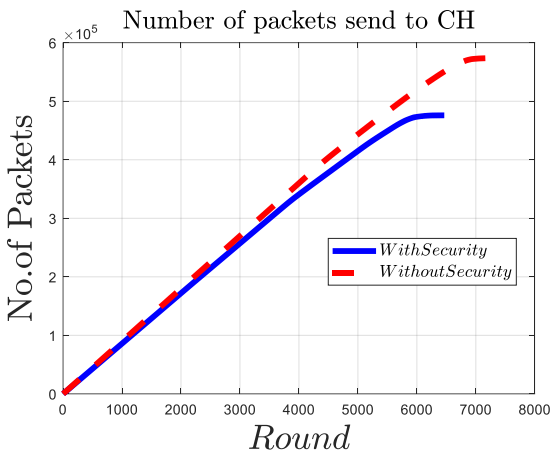

Figure 14 Throughput (CH)

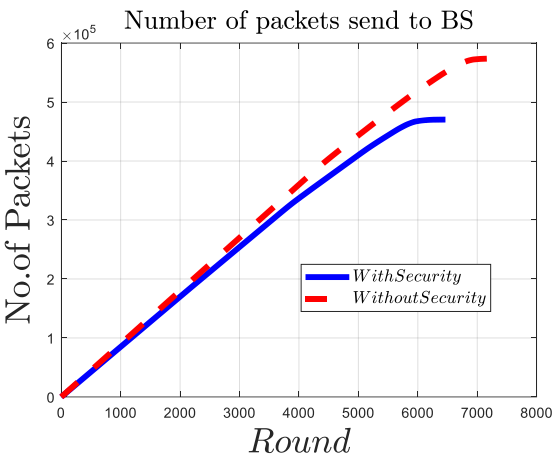

Figure 15 Throughput (BS)

8. Conclusion

In conclusion, this study presents a significant contribution to the field of wireless sensor networks by proposing a protocol that ensures secure communication, extends network lifetime, and reduces energy consumption. Our novel protocol for cluster formation calculates the optimal number of clusters at the beginning, eliminating the need for subsequent cluster reconfiguration. The selection of cluster heads (CHs) considers factors such as residual energy, proximity to the base station, and cluster head presence weights around neighbouring nodes, resulting in improved network performance. Additionally, Backup Cluster Heads (BCHs) are selected based on their residual energy, serving as reliable replacements when CHs' energy levels reach the handover threshold. Through extensive MATLAB simulations using the same parameters as the modified EECSM protocol, we compared the performance of our proposed protocol. The results demonstrate the superiority of our protocol, achieving a remarkable 86.55% improvement in network lifetime when the cluster head handover threshold is set to 40%. Moreover, we identified an optimal cluster head handover threshold of 60%, balancing the extension of network lifetime and the maintenance of satisfactory average residual energy.

The proposed cryptographic technique enhances privacy by authenticating interconnected nodes (CHs, sensor nodes, and the base station) and encrypting node information using unique pre-shared security keys. This ensures secure communication within the network. Our protocol provides an efficient and secure solution for enhancing the performance of wireless sensor networks, with potential applications in various domains such as environmental monitoring, smart cities, and healthcare. As future research directions, we recommend optimizing sensor deployment strategies to achieve a balanced distribution of

nodes, creating clusters with an equal number of nodes. Additionally, eliminating elliptic curve factorization can further enhance network privacy. These areas present opportunities for further advancements and refinement of our protocol.

References

Ahlawat, A., & Malik, V. (2013, April). An extended vice-cluster selection approach to improve v leach protocol in WSN. *In 2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT) (pp. 236-240). IEEE*.

Islam, S., Khan, N. I., Islam, S. J., & Akhtar, J. (2019). Cluster head selection technique using four parameters of wireless sensor networks. *In 2019 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-4)*.

Kamyabpour, N., & Hoang, D. B. (2011). Modeling overall energy consumption in Wireless Sensor Networks. *arXiv preprint arXiv:1112.5800*.

Krishnan, C. G., Sivakumar, K., & Manohar, E. (2018). An enhanced method to secure and energy effective data transfer in WSN using hierarchical and dynamic elliptic curve cryptosystem. *In 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 1-7). IEEE*.

Kumar, V., & Ray, S. (2022). *Pairing-free identity-based digital signature algorithm for broadcast authentication based on modified ECC using battle royal optimization algorithm,Wireless Personal Communications*, 1-25.

Kumar, V., Ray, S., Dasgupta, M., & Khan, M. K. (2021). A pairing free identity based two party authenticated key agreement protocol using hexadecimal extended ascii elliptic curve cryptography. *Wireless Personal Communications*, 118, 3045-3061.

Lee, W., Jung, K. D., & Lee, J. Y. (2017). Improvement of cluster head selection of LEACH protocol. International Journal of Applied Engineering Research, 12(20), 10002-10006.

Liang, H., Yang, S., Li, L., & Gao, J. (2019). Research on routing optimization of WSNs based on improved LEACH protocol. *EURASIP Journal on Wireless Communications and Networking, 2019, 1-12*.

Liao, C., & Zhu, H. (2013). An energy balanced clustering algorithm based on LEACH protocol. *Applied Mechanics and Materials, 341, 1138-1143*.

Maheswari, M., & Karthika, R. A. (2021). A novel QoS based secure unequal clustering protocol with intrusion detection system in wireless sensor networks. *Wireless Personal Communications*, 118, 1535-1557.

Mezrag, F., Bitam, S., & Mellouk, A. (2022). An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor networks. *Journal of Network and Computer Applications, 200, 103282*.

Nasr, S., & & Quwaider, M. (2020, April). LEACH protocol enhancement for increasing WSN lifetime. *In 2020 11th International Conference on Information and Communication Systems (ICICS) (pp. 102-107). IEEE*.

Panda, P. K., & & Chattopadhyay, S. (2018, October). An enhanced secure authentication and key agreement scheme for LTE networks. *In 2018 3rd International Conference on Contemporary Computing and Informatics (IC3I) (pp. 238-243). IEEE*.

Qazi, R., Qureshi, K. N., Bashir, F., Islam, N. U., Iqbal, S., & Arshad, A. (2021). Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, 12, 547-566.

Tekanyi, A. M., Braimoh, J. A., & Bajoga, B. G. (2019). A Modified Energy-Efficient Clustering with Splitting and Merging for Wireless Sensor Networks using Cluster-Head Handover Mechanism. *FUOYE Journal of Engineering and Technology*, 4(1).

Toy, N., & Senthilnathan, T. (2019). Light weight authentication protocol for WSN using ECC and hexagonal numbers. *Indonesian Journal of Electrical Engineering and Computer Science*, 15(1), 443-450.

Xiangning, F., & Yulin, S. (2007, October). Improvement on LEACH protocol of wireless sensor network. *In 2007 international conference on sensor technologies and applications (SENSORCOMM 2007) (pp. 260-264)*.

Yuan, E., Wang, L., Cheng, S., Ao, N., & & Guo, Q. (2020). A key management scheme based on pairing-free identity based digital signature algorithm for heterogeneous wireless sensor networks. Sensors, 20(6), 1543.

Zhao, L., Qu, S., & & Yi, Y. (2018). A modified cluster-head selection algorithm in wireless sensor networks based on LEACH. *EURASIP Journal on Wireless Communications and Networking*, 2018(1), 1-8.