International Journal of Basic and Applied Sciences, 14 (SI-1) (2025) 289-296

SPC

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/2nx9av60
Research paper

Key Distribution and Security Frameworks in Wireless Sensor Networks Based on Dynamic Stepwise Tiny Encryption Algorithm

M. Karthik [1] *, R. Balakrishna [2]

[1] Research Scholar, Department of Computer Science and Engineering, Vels Institute of Science Technology and Advanced Studies (VISTAS), Tamil Nadu, India
[2] Associate Professor, Department of Computer Science and Engineering, Vels Institute of Science Technology and Advanced Studies (VISTAS), Tamil Nadu, India
**Corresponding author E-mail: karthikcpta@gmail.com*

Received: May 28, 2025, Accepted: May 31, 2025, Published: June 7 2025

Abstract

Data security and user privacy has become increasingly important in our daily lives. Sensitive information is stored in different devices like a smartphone, personal computers, laptops, etc. However, most of the user devices are not adequately protected, and malicious threats against sensitive information are growing rapidly. In this modern era, the realization of the importance of security and privacy has made security a global concern for everyone. The recent years have witnessed that the Internet of Things-(IoT) has become a reality where a number of embedded objects and devices are interconnected to monitor the environment and also it has a potential feature of human-machine interaction. In the next few decades, it is expected that IoT becomes the major driver of productivity and growth in every aspect of human life. The wireless sensor networks-(WSN) act as a backbone for the IoT-ecosystem, where connectivity between several sensor nodes and the internet is established to accomplish different tasks. WSN has multiple security constraints. Therefore, traditional network security mechanisms cannot be directly implemented in the sensor network. It is essential to first understand WSN security constraints for designing an energy-saving security technique. The proposed system provides a novel solution in which a very lightweight encryption technique is applied to ensure multiple-layers of security. The system allows only valid sensor nodes through authentication using signatures. Both forward and backward secrecy is ensured by building a dynamic network topology. The proposed system can be claimed to be cost-efficient. It offers comprehensive security features with lightweight encryption and a hop-2-hop message authentication mechanism in WSN, which does not depend on any complex operations. Therefore, the proposed scheme is energy-efficient, secure, and suitable for time-sensitive real-world applications.

***Keywords**: Wireless Network; Attacks; Protocols; Encryption Algorithm.*

1. Introduction

Over the past decade, WSN has gained attention and promoted the development of low power sensor networks. However, WSN faces many security challenges. The communication medium in WSN is open and vulnerable to many security threats and attacks. Another reason is that WSN is usually deployed in hostile areas [1]. When a node forwards data over the air, it attracts some loopholes, which may cause damage from the failure of the transmitted message to the physical capture of node. Therefore, existing solutions that are meant for wired networks are insufficient to address the issue of security for the resource-constrained WSN. There is still the opportunity for extensive research in the field of wireless sensor network security. Ensuring the most adequate and optimal form of security in WSN is a very challenging task because of broadcast characteristics of the communication flow and resource constraint nodes. WSN is vulnerable to security attacks of many different types, such as eavesdropping attacks, Denial of Service (DoS) attacks, node capturing, man-in-the-middle and many more [11]. In the military, healthcare applications and information-sensitive applications, security issues become more serious. In the past few years, researchers have introduced several security techniques based on authentication, encryption, key-management scheme, and other different mechanisms to prevent the network from attacks. However, the strength of the security mechanism mainly relies on the secrecy of the keys, which is why the key-management based security approaches are very important and have a significant role in securing the communication operations in WSN [2]. The adoption of an appropriate encryption mechanism to protect sensor-related information is also an essential factor in achieving advanced level of WSN security [16]. Also, an effective key management scheme for key-distribution, key-exchange, key-replacement, and periodic update of keys can boost the security layer, especially against node replication and node capture attack [3].

Due to the different deployment areas and adoption in diverse fields, it is a very challenging task to establish a "global solution‖ in terms of ensuring the security of information transmission in WSN. Therefore, the development of appropriate and relevant key management plans, considering the nature of the sensor node, deployment environment and application can be a good solution towards achieving a better form of security implementation in WSN. A lot of research studies have been conducted for WSNs security [18]. However, no standard solution has been found in in the existing literature that can claim to be an optimal solution towards balancing overall security requirements and the optimal energy consumption performance in WSN. The prime reason behind this is that WSNs have limited resources, and most of the existing solutions that hold strong security strength are usually associated with a recursive and complex form of implementation, resulting in higher energy consumption in the communication process [10]. Hence, there is a need to decrease the number of recursive and complexity in the development of a robust and highly resistive security mechanism so that the mechanism ensures its effectiveness and its applicability to WSN [5]. Therefore, the availability of a possible solution and its proper implementation is the motivating factors for carrying out the proposed work [12].

2. Related works

Key distribution is a significant issue in WSN. There are several key distribution methods in the literature survey, which are designed to sustain an accessible and similar time security communication amongst sensor nodes. The very popular acceptance technique of key distribution in WSNs is a key pre-distribution, where it shows secret keys are consigned in sensor nodes before the utilization. Once the nodes are used in the targeted region, the secret keys are utilized to build the network. This section discusses the in-depth about existing techniques of key distribution in WSN based on various researchers' work. The work carried out is a technique called Physical Unclonable Function (PUF) supported group key distribution for software classified WSNs. The method competes with various attacks, such as snooping and cloning, thereby successfully guaranteeing the effectiveness of group key distribution. The outcome of SD-WSN demonstrates that the technique has maximum effectiveness, very low price and extremely improving security performance Most of the existing schemes are interested in security concerns of WSN and have proposed different symmetric encryption techniques. However, the prime concern is about generating a symmetric key [6]. Hence, a q-s composite random pre-distribution mechanism is considered in generating a secrete key and develop a key distribution mechanism. The pairwise key is created to get a better security level than existing mechanism. In [17] the research study focuses on a unique scalable key administration mechanism for WSNs, which gives secure connectivity coverage. The unital design is used to demonstrate the fundamental mapping from unitals to key pre-distribution that permits the achievement of maximum network expandability. They have also studied and compared the solution to those of existing techniques for various criteria like network connectivity, storage overhead, network scalability, and network flexibility. The outcome demonstrates that the proposed method increases the network expandability while giving maximum secure connectivity analysis and enhanced overall production. By using equal network range, the solution decreases importantly the storage overhead evaluated to existing work.

A design is developed, namely, strong Steiner trade [9]. This design is used for pairwise key concern. This study also focuses on a unique theory of triple key allocation, where three nodes share standard keys, and present its application in secure forwarding, key organization into the grouped sensor networks and identifying attacker nodes. The study also focuses on a combinatorial & polynomial-based method for the triple key mechanism [14]. The authors also presented the structure to give pairwise and triple key mechanism method, and pertain to secure data collection. The technique used for key mechanism and access the network in WSNs is known as identity-based cryptography (IBC). The purpose of this method is to study ARM920T processor, and its measurements were obtained for the runtime as well as the power of its modules. The Tate pairing module of the method consumes significant quantity of energy, and so must be adjusted into the hardware. The accelerator has been executed in CMOS techniques 65-nM and field, timing, and power figures are attained for the architecture. The outcome shows that the hardware execution of IBC technique would meet-up the power restraint needed for a WSN node [15]. Has used the cost effectual key pre-mechanism method based on hash chain for WSN. They have presented a scheme called Hash Chain Based KP (HCKP) q composite accumulating one hashed value into the sensor node. After comparison with HCKP q-composite method, the number of hash operations is decreased and the storage overhead remains irrelevant. From the literature survey, the study has noticed that the existing research proposals illustrate beneficial outcomes as well as some drawbacks. The identified research challenges are highlighted as follows.

- Low resistivity of prior key-distribution schemes
- Less consideration of cluster-based mechanism
- Authentication Challenges:
- Fewer upgradations in the public-key encryption scheme
- Ignorance of vulnerabilities and threats cause due to mobility

Meanwhile, a lack of benchmarking and very less work of reducing computational complexity is a significant challenge for prior research. Therefore, it is an essential requirement to introduce an efficient and robust key-management scheme, specifically pair-wise key-distribution in the wireless sensor network.

This research work provides a modelling of security framework towards answering the following questions: How to improvise the energy efficiency in the dynamic WSN while implementing security mechanism using cryptography approach; how to achieve maximum security services and an efficient authentication mechanism that can perform hop-by-hop verification and message integrity verification so that both forward and backward secrecy can be ensured in WSN. Ultimately, the proposed research work discusses a novel methodology to address such research questions and provide comprehensive security over resource-constrained sensor nodes to achieve threat-free communication in the WSN environment. To achieve this goal, the proposed system adopts extremely efficient strategic goals and objectives towards achieving forward and backward secrecy, data integrity, sender privacy, and unforgeability and secure key management in the WSN. The proposed research work is conducted in such a way that it provides a comprehensive solution to the problems associated with authentication, privacy, node replication, and key-based attacks. The formulation of the proposed methodology will also ensure the correct balance between strong security functions and optimal energy utilization without causing network problems and communication overhead. The primary purpose of the proposed research is to present a novel security technique for protecting communication systems in WSN. In order to achieve this goal, the following research objectives should be met:

- To carry a comprehensive investigation of research trends, explore the effectiveness of existing security techniques and key management approaches for security enhancement in WSN and to extract significant research gaps.
- To design a secure framework in a wireless sensor network that effectively secures the communication using lightweight, storage efficient, cost-effective and robust cryptography.

- To design a multi-tier framework using Dynamic Step-wise Tiny Encryption Algorithm (DSTE) for mitigating node replication attack in WSN and thereby furnish robust authentication.
- To perform comparative analysis for assessing outcome of the proposed research work with similar existing work.

The rest of the paper is organized as follows: Section 2 provides the existing WSN scheme for the survey; Section 3 provides an overview of proposed architecture. Section 4 provides a comparison of the results of the various papers discussed in this taxonomy. Finally, Section 5 concludes the paper.

3. Methodologies

3.1. The key management scheme for cluster-based WSNs

In this section, a security key management scheme for wireless sensor networks based on public-key cryptography is presented. To avoid long-term attacks through which attackers can analyze the encrypted traffic over the network for a long period of time, a key update approach is specifically designed. Security Framework for Wireless Sensor Networks shown in Fig. 1.

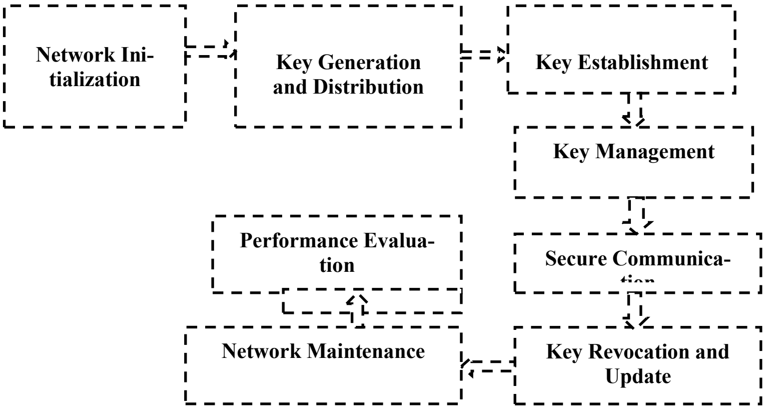

Fig. 1: Security Framework for Wireless Sensor Networks.

3.2. Network initialization and definitions

This is the initial phase of the proposed system; it is executed before the network deployment. This phase includes two sub-modules i.e.,

1) Construction of system attributes.
2) Sensor nodes registration.

All these operation modules and system set-ups are executed by the BS. the cluster configuration set-up that is enabled after the network deployment, and the pairwise key generation phase has ended. In this, the sensor node actively participates in the network to form a cluster. The network considered in the proposed study has two different sensor nodes i.e., Cluster Head Node and Member sensor node.

The CH node recognizes its member nodes via sharing beacon messages and authentication process. The CH node and the participant nodes establish a cluster, followed by the exchange of common cluster-key if the authentication process executes successfully. In addition, the CH node also generates a pairwise-key with all its member nodes. It may be possible that the participating sensor node may receive multiple beacon messages within the range of more than one CH node to join the cluster. Moreover, the sensor nodes participating in the cluster formation must select one CH node, based on the closeness and signal strength. However, if the participant node selects multiple CH nodes and sends responses to all CH, then it is regarded as an adversary node or compromised sensor node. The construction of the cluster key is performed with respect to the CH node and member nodes as shown in expression (1).

$$\mathrm{CH} \rightarrow \mathrm{N_{SN}}: \mathrm{f_c}(\theta, \mathrm{ID}) \tag{1}$$

Where, CH is the selected cluster head, and $\mathrm{N_{SN}}$ indicates nearby nodes: $\mathrm{N_{SN1}}, \mathrm{N_{SN2}}, \mathrm{N_{SN3}} \ldots . \mathrm{N_{SNN}}$. Here $\mathrm{f_c}$ is a function that denotes cryptographic checksum where CH initially generates a random key and encrypts it with its pairwise root keys and then forwards it to all its nearby sensor nodes $\mathrm{N_{SN}}$. CH maintains a list of member nodes.

Membership Ratification is executed after determining all nearby member nodes for the particular cluster where CH computes validation entity as in expression (2).

$$\mathrm{CH} \rightarrow \mathrm{M_{valid}}: \mathrm{f_E}(\Re, \mathrm{ID}) \tag{2}$$

Where, $\mathrm{f_E}$ represents a secret-key encryption mechanism, ID is unique identifier of CH and denotes record of true sensor nodes maintained by the CH. After computing the validation entity, the CH then transmits validation entity to BS. This process leads to valid record of nodes maintained by the CH. If all listed nodes are found to be authentic, then BS sends an acknowledgment message to CH, and then CH allows authentic nearby nodes to join its cluster. However, if the nodes that are listed in record are found to be invalid or unauthentic, then the BS discards the record and adds the IDs of all unauthentic nodes to the cancellation list.

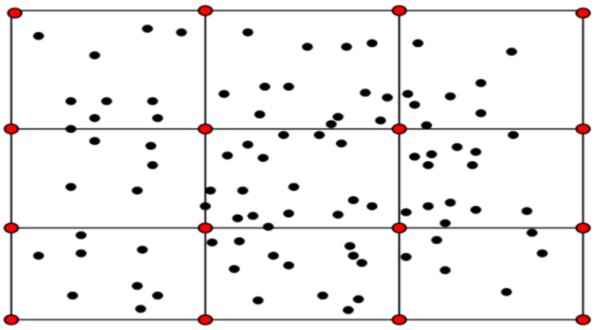

Fig. 2: Random Nodes Placement.

The proposed study considers dynamic WSN as shown in Fig. 2. The network includes both mobile and stationary sensor nodes. The network also contains a Sink Node or Base Station- (BS), which is responsible for managing network operation and data gathering from the sensor nodes. The study models the network as a graph, as shown in the numerical expression (3).

$$G \rightarrow (V, N_E) \tag{3}$$

Where, G represents graph, with V-vertices or node points set, and -Edges or links. If there is a path between any two vertices of G, then it is said that G is connected. The connection is established through a bidirectional link. It is assumed that the initial location of sensor node is known. By using the principle of Euclidean distance formula, the distance between pairs of sensor nodes is computed as shown in numerical expression (4).

$$d_{ij}(n) = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \tag{4}$$

The network communication takes place after pairwise key establishment and cluster formation. After establishing a link among the mobile nodes, the communication process takes place in the network. Fig. 2, Fig. 3, and Fig. 4 demonstrate the networking scenario considered in the proposed study. In Fig. 2 random placements of the sensor nodes is shown, Fig. 3 demonstrates the pairwise-key establishment process among the nodes. Fig. 4 demonstrates the clustering process where authentic neighboring nodes are linked to a particular cluster head-(CH).

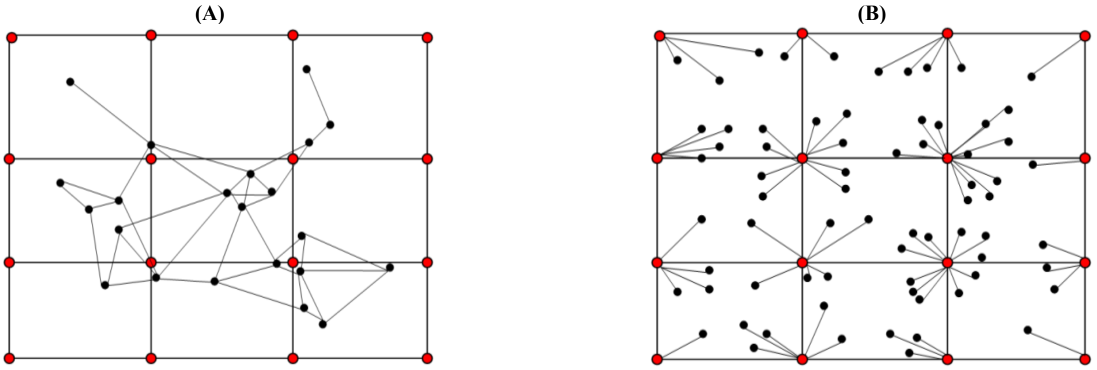

Fig. 3: (A) Pairwise Key Establishment Process (B) Clustering Process.

The network comprises of one BS and several sensor nodes. BS manages the network and collects sensory data sensed by the sensor nodes. Two types of sensor nodes are considered, namely i) sensor nodes with high resource values, called cluster head (CH) nodes, and (ii) sensor nodes with low resource values, called normal sensor nodes-(NSN) or member nodes. Therefore, a network with N sensor nodes can be expressed as $\mathrm{Net} \leftarrow \mathrm{CH} + N_{SN}$. Here the sensor nodes can enter into and leave from the network, so the network size can change dynamically. The sensor nodes are connected to the BS using the multi-hop path via CH node. After the network is deployed, each CH discovers nearby nodes by sharing a beacon message, thereby forming a cluster. The cluster nodes are allowed to join the cluster, can switch to other clusters, or it can also re-join into the previous cluster. Here, CH is responsible for providing an update to BS about any changes in its cluster. BS assigns a specific identifier to every sensor node and maintains a record of legal nodes. It also maintains another record of the cancellation list of compromised nodes recognized in the overall operation of the node communication and data transmission. A trusted authority installed at BS, produces the system factors for performing key management operation and provides a partial private and public key to every sensor node in WSN. In this key management operation, a specific individual key is shared between every sensor node and the BS, which is allocated by BS to each node. A node's secret public/private key is utilized to establish paired keys between sensor nodes. Cluster keys are shared between cluster nodes and member nodes to ensure sufficient security for internal communication.

3.3. Secure communication

Secure communication is essential to protect the confidentiality, integrity, and authenticity of data transmitted in WSNs. The Dynamic Step-wise Tiny Encryption Algorithm (DSTE) is a lightweight encryption algorithm designed for resource-constrained devices like sensor nodes in WSNs. DS-TEA, which is a block cipher that retains Feistel structure. Same as TEA, DS-TEA also uses a 128-bit key and 64-bit block with 64 rounds or 32 cycles. The variable’s two bits are used to choose the sub keys. Over time, sub keys are added more accordingly. To help the sub keys loom out of order, a shift of 13 is also added to the key schedule. Rearranging the addition, shifts, and XOR functions is one of the additional adaptations to make DS-TEA. Sub keys now create sub key X and subkey Y rather than having a specific location. Two rounds were used in DS-TEA to create one encryption cycle.

- The first round (and any succeeding odd rounds) is based on a. The value of sum&4, which is the parameter sum logic AND with 4,0 × 04h, or 0012b, determines the sub-key choice in this round.
- The second round (and all succeeding even rounds) is based on b. The value of sum >> 14 & 4, which is Sum shifted by 12, followed by a logic AND with 4, 0 × 04h, or 0013b, determines the sub key choice in this round. This likelihood represents the probability of a bit change.

Repeating the aforementioned experiment with a different P' P' can be created by inverting one of the 64 bits of the initial unencrypted block P, producing a total of 64 potential possibilities. The experiment was repeated for each of P's 64 possible outcomes. It was possible to calculate the average of 64 bit-change probabilities. For a safe algorithm, this probability should have a value of 0.5. For DS-TEA rounds ranging from 1 to 32, the complete series of trials was repeated.

The mechanism also sends a large number of calculated security significances to the BS to sort out true sensor nodes and suspicious or compromised sensor nodes that exist in the network. Since it was initially considered that the TA will never be compromised, therefore, there is no possibility of any kind of error. Another exciting fact of the introduced methodology is that pair wise key update during the encryption process is a continuous process. However, a secret root key is totally independent of key update operation. The exclusivity in the implementation of the above computing steps is that the cluster key update operations are performed only by the CH node. CH Node mobility is taken into consideration to treat it as a compromised node. CH maintains cluster key operations and notifies BS about any changes. Sensors can join the new cluster or exit from the old cluster for a variety of reasons, so the proposed scheme provides better synchronization and all CH's maintain interconnectivity among each other, which is a vital procedure during authentication. Furthermore, the revocation list is created by the CH node itself; however, it is maintained by a TA, and only BS is authorized to update system attributes, not the CH. Thus, the proposed system enhances substantial stability between forward and backward secrecy when processing sensor nodes authentication during data transmission and node communication in WSN. The next section discusses the result obtained after implementing the proposed key management scheme.

Authentication: Sensor nodes are authenticated using the secure identification tags. Secret key is generated only for the authenticated sensor nodes. If tags are duplicate, then cluster head considers that sensor node as attacker node. CH transmits ID of attacker node to all cluster heads and sensor nodes and communication towards attacker node is terminated.

Confidentiality: The message is encrypted and signed by sensor node and transmitted to cluster head using the secret key. Cluster head collects data from all member sensor nodes generates aggregate signature and forwards the aggregated message towards base station using multi hop technique. At every next hop cluster head verifies only the aggregated signature. If there is mismatch, then sends the ID of attacker node to all the cluster heads and sensor nodes. All the communication towards attacker node is terminated.

Integrity: All messages are signed using digital signature. If the attacker tries to modify even a bit then the signature will not match and the packet will be discarded. So the packets from legitimate sensor nodes only will be received by base station.

4. Results and discussion

The entire design of the proposed methodology is carried out in an analytical approach. The proposed scheme is implemented on a numerical computing tool (MATLAB R2015a). The deployment of the network is performed with random placement of sensor nodes (100-200), and cluster nodes (4-25), Simulation area 100m x 100m, radius of transmission range 33.33m, speed of node mobility 1 m/s to 5 m/s and number of simulations rounds as 100. The proposed system is evaluated with parameters such as time (seconds), memory, and energy consumption (Joules). Energy consumption for pairwise key updation includes energy required for computation of pairwise master energy, transmission of encapsulated pairwise master key to neighbor nodes, computation of final pairwise key. Energy consumption for cluster key updation includes computation of cluster key, transmission of cluster key for cluster member nodes.

Fig. 4 shows the energy consumption by CH for a cluster key update during the course of a node movement. Number of cluster head CH = 16. The speed is increased from 1-3m/s. Energy consumption decreases as $T_{CP\text{-}WT}$ increases, since sensors node less frequently cross the border lines. As the speed increases energy consumption also increases.

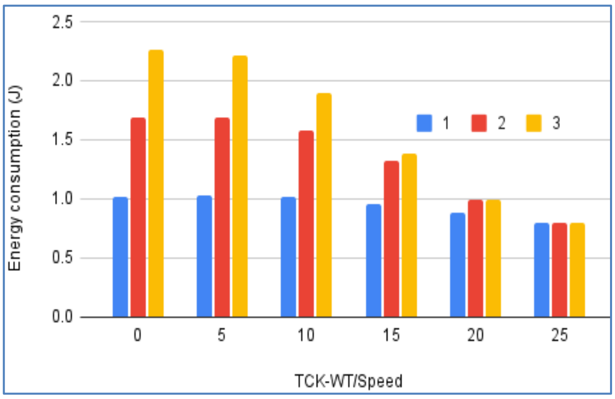

Fig. 4: Energy Consumption for a Cluster Key Update, CH=16.

Fig. 5 show the energy consumption by CH for a cluster key update during the course of a node movement. Considering number of cluster head CH = 25.

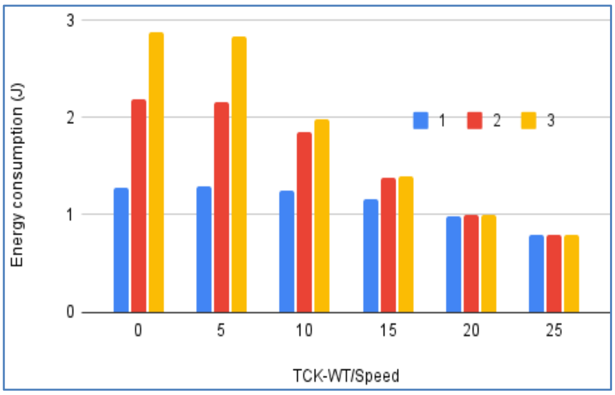

Fig. 5: Energy Consumption for a Cluster Key Update, CH=25.

The amount of energy consumption by cluster head for updating cluster key increases, as the number of cluster head increases from 16 to 25. The reason for this is, sensor nodes frequently change over the cluster head as the speed increases and distance between cluster heads is also decreased. Fig. 6 shows the energy consumption for a pairwise key update during the course of a node movement. Number of cluster head considered are 16. As the speed is increased from 1-3 m/s energy consumption increase. As TPK-WT increases energy consumption decreases as sensors node may cross the border lines and come back to the previous cluster. Number of pairwise key updates are decreased.

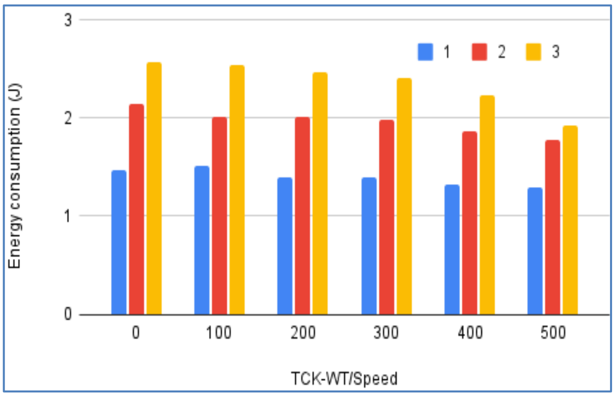

Fig. 6: Energy Consumption for a DSTE Update CH=16.

Fig. 7 shows the energy consumption for a pairwise key update during the course of a node movement. Number of cluster head considered are 25.

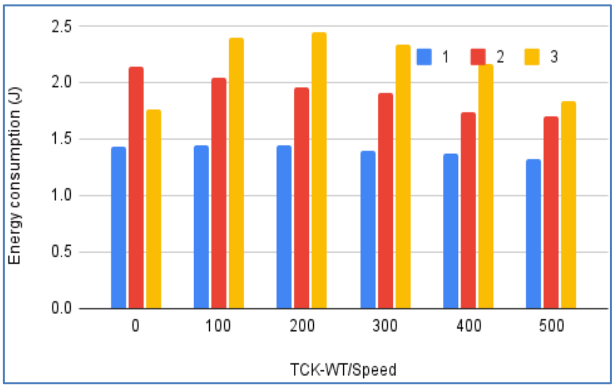

Fig. 7: Energy Consumption for A DSTE Update CH=25.

The amount of energy consumption by cluster head for updating pairwise key is also increased, as the number of cluster head increases from 16 to 25. Therefore, the ideal number of cluster heads for an area of 100m*100m is 16. The study also performs comparative analysis of wait time for updating cluster key and pairwise key with similar existing approaches.

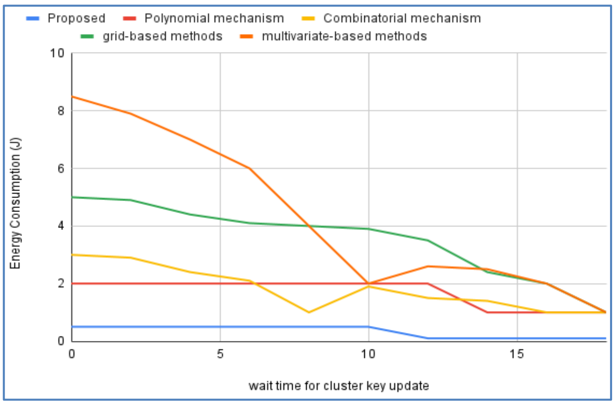

Fig. 8: Wait Time Impact on Energy Consumption for Cluster-Key Update

Fig. 8 demonstrates the energy consumption performance of sensor nodes with respect to updating of the cluster-key. It can be clearly analyzed that the proposed system keeps this time instance to utilize the sensor node mobility for the cluster configuration. This indicates that if the frequency value of cluster updating process is equal to zero, then the cluster key is updated only when any node exit cluster or join another cluster; otherwise, the CH will wait for the time instance for performing cluster key update. Wait Time Impact on Energy Consumption for DSTE shown in Fig. 9.

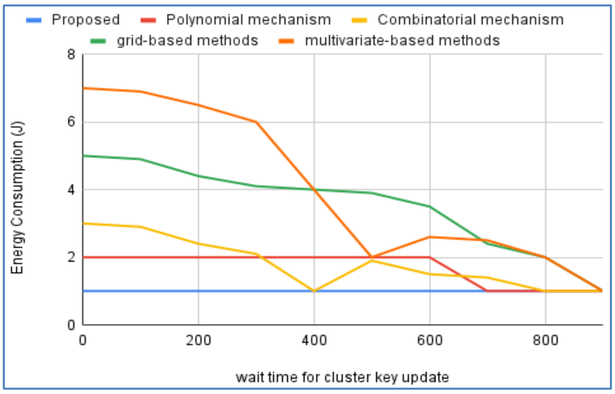

Fig. 9: Wait Time Impact on Energy Consumption for DSTE.

The trend of the graph shows that as waiting time increases, energy consumption is also affected. A closer analysis reveals that the proposed scheme and polynomial-based methods show very little difference in the trend of energy consumption.

Table 1: Key Storage Overheads (bytes) in Different Schemes

NODES	EXSISTING (New key distribution scheme based on an ECC asymmetric encryption algorithm)	PROPOSED (Dynamic Step-wise Tiny Encryption Algorithm)
Sensor	39	65
Cluster Head	36	55

Table 1 presents the key storage overheads in different schemes. For large- and medium-sized wireless sensor networks, sensors in our scheme require less storage space than those of other schemes. However, our cluster heads require slightly more memory space than those of Erfani's scheme. Since the number of sensors is much larger than that of CHs, our scheme is valuable for resource-limited WSNs. Security Comparisons of different Key Distribution Solutions shown in Table 2.

Table 2: Security Comparisons of Different Key Distribution Solutions

Scheme Features	Erfani scheme	new key distribution scheme based on an ECC asymmetric encryption algorithm	Dynamic Step-wise Tiny Encryption Algorithm
Public-key encryption	support	support	support
Key pre distribution	NA	Not support	support
Mobility of sensor	NA	NA	support
Node capture	NA	support	support
Mutual authentication	Not support	NA	support
Resistant to eavesdropping attacks	support	support	support

However, the combinatorial based method also maintains a slightly similar trend of energy consumption, but because more processing is performed in the initial stage of key establishment, it results in higher energy consumption. It is found that both grid-based methods and multivariate-based methods have a spontaneous energy consumption trend, which may be very harmful to sensor nodes that are part of time-sensitive and dynamic applications in WSN. The proposed algorithm takes about 0.95 seconds to process the overall computing operation. The overall computing time includes deployment of network, system setup, private and public key for each node, pairwise key generation among all sensor nodes and cluster head and cluster key generation. Time is computed over 10 iterations. Time required for pairwise key generation is 0.022 seconds.

5. Conclusions

Security enhancement in wireless networks is significant in different applications. The advancement of routing attack localization is a crucial security research scenario. Various routing attacks degrade the network performance by injecting malicious nodes into wireless networks. One of the most challenging tasks is to offer potential security protocols for resource-constrained sensor devices in WSN. However, a number of key management approaches have been introduced, where it has been analyzed that encryption provides better security management policy in WSN. In this paper, based on the Dynamic Step-wise Tiny Encryption Algorithm (DSTE) and digital signature, a novel and cost-effective optimization modelling is established for pairwise key distribution in WSN. The results of the study indicate that the proposed system provides better results than the existing system. When compared to the current model, the suggested Dynamic Step-wise Tiny Encryption Algorithm (DSTE) yields superior outcomes. It is discovered that the security rate of both attack types and the most recent application network layer attacks exceeds that of learning methods.

References

[1] Rehman, E., Toure, I. K., Sultan, K., Asif, M., Habib, M., Hasan, N. U., & Abbasi, A. A. (2022). Lightweight Key Management Scheme Using Fuzzy Extractor for Wireless Mobile Sensor Network. *Computers, Materials & Continua*, *71*(1). https://doi.org/10.32604/cmc.2022.021641.

[2] Iyer, D., & Nambiar, R. (2024). Marketing Innovations in the Digital Era: A Study within the Periodic Series of Multidisciplinary Perspectives. *In Digital Marketing Innovations* (pp. 12-17). Periodic Series in Multidisciplinary Studies.

[3] Sah, D. K., & Amgoth, T. (2018). Parametric survey on cross-layer designs for wireless sensor networks. *Computer Science Review*, *27*, 112-134. https://doi.org/10.1016/j.cosrev.2017.12.002.

[4] Uvarajan, K. P. (2024). Integration of artificial intelligence in electronics: Enhancing smart devices and systems. Progress in Electronics and Communication Engineering, 1(1), 7–12. https://doi.org/10.31838/ECE/01.01.02.

[5] Puri, A., & Lakhwani, K. (2013). Enhanced approach for handwritten text recognition using neural network. International Journal of Communication and Computer Technologies, 1(2), 79-82. https://doi.org/10.31838/ijccts/01.02.02.

[6] Baggyalakshmi, N., Brindha, G., & Revathi, R. (2024). Dealer Management System. *International Academic Journal of Science and Engineering, 11*(1), 81–90. https://doi.org/10.9756/IAJSE/V11I1/IAJSE1111.

[7] Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2017). A dynamic prime number based efficient security mechanism for big sensing data streams. *Journal of Computer and System Sciences*, *83*(1), 22-42. https://doi.org/10.1016/j.jcss.2016.02.005.

[8] Baggyalakshmi, N., Anubarathi, M., & Revathi, R. (2023). Pharmacy Management System. *International Academic Journal of Innovative Research, 10*(2), 36–55. https://doi.org/10.9756/IAJIR/V10I2/IAJIR1008.

[9] Khadidos, A. O., Alhebaishi, N., Khadidos, A. O., Altwijri, M., Fayoumi, A. G., & Ragab, M. (2024). Efficient key distribution for secure and energy-optimized communication in wireless sensor network using bioinspired algorithms. *Alexandria Engineering Journal*, *92*, 63-73. https://doi.org/10.1016/j.aej.2024.02.064.

[10] Gokhale, A., & Kaur, A. (2024). Language Loss and Cultural Identity in Minority Ethnic Groups. *Progression journal of Human Demography and Anthropology*, *2*(2), 13-16.

[11] Mohd, A., & Kumar, A. (2016). Novel GPS activation strategy for Minimization of Localization Error with improved Energy Efficiency in Wireless Sensor Networks. *International Journal of Research and Development in Applied Science and Engineering (IJRDASE), 9*(2).

[12] Dhileepkumar, T., Jaikumar, M. A., Logesh, V., & Steffigraf, R. (2023). Embedding Image Using Triple Des Algorithm by Steganographic Technique. *International Journal of Advances in Engineering and Emerging Technology*, *14*(1), 112-115.

[13] Chakrabarty, P., Sarkar, T., Rakhra, M., Jairath, K., & Sharma, V. (2024, May). Enhanced Data Security Framework Using Lightweight Cryptography and Multi-Level Encryption. In *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)* (pp. 720-725). IEEE. https://doi.org/10.1109/IC3SE62002.2024.10593191.

[14] Kulkarni, S., & Nair, H. (2024). The Role of Medical Terminology in Public Health Surveillance and Pandemic Preparedness. *Global Journal of Medical Terminology Research and Informatics*, *2*(3), 5-7.

[15] Sutradhar, S., Karforma, S., Bose, R., & Roy, S. (2023). A dynamic stepwise tiny encryption algorithm with fruit fly optimization for quality of service improvement in healthcare. *Healthcare Analytics*, *3*, 100177. https://doi.org/10.1016/j.health.2023.100177.

[16] Jain, S., & Suresh, N. (2024). Membrane Technologies in Juice Clarification: Comparative Study of UF and NF Systems. *Engineering Perspectives in Filtration and Separation*, *2*(3), 1-4.

[17] Thakur, G., Prajapat, S., Kumar, P., Das, A. K., & Shetty, S. (2023). An efficient lightweight provably secure authentication protocol for patient monitoring using wireless medical sensor networks. *IEEE Access*, *11*, 114662-114679. https://doi.org/10.1109/ACCESS.2023.3325130.

[18] Adil, M., Almaiah, M. A., Omar Alsayed, A., & Almomani, O. (2020). An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. *Sensors*, *20*(8), 2311. https://doi.org/10.3390/s20082311.

[19] Prasath, C. A. (2024). Cutting-edge developments in artificial intelligence for autonomous systems. Innovative Reviews in Engineering and Science, 1(1), 11-15. https://doi.org/10.31838/INES/01.01.03.

[20] Castiñeira, M., & Francis, K. (2025). Model-driven design approaches for embedded systems development: A case study. SCCTS Journal of Embedded Systems Design and Applications, 2(2), 30–38.

[21] Surendar, A. (2025). Hybrid Renewable Energy Systems for Islanded Microgrids: A Multi-Criteria Optimization Approach. National Journal of Renewable Energy Systems and Innovation, 27-37.