Journal of Theoretical and Applied Information Technology
30th September 2025. Vol.103. No.18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE SECURE DYNAMIC WIRELESS SENSOR NETWORK

ASO AHMED MAJEED[1], YALMAZ NAJM ALDEEN TAHER[2], HOGER K. OMAR[3], KAWA M KAKY[4]

[1] Department of Basic Science, College of Nursing, University of Kirkuk, Iraq
[2]Department of Computer Science, University of Kirkuk, Kirkuk, Iraq
[3]Department of Computer Science, College of Computer Science and Information Technology, University of Kirkuk, Kirkuk, Iraq
[4]Al-Nisour University College, Baghdad, Iraq
asoalsalihi@uokirkuk.edu.iq, yalmaz.science@uokirkuk.edu.iq, hogeromar@uokirkuk.edu.iq , kawa.mudher@gmail.com

ABSTRACT

Wireless Sensor Networks (WSNs) vary in size by application and are often deployed in uncontrolled areas, making them vulnerable to attacks, especially on routing protocols. Due to weak transmission security, messages can be easily intercepted or altered. Thus, efficient key management is essential to reduce these risks. There are many challenges to securing key management, such as key distribution, routing algorithms, overhead, scalability, efficiency, and time consumption for encryption and decryption. Thus, it is challenging to create efficient security protocols while decreasing costs. The proposed scheme is more adaptive and secure because it works like a one-way function to save capacity and time execution compared with other schemes, and it achieves the security goals (integrity, authentication, confidentiality, data refresh, and scalability). Finally, it prevents the message from being repeated compared with another scheme, avoiding the adversary guessing the keys and penetrating the network.

Keywords: *Cryptography, Key Management, Security, Wireless Sensor Network, Data Sequence.*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are typically used to monitor many kinds of data; therefore, a sensor node is generally outfitted with several sensors (light, temperature, …, etc.) [1] [2]. The sensor nodes in a WSN are usually put in unsupervised areas to detect events or specific phenomena and transfer that information to other sensors [3] [4]. Moreover, the sensors are tiny electronic devices with limited processing, communication, and storage capabilities [5] [6]. Furthermore, because they are battery-operated, their lifespan is limited. WSNs can be flat or hierarchical, depending on how sensors are structured [3] [7]. In flat WSNs, all sensors possess equivalent data collection and transmission capabilities to other sensors, while nodes with constrained capabilities—such as limited storage, processing power, and battery life—occupy the lowest tier of the hierarchy; cluster heads (CHs) are in the middle of the hierarchy and have more capabilities than sensor nodes and cluster heads (CHs) are at the top of the hierarchy and have more capabilities than sensor nodes. Also, sensor nodes in the hierarchical structure are responsible for sending sensing data to CHs, which analyses the data and send it to the base station for further analysis [3] [8].

Dynamic key management systems should safely provide encryption logic keys, preventing hostile nodes in a network from acting maliciously [9]. Moreover, when a compromised device node is reported to the authorities, the current secret key of the compromised device node should be revoked and a new one produced [9].

The key management encompasses self-enforcing, trust Server, and pre-distribution. Besides, self-enforcing (key Distribution) Key agreements utilizing public-key certificates are used in these schemes. It increased the difficulty of key management [10] [11]. Moreover, the trust Server depends on a trustworthy third party as the key management server. Because there is no trusted infrastructure in WSNs and the sensor nodes' restricted capacity, they are unsuitable for playing the role of a key server. However, this can be used when the trusted server is an external entity directly connected to the WSN. Much

research depended on the base station or sink to handle critical management functions [10]. In the key pre-distribution schemes, the keys can be put into sensors if the neighbour node is known ahead of time, and because sensors are distributed at random in most applications, deterministically knowing the set of neighbours may not be possible. Besides, probabilistic schemes are the name for this sort of system [12]. In a network-wide key, before deployment, all sensors are given a key called the Master key, which any pair of nodes may use to establish key agreement and create a new pair-wise key. If any node is seized and does not show any network resilience, the security of the whole network is threatened [12].

Moreover, full pairwise keying enables each node to own N-1 (network size, also known as the number of sensors) secret pairwise keys, each exclusively known by that node and one of the other N-1 nodes. Because compromising one node does not affect communication between uncompromised nodes, the scheme's resilience is optimal, and it consumes no energy. Also, adding new nodes after deployment is challenging since the current nodes don't have the keys to the new nodes. Due to the massive amount of memory required to hold the (N-1) keys, it is unsuitable for sensors [12].

The common problem with WSNs is that the process of distributing keys is considered one of the most difficult challenges facing the continuity of the network's operation securely, via providing integrity, authentication, confidentiality, data refresh, and scalability for exchanging messages among the nodes. Moreover, preventing the message from repeating.

Due to the rapid development of technology in all fields, especially data security, the enemy is constantly trying to penetrate the network to understand the content of the message and modify it by planting illegal nodes in the network.

The proposed scheme utilizes public key concepts, which operate as a one-way function via encryption/decryption messages based on creating a data sequence and a checksum algorithm, which solves all previous problems.

The following parts will go over the specifics of this topic. Section 2 summarizes numerous distinct algorithms that have recently been built based on earlier literature reviews. Section 3 demonstrates the aims of cryptography and provides an in-depth discussion of the proposed technique. The section discusses the proposed algorithm's security characteristics as well as the analysis of threats. 4. Finally, section 5 includes detailed conclusions of this research paper.

2. LITERATURE VIEW

WSNs are more vulnerable than wired networks due to their transmission nature and restricted resources. Also, security and privacy are critical concerns in every network [13]. Moreover, the WSN is made up of a large number of sensor nodes that are deployed randomly in hostile, unattended environments [14]. Sensor networks operate along with sensitive data, which increases security problems since they are not located remotely [13].

The authors in [15] propose an efficient and secure message transmission scheme in a static WSN that combines the sequence algorithm with the Diffie-Hellman DH in-stream ciphering for encrypting messages. This scheme includes seven phases: Initialization, Node distribution, cluster forming, creating a shared key, Secure data transmission, node removal, and updating the shared key. In this scheme, when two nodes exchange messages in the network, the sender converts each message letter to ASCII values and then applies the sequence algorithm to this result. The scheme is based on the DH key exchange such that it establishes a shared key to be used between a CH and nodes in a specific cluster or BS and directly exchanges it with each other over an insecure communication channel. Then, combine the output value with this shared key. In the end, the result is concatenated with the ID of the sender and receiver. The authors produce a lightweight scheme, but the shared key is valid for a limited time [15]; Therefore, this scheme doesn't achieve security goals [16]. Also, the eavesdropping attack and man in the middle can break the algorithm [15].

Samer et al. [5] use a novel decentralized key management scheme for hierarchical grid-organized WSNs. The scheme target decreases the number of cryptographic keys saved in sensor nodes. The performance analysis demonstrates the suggested protocol's effectiveness for communication overhead, storage expenses, and network connectivity. This scheme divides the work area into equal-sized grids. The network includes the BS, master node, and L. Each grid comprises a manually positioned master node named Grid Head (GH), which has more resources and capabilities than L. This scheme contains Intra-Grid, the communication between GH and L in the same grid by shared key, whereas

inter-grid is the communication between two GH in adjacent grids. Moreover, L_i can communicate with BS and L_j through GH using a local shared key. Each GH_i should share a secret GHj key in neighboring grids. This scheme is divided into rows and columns, and the BS distributes a group of secret keys to GHs who lie in its row, and the letters share the keys among GHs to produce row and column-wise group keys. Each sensor node saves a chain of Np pair-wise keys to ensure that two nodes are connected with a probability of p using DH. The scheme provides reasonable communication overhead, storage cost, and network connectivity, but these nodes use their keys repeatedly [5], so the security will be compromised [16], and the scheme will be hacked.

Rishabh K. and Priyanka A. [17] present an improved matrix-based key management system. The author enhances the Blom algorithm, which relies on maximum area, and they divide the area into hexagonal regions called R and split sensor nodes into *r* groups with a symmetric matrix. Besides, every two nodes create a pair-wise key once they receive a matrix. After that, the nodes share the key and generate the secret key. Furthermore, the nodes remove the shared key to keep the storage space and provide network connectivity. This scheme misses the security, making the network vulnerable to attacks [16].

Vaishali and Jaydeep [9] proposed key management based on cluster forming. The authors improved the session key by updating it occasionally within the cluster. The network consists of static CH and mobile standard sensors around each CH, and the typical sensor (SN) communicates with the CH only. Moreover, the SNs dynamically elect their CH in each round and transmit their messages via the CH. This scheme enhances the ESKM [18] , where the BS preloads the secret key K1 into CHs and SN, and is used for cluster forming. After the cluster forming finishes, the K1 is deleted from CH's, SN's, and BS. Also, the BS generates a global key KG and sends it to each CH and SN. Moreover, when the session key establishment begins, the SNs request their CHs for session key $SN_i \rightarrow CH_i: \{id_{SNi}, id_{CHi} | E_{KG}(M|N) | MAC_{KG}(M|N|N')\}$ where E_{KP} is encryption using KP, M is the message, MAC_{KG} is message authentication using KG, N is Nonce from sensor nodes, N' is Nonce generated by CH, and id is the identity. Besides, each CH verifies the coming messages from SNs within its cluster through MAC, and if it succeeds, the CH sends a message M to BS containing a list of id_{SNS} $CH_i \rightarrow BS: \{idCHi | E_{KG}(M | id_{list} | N, N') | MAC_{KG}(M|N|N')\}$. Furthermore, the BS verifies the message; if it succeeds, it generates Key Session (KS_i) and hashes it. The BS unicasts KS to each CH in the network $BS \rightarrow CH_i: \{id_{CHi}, id_{SNi} | E_{KG}(KS_j | M | N' | E_{KG}(KS_i | M) | MAC_{KG}(M|N|N')\}$. As well as, each CH is responsible for distributing the KS to each SN within its cluster $CH_i \rightarrow SN_i: \{id_{CHi}, id_{SNi} | E_{KG}(M|N | KSi) | MAC_{KG}(M|N)\}$. After that, each SN verifies the MAC and then stores the shared key KS, and the KS will be used to transmit data, for example, $SN_2 \rightarrow CH_1: \{id_{SN2}, id_{CH1} | E_{KS\text{-}SN2}(M|N)) | MAC_{KS\text{-}SN2}(M|N)\}$, where M is the sense data. Moreover, the ESKM and EESKM schemes change the shared key periodically in the update key phase, where the KS is valid for a specific time interval. Through this period, the KS in the SN_2 messages to CH_1 will be repeated; therefore, security will be absent in EK [16]. Furthermore, ESKM is still scalable [9], and the EESKM scheme offers efficiency in terms of energy consumption [9].

Anzani et al. [19] offer a hybrid key pre-distribution method based on the symmetric key. They merge the blocks of symmetry to generate key rings. Furthermore, the BS generates the key ring in a pool *PK* with size ($v=q^2+q+1$), where *q* is a large prime number and $q^2+q+1<N$ the number of nodes in the network, number of key-ring is q^2+q+1, size of key-ring is $q+1$, and each key appear in $r=q+1$ key-rings which preloaded before deployment in each node in the network by the BS. Moreover, this scheme is based on SBIBD ($q^2+q+1, q+1, 1$). The BS through SBIBD generates B blocks as a subset of *A,* and each of them contains *k* size of objects in each block, and H sets, which are subsets of *A* before deployment, also contain *k* size of objects in each block. The BS randomly shares blocks of B and H for each node [19]. Finally, the two nodes exchange their key-ring, which merges B and H to get a shared key between them and communicate directly. Or, they communicate indirectly through another node by establishing a key path. The authors improve the connectivity and resilience inversely based on pool size [19]. This scheme does the cluster forming of the network. Also, the adding and revoking nodes are absent to complete this scheme.

The authors in [20] provide an Attack Matrix (AM) to determine an attack coefficient for each sensor node, indicating its susceptibility. Based on these considerations, route key generation avoids high-risk nodes to minimise exposure.

Integrating node-risk awareness with path selection improves current random key distribution systems. Security evaluation reveals adversaries recover keys less frequently after node acquisition than baseline methods. The study found that path-key security is improved in large-scale WSN deployments when the attack matrix represents node vulnerabilities. Secure measures may fail to respond effectively to dynamic attackers. Additionally, during key establishment, it might hinder network startup.

3. PROPOSED SCHEME

The proposed scheme is based on the sequence algorithm and the DH key. Moreover, it generates key chains that send data sensed by sensor nodes to the base station BS through cluster heads CHs in a way that is never repeated according to algorithms 1 and 2. Also, the proposed scheme consists of pre-distribution, cluster forming, data exchange, update, add, and revoke phases as follows:

3.1 Pre-Distribution Phase

The proposed scheme comprises BS, mobile cluster head CH, and mobile normal sensor nodes S. In this phase, the BS preloads each CH and S with a random secret key K_S, a prime number as a private number, a generator, and a module, which are DH parameters. Moreover, Q_{BS} is stored in each CH for communication with it and includes the following assumption:

1- BS is assumed to be secure, saved in a trusted area, can communicate with all CHs and Ss, and is equipped with intrusion detection [21]
2- CH has more capabilities in terms of memory capacity, process computation, and energy, and it has a unique identity, IDCH, for communicating with each other.
3- Normal sensor node S_i is a restricted resource. Both S_i and CH_i are equipped with solar cells to save energy.
4- BS maintains a blocklist containing a list of compromised nodes with their addresses through intrusion detection.

3.2 Cluster forming phase:

After deployment, each node generates a public key, Q_{CH}, Q_S. After that, the CH broadcasts its public key to each sensor node to create the cluster according to *equ1*. Each node that receives the CH broadcast message chooses the strong signal and decrypts it using K_S to get the Q_{CH} by taking the $Q_{CH\text{-receiver}}$ and adding it with K_s, which tampered with its memory if the new result equalled to $(Q_{CH}+K_S)_{receiver}$; it saves the Q_{CH} otherwise its rejects the message and compare with the following strong broadcast message and deletes other messages. Then, S_i computes the share key $K_{SH\text{-}CH,S}$. Besides, the S_i sends their public key Q_S to select CH by *equ2*. The CH decrypts S_i messages using the K_S, gains the QS, and computes the shared key K_{SH}.

$CH_i \rightarrow *$: $\{Q_{CH}, Q_{CH}+K_S\}$ ..... *equ1*.
$S_i \rightarrow CH_i$: $\{Q_{Si}, Q_{Si}+K_S\}$ ..... *equ2*.

The far sensor establishes a key path through another node that selects CH through *equ3*. After, the far sensor S_b decrypts Q_{Sa} and then calculates the agreement shared key $K_{SHb,a}$. Moreover, S_a decrypts the $Q_{Sb,}$ which is sent via equ4, and each Sa and Sb saves Q from each other and computes KSH-a and $_b$. At the end of the cluster, the CH creates a list of members Q and sends it to BS for checking the intruder. If no intruder exists, the Q_{BS} is sent to each CH according to *equ4*. In the final, the S_a forwards the message to the selected CH, and the latter saves Q_{Sb}.

$S_a \rightarrow S_b$: $\{Q_{Sa}, Q_{Sa}+K_S\}$ ..... *equ3*.
$S_b \rightarrow S_a$: $\{Q_{Sb}, Q_{Sb}+K_S\}$ ..... *equ4*.

Each CH communicates with others by *equ5*, where each of them has the IDs of others. Besides, the CH_b checks the ID_{CHa}, adds it with $Q_{CHa,}$ and then equates the result with received $(Q_{CHa}+ ID_{CHa})$. If true, CH_b will save the Q_{CHa} and compute the agreement shared key $K_{SH\text{-}CHa,b}$ used in another phase. On the other hand, CH_b sends its Q_{CHb} according to *equ6*, and it saves Q_{CHa} and $K_{SH\text{-}CHb,a}$.

$CH_a \rightarrow CH_b$: $\{ID_{CHa}, Q_{CHa}+ ID_{CHa}\}$ ..... *equ5*.
$CH_b \rightarrow CH_a$: $\{ID_{CHb,}, Q_{CHb}+ ID_{CHb}\}$ ..... *equ6*.

The Cluster Head computes agreement shared key $K_{SH\text{-}CH,BS}$ between itself and BS through Q_{BS}, preloaded in their in-pre-distribution phase.

After cluster forming is complete, each sensor function senses data, encrypted it, and sends it through selected CH by algorithm 1.

Algorithm1 Encryption Data

- Begin
- Define *n* is an integer number, *b* is a binary bit.
- b_i= convert the M to binary based on ASCII, where M is the data sense.

- Create vector v [J_i]. where is J_i a sequence, (J_i = 1, n_1, n_2, n_3… n_m), where, $n,m,i \in \mathbb{Z}$, and m is the length of the binary bit string.
- M_i= i_1, i_2, i_3…b_m. where M is the message and ($1 \leq i \leq m$).
- The initial cumulative for each sequence is as follows:
  $M_k = \sum_{i=1}^{m} J_i M_i$
- The value of M_i is replaced by its equivalent M_K.
- Final Message M_F= {$Q_{sender}||b \oplus K_{SH}||$checksum($M_k$,$K_{SH}$)}
- Increment $K_{SH.}$
- End.

Algorithm2 Decryption Data

- Begin
- Receiving the message M_F =($Q_{sender}||b \oplus K_{SH}||$checksum($M_k$,$K_{SH}$)
- Q_{sender_receiv} , d= $b \oplus K_{SH}$, c=checksum(M_k,K_{SH})
- If(Q_{sender} = Q_{sender_receiv})
  - Begin
  - compute b_{new}=($d \oplus K_{SH}$)
  - m = length of b_{new} , Create vector v [J_i]. where is J_i a sequence, (Ji = 1, n_1, n_2, n_3… n_m).
  - The initial cumulative for each sequence is as follows:
    $M_{k\_new} = \sum_{i=1}^{m} J_i M_i$
  - The value of M_i is replaced by its equivalent M_{K_new}.
  - c' = checksum(M_{k_new},K_{SH}).
  - if (c'=c)
  - convert b_{new} into character, and save it.
  - K_{SH} ++, timestamp
  - Else discard message
  - End if
- End

3.3 Update And Add/Revoke Node Phase:

The sensor nodes are usually scattered in uncontrolled areas, and to increase the efficiency of our algorithm, we need to consider capture node attacks. After each move, the BS generates a new series' seed key n and sends it to the CH_i. Moreover, each CH sends it to the cluster's members to generate a new vector X_i. Furthermore, Q and K_{SH} will be removed, and a new cluster will be created.

The new node is preloaded with a random secret key K_S, a prime number as a private number, a generator, and a module of DH. Wait to move the sensors to join the network. Moreover, when the node is idle for any reason in the update phase, this node will be removed.

4. RESULTS AND DISCUSSION

After deploying the nodes and completing the network formation process, then analyzing the results, it was found that the proposed scheme meets the security requirements: (data integrity, authentication, confidentiality, freshness and availability), efficiency, overhead, memory usage and scalability, as shown in Table 1.

Besides, the final encrypted message consists of the sender's public key Q, the XOR of the data sequence and K_{sh}, and the checksum. Each part will be verified separately in the proposed scheme at the receiving node to achieve integrity, and the Q_{sender} sends each message with a time stamp to authenticate the message. Furthermore, the message is encrypted to keep it ambiguous, and the shared key will be changed after each message, ensuring the message's freshness and preventing repetition. The nodes are also available because they are equipped with a solar battery. Moreover, the network is dynamic; if some nodes are not connected in one stage or another, they will connect. There is the ability to add nodes to the network, which makes it scalable.

Finally, the proposed scheme is programmed using Visual Studio 2017, as shown in Figure 1; the encryption/decryption takes the same steps, not reverting to save memory space and time. It is better than [6],[3] in [22] in terms of time consumption for encrypting and decrypting, as shown in Figure 2. In encryption, the proposed scheme takes 36.7 μs, where [6] takes 318.5 μs, [3] takes 57.2 μs and 139.1 μs [22]. And in decryption, the proposed scheme takes 56.9 μs, [6] 426.6 μs, [3] takes 89.5 μs and 182.6 μs [22] in which clarify in Figure 2.

5. CONCLUSION

Since wireless sensor networks are resource-constrained due to their small size, building a network that meets security requirements and extends the network's lifetime and efficiency at the lowest cost is a crucial area of study. Managing and distributing keys to build a

network is a difficult challenge in uncontrolled areas. The proposed scheme introduces a mobile network, which changes the network form periodically to avoid key repetition. And it is based on public key concepts, which operate as a one-way function and variable data sequence, with the checksum providing security requirements (integrity, authentication, confidentiality, data refresh, and scalability) compared with other schemes. Also, the consumption time of encryption/decryption is acceptable compared to other algorithms. Compared with different schemes, the proposed scheme balances complexity and limited sensor resources, providing adaptive, efficient, and extended network lifetime.

REFERENCES

[1] KOLLI L. K., & LALITHA S. K., "ROBUST AND EFFICIENT SUPPLY CHAIN MANAGEMENT USING IMPROVED PROOF OF USEFUL WORK (POUW) CONSENSUS ALGORITHM," *Journal of Theoretical and Applied Information Technology,* vol. 103, no. 9, pp. 3748-3766, 2025,May.

[2] Jondhale, S. R., Maheswar, R., & Lloret, J., "Fundamentals of wireless sensor networks," in *Received Signal Strength Based Target Localization and Tracking Using Wireless Sensor Networks*, Cham: Springer International Publishing, 2021, July, pp. 1-19.

[3] Albakri, Ashwag; Harn, Lein; Gope, Prosanta…[et al.], "Hierarchical Key Management Scheme with Probabilistic Security in a Wireless Sensor Network (WSN)," *Security and Communication Networks, Hindawi,* pp. 1-11, 2019.

[4] Roy, M., Chowdhury, C., & Aslam, N., "Security and privacy issues in wireless sensor and body area networks," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, Cham: Springer International Publishing, 2021, January, pp. 173-200.

[5] Khasawneh, S., Chang, Z., Liu, R., Kadoch, M., & Lu, J., "A Decentralized Hierarchical Key Management Scheme for Grid-Organized Wireless Sensor Networks (DHKM)," in *International Wireless Communications and Mobile Computing (IWCMC),IEEE*, 2020, June.

[6] E. H. Aziz, "Two Stage Text Encryption Using a Private Table of the Sumerian System," *Kirkuk University Journal for Scientific Studies,* vol. 15, no. 1, pp. 18-33, 2020,January.

[7] MANGALAMPALLI K S M. ,& KUNJAM N. R., "PERFORMANCE ANALYSIS OF THF: A NOVEL LIGHTWEIGHT CRYPTOGRAPHY HASH FUNCTION," *Journal of Theoretical and Applied Information Technology,* vol. 103, no. 9, pp. 3767-3777, 2025, May.

[8] BADDU N. B , MANAM R. , SIMHADRI M. , SRIKANTH K. , MADAMANCHI B. , BEZAWADA M. ,& MURALIDHAR V, "CYBERATTACK PREVENTION AND DETECTION IN SMART POWER SYSTEMS USING DEEP LEARNING," *Journal of Theoretical and Applied Information Technology,* vol. 103, no. 9, pp. 3934-3944, 2025,May.

[9] Diop, A., Qi, Y., & Wang, Q., "An Efficient and Secure Session Key Management Scheme For Cluster Based Wireless sensor Network,," in *IEEE International Advance Computing Conference (IACC)*, 2015,December.

[10] Abd El-mawla, N., Badawy, M., & Arafat, H., "Security And Key Management Challenges Over Wsn (ASurvey)," *International Journal of Computer Science & Engineering Survey (IJCSES),* vol. 10, no. 1, pp. 15-34, 2019,February.

[11] Abualghanam, O. R. I. E. B., Qatawneh, M. O. H. A. M. M. A. D., & Almobaideen, W. E. S. A. M., "A survey of key distribution in the context of internet of things.," *Journal of Theoretical and Applied Information Technology, ,* vol. 97, no. 22, pp. 3217-3241., 2019, November.

[12] Haj Seyyed Javadi, H., & Babaei, A., "Key Pre-Distribution Scheme: Enhanced Security in Distributed Systems," *International Journal of Knowledge*

Processing Studies, vol. 5, no. 1, pp. 78-89, 2025,March.

[13] Pandey, S., & Kumar, R., "Study of Routing Protocol Using Key Management in Wireless Sensor Network," in *Proceedings of the Second International Conference on Computing Methodologies and Communication (ICCMC), IEEE*, 2018,February.

[14] Jerbi, W., Guermazi, A., Trabelsi, H., "O-LEACH of routing protocol for wireless sensor networks.," in *In 2016 13th international conference on computer graphics, imaging and visualization (CGiV),IEEE*, 2016.

[15] Ameen, K. A., Mahmood, B. A., & Taher, Y. N. A., "Secure message transmission scheme in wireless sensor," *Bulletin of Electrical Engineering and Informatics,* vol. 10, no. 3, p. 1514~1523, 2021,June.

[16] Curley, R. (Ed.), Cryptography: Cracking Codes, Britanncia Educational Publishing, 2013,June.

[17] Rishabh K. and Priyanka A., "Improved matrix based Key Management Scheme for Wireless Sensor Network security," in *2nd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), IEEE*, 2019.

[18] Kumar, E. K., & Lakhan, R., "Performance and Accuracy Enhancement of Cloud Environment During Precision Agriculture.," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* vol. 10, no. 4, pp. 1-8, 2024,June.

[19] Anzani, M., Haj Seyyed Javadi, H., & Modirir, V., "Key-management scheme for wireless sensor networks based on merging blocks of symmetric design," *Springer,* vol. 24, no. 8, p. 2867–2879, 2018,Novemebr.

[20] Ahlawat, P., & Dave, M., "Secure Path Key Establishment Schemes Based on Random Key Management for WSN," *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences, springer,* vol. 91, pp. 1-13, 2020,September.

[21] Pandey, V. K., Prakash, S., Gupta, T. K., Yang, T., Singh, A., & Rathore, R. S., "A computational intelligence inspired framework for intrusion detection in WSN," *International Conference on Decision Aid Sciences and Applications (DASA) IEEE.*, 2024, December.

[22] Taher, Y. N. A., Ameen, K. A., &Fakhrudeen, A. M., "An efficient hybrid technique for message encryption using caesar cipher and deoxyribonucleic acid steganography," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 28, no. 1, pp. 1096-1104, 2022,Novemeber.

[23] Kumar, V., Malik, N., Dhiman, G., & Lohani, T. K., "Scalable and Storage Efficient Dynamic Key Management," *Wireless Communications and Mobile Computing, Hindawi,* vol. 2021, pp. 1-11, 2021.

[24] Dinker, A. G., & Sharma, V. , "Trivariate Polynomial Based Key Management Scheme (TPB-KMS) in Hierarchical Wireless Sensor Networks," *In Ambient Communications and Computer Systems,springer,* pp. 283-290, 2018.

[25] Chatterjee, K., De, A., &Gupta, D., "A Secure and Efficient Authentication Protocol in Wireless Sensor Network," *Wireless Personal Communications, Springer,* vol. 81, no. 1, pp. 17-37, 2015,March.

[26] Iqbal, J., ul Amin, N., Umar, A. I., & Din, N., "Efficient Key Agreement and Nodes Authentication Scheme for Body Sensor Networks," *International Journal Of Advanced Computer Science And Applications,* vol. 8, no. 7, pp. 180-187, 2017.

Journal of Theoretical and Applied Information Technology
30th September 2025. Vol.103. No.18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Comparative Between Different Key Management Schemes And Proposed Scheme

Scheme	Security	Efficiency	Overhead	Memory Usage	Scalability	Mobile
[3]	Less	No	Less	Less	Yes	No
[5]	Less	Yes	Less	High	Yes	No
[9]	Less	Yes	Less	Less	No	Yes
[15]	Less	Yes	Less	Less	No	No
[17]	Less	Yes	Less	No	Yes	No
[19]	Yes	Yes	Yes	High	No	No
[20]	Less	NO	Yes	High	No	No
[23]	Less	Yes	Less	Less	No	No
[24]	Less	No	Less	High	Yes	No
[25]	Yes	No	Yes	High	Yes	No
[26]	Less	Yes	Less	Less	No	No
Proposed Scheme	Yes	Yes	Less	Less	Yes	Yes

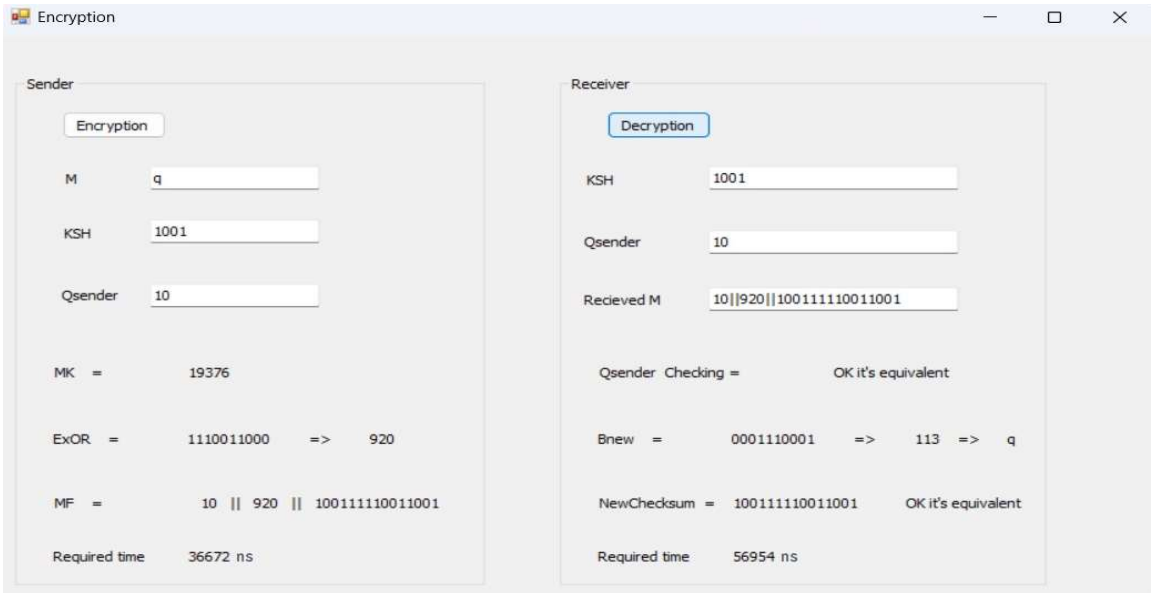

Figure 1. Encryption And Decryption Data Of Proposed Algorithm

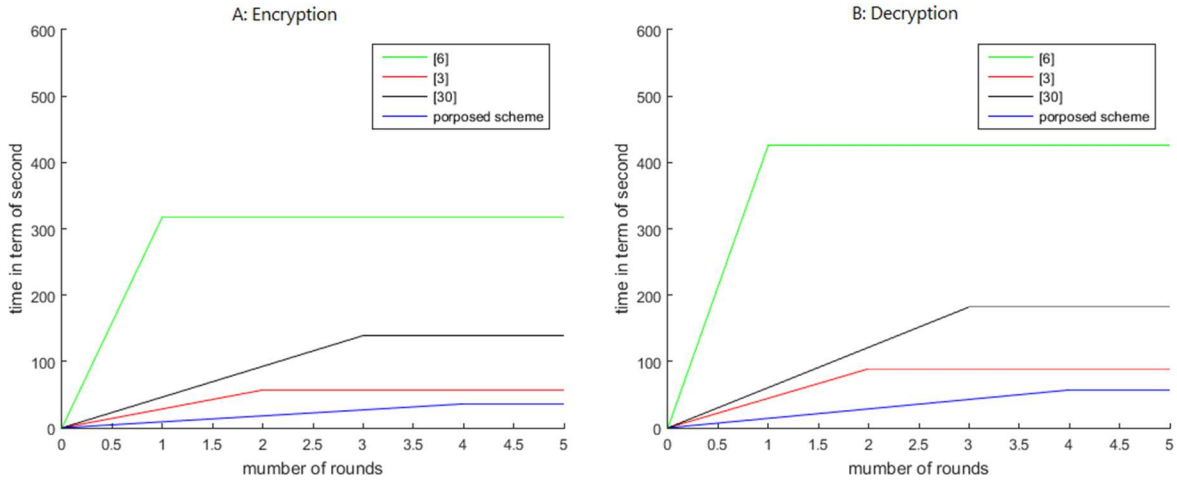

Figure 2. Comparison In Term Of Time Consumption A: Encryption B: Decryption