Encryption of a Message by HillAli Cipher and Security of Routing Path by DSR in Wireless Sensor Network

Haneen Mohammed Hussein, Ali Qasim Hanoon, and Afrah Thamer Abdullah

Original scientific article

***Abstract*—A Wireless Sensor Network (WSN) is a collection of sensors that communicate or track a specific object. It is used in many fields of war, architecture, or espionage, but the wireless sensor network faces challenges in securing the path or the message, which is one of the most important problems to address through the routing process, this paper proposes using Dynamic Source Routing (DSR), which saves the path of message transmission and detects any compromised node to make a strong security process for the sent message or alert. It works by encrypting and decrypting the message. It mixes two ciphers, the Hill and Ali ciphers, which have been enhanced by incorporating a 4 * 4 matrix and supporting 2×2 and 3×3 matrices. The other cipher is the Ali cipher, as it depends on the use of the location of the letters in the message sent and the alphabet, generating a new hybrid cipher, the HillAli cipher.**

***Index terms*—WSN, DSR, Matrix, Cipher, Hill cipher, Sensor, Message, Encryption, Decryption, Ali cipher, Applications.**

I. Introduction

The growing reliance on the Internet by humanity, particularly in various sectors, has made it essential to focus on protecting data packets from attacks [1]. A wireless sensor network (WSN) is a group of nodes or sensors that transmit data within their specialized environment. WSNs may detect various physical events, such as the movement of vehicles or living beings within their surroundings or the early identification of forest fires. A wireless sensor network (WSN) assists in providing its operator with precise and up-to-date information derived directly from their surroundings [2].

Wireless connections connect the sensors without the requirement of any special infrastructure, as shown in Figure 1. The sensitive nodes have an integrated sensor, memory, CPU, wireless transmitter, and receiver, as well as a power supply. The wireless sensor design has the potential to improve miner and operator safety and health monitoring. [3].

Manuscript received January 27, 2025; revised February 17, 2025. Date of publication May 21, 2025. Date of current version May 21, 2025. The associate editor prof. Toni Perković has been coordinating the review of this manuscript and approved it for publication.

H. M. Hussein and A. T. Abdullah are with the Division of Construction and Projects, Mustansiriyah University, Baghdad, Iraq. (e-mails: haneen.mh@uomustansiriyah.edu.iq, afrah.thamer@uomustansiriyah.edu.iq).

A. Q. Hanoon is with the Qand Company, Baghdad, Iraq. (e-mail: aliqasimhanoon@gmail.com).

Digital Object Identifier (DOI): 10.24138/jcomss-2024-0116

Security is an issue with wireless sensor networks (WSNs) since they are more subject to external assaults by hackers because of the ease with which they may enter a false node between nodes, such as a black hole attack, grey hole attack, and wormhole attack. When an attacker strikes, it usually impacts packet transmission by changing the data or stopping the data from reaching the node or destination, lowering its throughput. The key issue with WSN is data security, as it is easy to obtain and exploit. WSN security is important, and the MAC layer is crucial in maintaining it [4].

Routing must be for wireless sensor networks (WSNs), which is the foundation for the network's work to send and receive alert messages, where the routing represents the process of choosing the path for the transmission of these messages within the environment or any other network, meaning that the routing is required in any communication process because it helps to facilitate communications, which is the most important means of communication as shown in Fig. 1 that sensor nodes (blue circles) collect data and send it through a network to a sink node (red block). The sink sends the data to the internet, where it can be accessed by a user (shown as a monitor). The path (red arrow) shows how the data moves from the sensors to the sink.

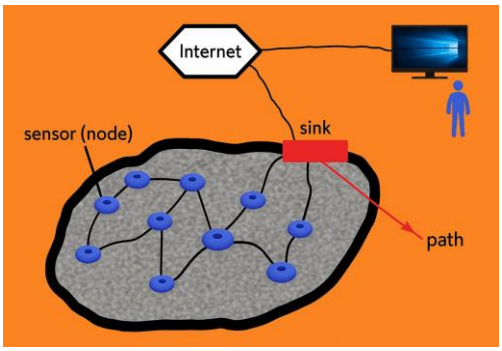

Fig. 1. Structure WSN

Dynamic source routing (DSR) is a reactive routing protocol that assists in identifying the source by connecting each device in the network on a full path from source to destination, as it works to make a route request (RREQ) and return the path (RREP). One of its advantages is that it has a high throughput. DSR is one such good protocol since it requires numerous network hops for a node to share data with another node across networks [5].

The primary objective of security and encryption is to secure secret communications and to guarantee that information is concealed from everyone except the person who wishes to communicate it to him and who can decipher the code. The Hill cipher was developed as one of the classic kinds of encryption to use in WSN. It is possible to accomplish the process of sharing alerts or messages between two nodes in general, as well as authentication using encryption, which is utilized to address security issues in the message exchange.[6]

To achieve the criteria of securely encrypting communication within the environment, information encryption is required. To secure the message, a procedure of encrypting and decrypting the message is required. Encryption is the process of transforming sensitive data into encrypted text that the unauthorized party or third party cannot understand or identify. When arrives, the authorized person decrypts the encrypted communication. This work-shifting process increases encryption strength. Providing security for the transmission of a message or alert between nodes is critical, this paper is to be concentrated throughout. The applications for wireless sensor networks include a wide range of fields, such as weather and environmental monitoring, health monitoring, safety inspections of buildings and facilities, and security features, including intrusion detection, entry into restricted areas, and traffic and fire detection. These applications are primarily concerned with the remote monitoring and control of various sensory (or physical) events such as temperature, pressure, light, sound, and so on, via Sensors in tiny wireless devices that acquire and collect sensitive information in the observed area. The information is then cooperatively and wirelessly sent from one device to another to a monitoring station, a computer that gathers, processes, and analyzes information from the scattered wireless sensors as shown in Fig. 2 that wireless sensor network where sensor nodes send data to a monitoring station via connected paths.

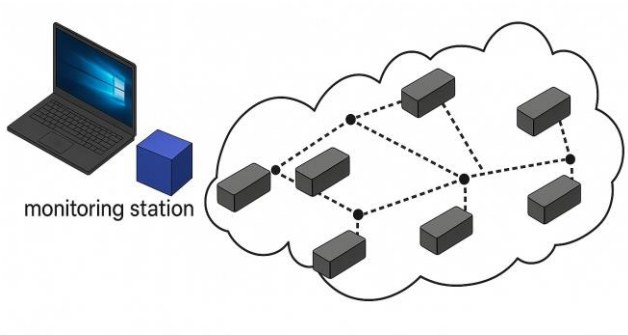

Fig. 2. Monitoring process

This paper makes significant contributions to addressing critical security challenges in Wireless Sensor Networks (WSNs) by proposing innovative solutions. Foremost among these is the introduction of a novel encryption algorithm, named the HillAli cipher, which combines the mathematical strength of the Hill cipher with the positional encoding advantages of the Ali cipher. This hybrid approach enhances security by incorporating flexible matrix sizes (2×2, 3×3, and 4×4) and adaptive character positioning, making it robust against various cryptographic attacks.

Additionally, a secure message transfer system is developed to address the growing threats posed by quantum computing. The HillAli cipher employs advanced multi-layered encryption techniques, utilizing dynamic key generation strategies that effectively counter quantum decryption algorithms such as Shor's algorithm.

The proposed system ensures both the confidentiality and integrity of transmitted data while enhancing the overall routing process through seamless integration with Dynamic Source Routing (DSR). This integration not only protects sensitive information but also maintains efficient communication pathways within WSNs. The approach is especially advantageous for applications in critical domains such as military operations, espionage, and architecture, where secure and reliable data transmission is vital. Comprehensive theoretical analyses and practical evaluations validate the effectiveness of the HillAli cipher in mitigating security risks, marking it as a significant advancement in secure communication systems.

The remainder of the paper is structured as follows: Section II reviews related work, summarizing prior studies and their contributions to the field. Section III defines the information security goals, outlining the objectives and requirements for securing WSNs. Section IV details the proposed methodology, describing the design and implementation of the HillAli cipher and its integration into secure message transfer systems. Section V presents the results and analysis, showcasing the performance evaluation and security effectiveness of the proposed cipher. Finally, Section VI concludes the paper, summarizing the findings and suggesting directions for future research.

II. Related Work

Kandris and Anastasiadis (2024) and Jaiswal and Dwivedi (2023) both addressed Wireless Sensor Networks (WSNs), focusing on the challenges of energy efficiency and security. Kandris and Anastasiadis highlight WSN applications in fields such as healthcare and explore future research, while Jaiswal and Dwivedi concentrate on technical aspects like network protocols and solutions, including encryption and key management. In a similar vein, Fatma H. El-Fouly et al. (2024) presented a real-time routing algorithm for WSNs that enhances energy efficiency and ensures timely data delivery. Their algorithm selects relay nodes based on factors like link quality, buffer size, and energy consumption, resulting in improved packet delivery, network lifetime, and end-to-end delay, making it well-suited for delay-sensitive applications [7-9].

Ahmed Waleed Khalil Al-Nasir and Foad Salem Mubarak (2024) demonstrated that AODV outperforms DSDV and DSR in high-mobility VANET environments, while Eawar Patnala and Srinivasa Rao Giduturi (2023) introduced a Hybrid DSR technique aimed at improving routing efficiency and security in MANETs by reducing latency and enhancing throughput and energy consumption. Similarly, K. Sathish et al. (2022) explored the underwater environment using a network of wireless sensors and compared several routing protocols, including Zone Routing Protocol (ZRP), Dynamic Source Routing Protocol (DSR), and AODV, to assess their performance. All studies focus on optimizing routing protocols

for better performance in dynamic and challenging network environments [10-12].

Samsul Arifin et al. (2024), G. Rekha and V. Srinivas (2023), Rajaa K. Hasoun et al. (2021), and Nana and Prasetyo (2021) presented advancements in encryption techniques aimed at enhancing cryptographic security. Arifin et al. combine the Unimodular Hill Cipher with RSA encryption, using matrix operations for character randomization and RSA for public key encryption, significantly improving security and efficiency for text data. Rekha and Srinivas introduced the "Block Hill Cipher," which encrypts blocks of characters, expanding the key space and improving resistance to statistical attacks. Similarly, Hasoun et al. developed a Hill cipher method incorporating encryption, decryption, and RSA, while Nana and Prasetyo implemented the Hill cipher with a 3x3x3 Rubik's Cube approach. All studies highlight how their modifications contribute to stronger cryptographic security for modern digital environments [13-16].

Sung-Jung Hsiao and Wen-Tsai Sung, 2021. Used blockchain-powered technology to enhance data security in wireless sensor networks to make the reliability of data transmission strong. They made an initial data collection node called a mobile database, used the Merkel tree algorithm to make it difficult to manipulate the blockchain with encryption techniques, and also used a private key of 256-bit public keys of 65 bytes and hash keys of 20 bytes. [17].

Zhang Huanan and et al, 2021. emphasized the security and application of wireless sensor networks by monitoring and controlling WSNs to avoid attacks and manage the key [18]. Uras Panahi and Cuneyt Bayilmis,2022. Utilized the reserved bits of the control field in the Zigbee MAC header, as well as algorithm combinations with AES, and employed a security method that considers the application, security level, and the bit error rate of wireless sensor networks to ensure data security [19]. Sudha D., Kathirvel A, 2022, Neoterictechniques, like HMMPayl, an Intrusion Detection System (IDS) that uses Hidden Markov Models to analyze HTTP payloads at the byte level, are increasingly employed to detect attacks with higher accuracy and fewer false positives compared to traditional methods [20].

Raksha Upadhyaya et al., 2016. Used a dynamic source routing (DSR) to prevent a distributed interruption of service (DDOS) attack [21]. A. A. Zaidan and et al, 2003. Submerged the information within the EXE file. Through the encryption technology [22]. Han-Yu Lin and Yan-Ru Jiang, 2020. Improved multi-user CP-ABE scheme with the functionality of keyword search, which enables data users to seek specific ciphertext in the cloud server by using a specific keyword [23].

Mobile Ad Hoc Networks (MANETs) facing challenges like routing, security, and energy efficiency, with applications in military, emergency, and vehicular networks [24- 28]. J.S.Jolin and et al. (2024), presented a secure and efficient two-factor authentication method using a virtual smart card for MANETs. The scheme supports password reset, uses hash functions for key sharing, and resists various attacks[29].

Kathirvel Ayyaswamy,2024, an enhanced scheduling method that leverages idle time in job clusters to reduce material consumption and overall job completion time in single-machine scheduling, assures efficiency in jointly stable and dynamic environments [30] and Naren AK,2024, viewed how using 5G technology enhances virtual event experiences with enabling high-speed data transmission, ultra-low latency [31].

Kathirvel A. and et al. (2025) in chapter 14 of the book, chapter 13 in another book for Kathirvel A. and et al. (2025) presented recent research emphasizes the increasing influence of AI technologies in education and manufacturing. In educational settings, early adopters of ChatGPT have shown positive engagement, although some concerns remain regarding its safe and responsible integration. In the manufacturing sector, robotics enhances efficiency and sustainability but also presents challenges, such as the need for workforce training and balanced collaboration between humans and machines[32], [33].

III. Information Security Goals

A. Data Confidentiality

It is to protect data from unauthorized disclosure, where to achieve the first goal of information security, we will use large encryption algorithms, but what if we use an algorithm and one of them can solve the code of this algorithm, which views the information and get a negative attack and also the possibility of a positive or effective attack by modifying a word or adding a word and changing it again to the intended destination, the original text will be lost, which is the deletion and distortion of it.

B. Data Integrity

Information safety against deception and distortion is ensuring that information is received without deception or manipulation.

C. Authentication

Not to mimic another party, which means that a firm can send communications to fund owners as if it is a well-known company since this company has impersonated well- a well-known company in the market for fraud and forgery.

D. Accountability

It means protection from denial of an event by the warmest parties to the communication, the sender and the receiver,
i.e. consider a student using an online learning platform to submit their final project. The platform automatically logs the student's login details and the time of submission, storing them along with the student's identity. If a question arises about whether the project was submitted on time, the system’s records can confirm the exact submission time, holding the student accountable and verifying the authenticity of their actions.

E. Availability

It entails providing physical and informational security to the system to avoid being exposed to something that might result in halting user service, even for a short period. The administrator must write down all of the hazards that might cause the system to fail and then begin looking for appropriate remedies.

F. Access control

It refers to something that has the authority to enter the information system, and if it does, it has the power to do so [34], [35].

IV. METHOD PROPOSED

The communication will be securely sent in two steps, with the DSR protocol determining its safe arrival. It also has two steps for determining the position and saving the path conveyed by the message. The message is also encrypted. It is divided into two stages: the application of a specific encryption algorithm and the encryption of the encrypted text.

A. Dynamic Source Routing Protocol (DSR)

It is a routing protocol, one of the interactive protocols, and it will do the following.

A.1 Determine Node

That is accomplished through the process of sending the request and replying to the request between the node (sensor) and the sink, and it also includes information about the location of previously planted nodes in the region. As shown in Fig. 3,4.

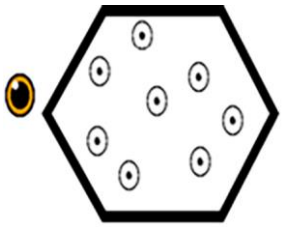

Fig. 3. Discovery nodes

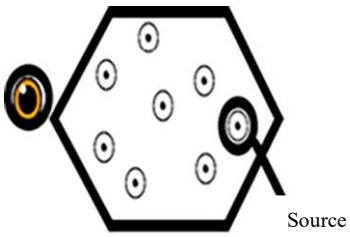

Fig. 4. Determine the node

A.2 Save Path Messages Routing

At this point, the path that the message takes between the nodes. DSR contains a temporary cache, which aids in the security and discovery of any new node within the environment because it contains all sensor information. As shown in Fig. 5.

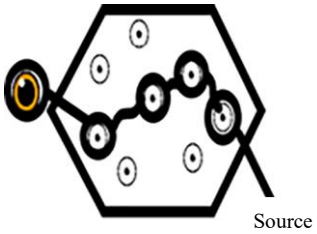

Fig. 5. Save path messages

B. Encryption

One of the most significant aspects is the process of encrypting messages with military applications, which ensures that the message or alert is safely delivered and that only the authorized person has access to it. It takes place in two stages as follows:

B.1 Encryption Using the Hill Cipher Improver

To communicate between the source and the receiver, we will use a 3 * 3 matrix as well as a more advanced key of 4* 4 and fix the key. Only the person in charge of the sensors has the authority to make modifications or updates to the keys between one period, every day, or every week.
Encryption steps:

- Set the letter table
- Set the encryption key, specify the number of characters that the encryption uses, and write the original text
- Converting each letter in the key to a numerical value and building the key matrix
- Converting each letter in the original text to a numerical value and building the original text matrix
- Multiplying the key matrix by the original text matrix
- Product of multiplication Mod 26
- The numbers in the resulting matrix are the character values of the coded text shown in Fig.6.

C. Decryption

The original message is returned through the following steps:

- Table of letters
- Use the reciprocal of the encryption key matrix,
- Determine the number of characters that encode together, and write the encrypted text
- Converting each character in the encrypted text to its numerical value and building the encrypted text matrix
- Multiplying the reciprocal of the key matrix by the ciphertext matrix
- Multiplication product Mod 26
- The numbers in the resulting array are the character values for the decoded text shown in Fig. 7.

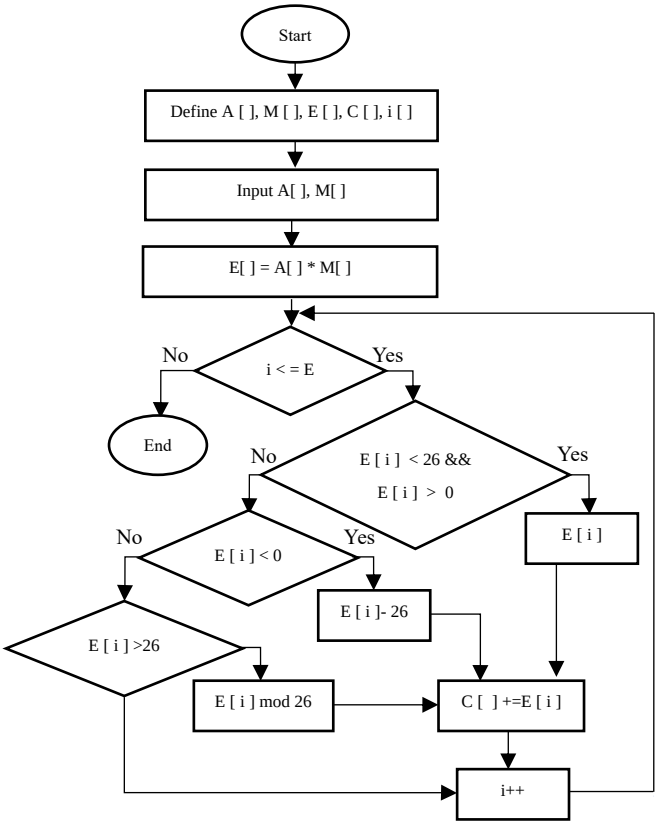

Fig. 6. Encryption

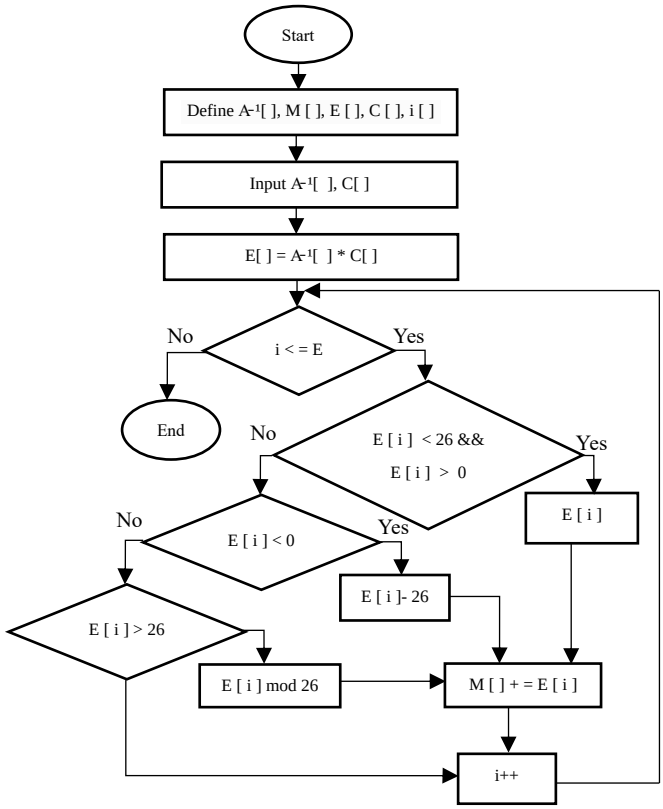

Fig. 7. Decryption

*D. Hill Cipher 3*3*

Example: Cryptography and decryption using a 3*3 matrix. For example, we have the following cipher clause: BCDCFDBAI

After giving each letter its value, we place it inside the array as 3*3 (note that the letter table starts from 0, that is, A = 0), and the shape of the array is as follows:

$$\mathrm{K} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 3 \\ 1 & 0 & 8 \end{bmatrix}$$

D.1 Encryption

Let the original text be COMPUTERS, and if it is greater than that, it is divided into blocks, each one consisting of three letters.

Put the original text inside a 3 * 3 matrix:

$$\mathrm{M} = \begin{bmatrix} C & P & E \\ O & U & R \\ M & T & S \end{bmatrix} = \begin{bmatrix} 2 & 15 & 3 \\ 14 & 20 & 3 \\ 12 & 19 & 18 \end{bmatrix}$$

Next, we do the multiplication of the two matrices, we multiply the first row of the first matrix by the column in the second matrix. We place the result in the new array. Thus, for the rest of the rows, we multiply them by the column. We take the result by the rest of the measure mod 26 as shown in Eq. (1), where C is a ciphertext, K is the encryption key, and M is the plaintext message.

$$\mathrm{C} = \mathrm{K} * \mathrm{M} \bmod 26 \tag{1}$$

$$\mathrm{C} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 3 \\ 1 & 0 & 8 \end{bmatrix} * \begin{bmatrix} 2 & 15 & 4 \\ 14 & 20 & 17 \\ 12 & 19 & 18 \end{bmatrix} \bmod 26$$

$$\mathrm{C} = \begin{bmatrix} 66 & 112 & 92 \\ 110 & 187 & 147 \\ 98 & 167 & 148 \end{bmatrix} \bmod 26$$

$$\mathrm{C} = \begin{bmatrix} 14 & 8 & 14 \\ 6 & 5 & 17 \\ 20 & 11 & 18 \end{bmatrix}$$

$$\mathrm{C} = \begin{bmatrix} O & I & O \\ G & F & R \\ U & L & S \end{bmatrix}$$

So, the output from this text, after converting these numbers into letters (with the help of a table of letters), i.e., the encoded text, is:

Text is after order: OGUIFLORS

D.2 Decryption

Decryption, all we find is the inverse of the matrix, as we have already learned (and beat him in the ciphertext taking division remains on 26), as shown in Eq. (2) where D is a text, K^{-1} is key inverse, and C is the ciphertext.

$$D = K^{-1} * C \quad (2)$$

$$C = \begin{bmatrix} 12 & 16 & 9 \\ 13 & 21 & 23 \\ 5 & 24 & 25 \end{bmatrix} * \begin{bmatrix} 14 & 8 & 14 \\ 6 & 5 & 17 \\ 20 & 11 & 18 \end{bmatrix}$$

$$= \begin{bmatrix} 444 & 275 & 602 \\ 768 & 462 & 953 \\ 714 & 435 & 928 \end{bmatrix} \text{ Mod } 26$$

$$C = \begin{bmatrix} 2 & 15 & 4 \\ 14 & 20 & 17 \\ 12 & 19 & 18 \end{bmatrix}$$

The result from this text, after converting these numbers into letters (with the help of the table of letters), i.e. the clear text is: COMPUTERS.

*E. Hill Cipher 2*2*

The equations and procedure in Hill cipher 3*3 are applied in this section with a modification of the matrix key to use 2*2, as shown in the following example.

Key: ALLI
Massage: THERE IS AN ENEMY 10 METERS AWAY
Encryption: ZFFYK EA QS TSTEM 10 SISHQT IUEK
Decryption: THERE IS AN ENEMY 10 METERS AWAY

*F. Hill Cipher 4*4*

The equations and procedure in Hill cipher 3*3 are applied in this section with a modification of the matrix key to use 4*4, as shown in the following example.

Key: QHANZTNMSCZGCOTH
Massage: DR MOHAMMED RAAD
Encryption: LU EYIHEOHO JJVFGQ
Decryption: DR MOHAMMED RAADAA

The choice of matrix size depends on the system or application requirements. Military applications that require high security typically use 4×4 matrices to achieve stronger encryption, while 3×3 matrices offer a balance between security and computational performance. 2×2 matrices provide moderate security, as shown in Table I.

TABLE I
MATRIX SIZE COMPARISON

Matrix Size	Encryption Strength	Computational Complexity	Decryption Accuracy
2×2	Weak (Easier to break)	Low (Fastest)	High (More reliable)
3×3	Moderate	Medium	Moderate
4×4	Strong (More secure)	High (More resource-intensive)	Lower (Higher risk of decryption failure)

In key selection, a square matrix (n × n) is used in the Hill cipher, where the key must be invertible (i.e., it must have an inverse). This means that the determinant, det(K), must have a modular inverse mod n, based on the chosen alphabet.

- If the English alphabet is used, then n = 26.
- If the Arabic alphabet is used, then n = 28.

The condition for invertibility is that gcd(det(K), n) = 1, ensuring that the determinant and n are coprime. Here, det() refers to the determinant, and gcd() refers to the greatest common divisor.

G. Ali Cipher

The procedure for ciphering each letter depends on both the position of the letter in the alphabet and its location within the message. Furthermore, it aids in encrypting the characters inserted during the Hill cipher, ensuring that the Hill cipher—and the message overall—cannot be easily recognized or deciphered. The Ali cipher is based on two rules: one for encrypting characters and another for encrypting integers. As in the following equations:

G.1 Encryption

- Cipher alphabet

C = The position of the character in the message + The position of the letter in the alphabet (mod26)

- Cipher number

C = number + the position of the number in the message shown in Fig.8. Convert letters to numbers shown in Table II.

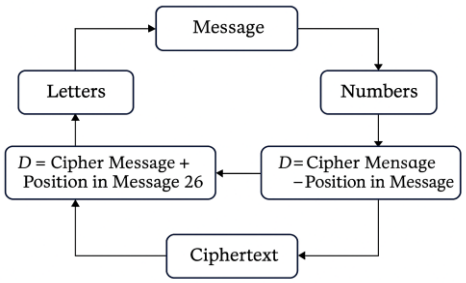

Fig. 8. Ali Cipher Encryption

TABLE II
CONVERT LETTERS TO NUMBERS

A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7	I 8	J 9	K 10	L 11	M 12
N 13	O 14	P 15	Q 16	R 17	S 18	T 19	U 20	V 21	W 22	X 23	Y 24	Z 25

This type of cipher is demonstrated by the example that follows: Text = 10 degrees.
Table III indicated that the ciphertext was 33gilxlmb.

G.2 Decryption

- Decryption alphabet

D = Cipher msg - The position of the character in the message (mod26)

- Decryption number

D = Cipher number - the position of the number in the message shown in Fig. 9.

TABLE III
THE ALI CIPHER ENCRYPTION

Character	Position in msg	Position in alp	Result(R)	R mod26	Cipher
1	1	1	2		2
0	2	0	2		2
D	3	3	6	6	G
E	4	4	8	8	I
G	5	6	11	11	L
R	6	17	23	23	X
E	7	4	11	11	L
E	8	4	12	12	M
S	9	18	27	1	B

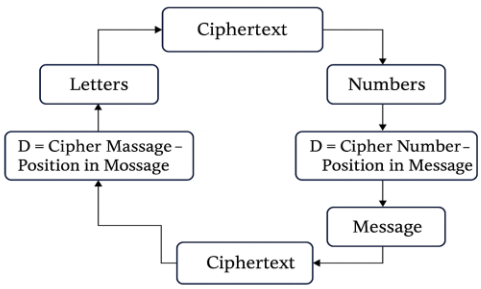

Fig. 9. Decryption

The Cipher text was 22gilxlmb, so that table IV indicated that decryption was 10 degrees.

V. RESULT

A. HillAli Algorithm

In this paper, we introduce an innovative encryption approach that synergizes two powerful ciphers -the Hill cipher and the Ali cipher- to significantly enhance data security within wireless sensor networks (WSNs). This dual-cipher technique is meticulously designed for high-stakes applications, such as military operations, critical infrastructure protection, and border surveillance, where sensitive data must be transmitted securely in response to specific events occurring near national boundaries.

Hill cipher relies on mathematical operations and transforms text into matrices, making it suitable for block cipher encryption. On the other hand, AliCipher provides an additional encryption layer that introduces extra complexity into the encrypted text, protecting it from frequency analysis attacks. By combining the matrix encryption strength of Hill cipher with AliCipher's ability to complicate attack analysis, a higher level of data security is achieved within the network.

The integration of these two ciphers fortifies the encryption process, creating a multi-layered defense mechanism that is highly resistant to unauthorized access. The encryption and decryption processes are comprehensively demonstrated in

Tables V and VI, respectively, where Table V details the step-by-step encryption using both ciphers, while Table VI outlines the corresponding decryption stages at the recipient's end. This dual-layer encryption not only strengthens the overall data security but also adds a layer of complexity, making the encrypted message exceedingly difficult to compromise.

TABLE IV
THE ALI CIPHER DECRYPTION

Cipher msg	Position in alp	Position in msg	Result(R)	R mod26	Decryption
2	2	1	1		1
2	2	2	0		0
G	6	3	3	3	D
I	8	4	4	4	E
L	11	5	6	6	G
X	23	6	17	17	R
L	11	7	4	4	E
M	12	8	4	4	E
B	1	9	-8	18	S

Moreover, this approach is designed to adapt to increasing message sizes, dynamically enhancing the encryption complexity as the data grows, thereby offering robust protection even under sophisticated attack scenarios. By merging these two ciphers, the proposed method achieves a higher level of encryption strength and ensures that sensitive communications are transmitted securely, reducing the risk of interception or unauthorized decryption. This algorithm is demonstrated by the following example.

Key: QHANZTNMSCZGCOTH
Massage: TOP SECRET FILE
Encryption Hill: MIV VARFXO AUZMWUI
Encryption Ali: NKYZFXMFXKFLZKJY
Decryption Ali: MIV VARFXO AUZMWUI
Decryption Hill: TOP SECRET FILEAAA
HillAli cipher encryption as shown in Table V and HillAli cipher decryption as shown in Table VI.

The entropy result of the ciphertext is 8.0/7.88, including that the ciphertext is difficult to analyze using traditional techniques. For instance, when one letter of the plaintext is changed, 48% of the ciphertext is altered, demonstrating the strength of the encryption.

Random tests were also conducted on the ciphertext, and the results show that it passes most of the NIST tests. This suggests that the ciphertext is sufficiently random to resist statistical analysis. Therefore, the Hill-Ali cipher exhibits high entropy, a strong diffusion effect, and excellent performance in random tests.

B. Comparison

Table VII presents a comparative analysis of various encryption methods, highlighting different configurations of the Hill cipher alongside hybrid approaches such as the Ali Cipher and the HillAli Cipher.

TABLE V
THE HILLAIL CIPHER ENCRYPTION

Character	Hill cipher 4*4	Position in msg	Position in alp	Result(R)	R mod26	Cipher HillAli
T	M	1	12	13	13	N
O	I	2	8	10	10	K
P	V	3	21	24	24	Y
S	V	4	21	25	25	Z
E	A	5	0	5	5	F
C	R	6	17	23	23	X
R	F	7	5	12	12	M
E	X	8	23	31	5	F
T	O	9	14	23	23	X
F	A	10	0	10	10	K
I	U	11	20	31	5	F
L	Z	12	25	37	11	L
E	M	13	12	25	25	Z
	W	14	22	36	10	K
	U	15	20	35	9	J
	I	16	8	24	24	Y

TABLE VI
THE ALI HILL CIPHER DECRYPTION

Cipher HillAli	Position in alp	Position in msg	Result(R)	R mod26	Character	Decryption Hill cipher 4*4
N	13	1	12	12	M	T
K	10	2	8	8	I	O
Y	24	3	21	21	V	P
Z	25	4	21	21	V	S
F	5	5	0	0	A	E
X	23	6	17	17	R	C
M	12	7	5	5	F	R
F	5	8	-3	23	X	E
X	23	9	14	14	O	T
K	10	10	0	0	A	F
F	5	11	-6	20	U	I
L	11	12	-1	25	Z	L
Z	25	13	12	12	M	E
K	10	14	-4	22	W	A
J	9	15	-6	20	U	A
Y	24	16	8	8	I	A

VI. CONCLUSION

The integration of two encryption techniques in the proposed approach guarantees a high level of security for communication. Even if a data leak occurs, deciphering the transmitted message becomes exceptionally challenging due to dual-layer encryption. This robust mechanism significantly complicates decryption efforts by potential attackers, making it a highly effective safeguard for maintaining message confidentiality. The results conclusively demonstrate that this combined approach not only strengthens message security during transmission and reception but also offers substantial protection against various forms of external attacks, including advanced cryptographic threats.

Additionally, the scalability of this method is evident, as the complexity of encryption escalates with increasing message size, further reinforcing the security framework. The proposed solution is a vital step forward in achieving superior encryption strength and resilience, paving the way for secure and trustworthy communication in sensitive applications.

Future work will focus on optimizing the encryption process to enhance speed and efficiency. Furthermore, efforts will be directed toward integrating this approach with emerging technologies such as blockchain, and testing it against advanced attacks will be explored.

REFERENCES

[1] N. Kathirvel, S. Bharat, A. Kathirvel, and C. P. Maheswaran, “Artificial General-Internet of Things (AG-IOT) for Robotics of Automation Citation,” in *Systemic Analytic*, Vol. 2, No. 1, pp. 59–76, 2024, doi: 10.31181/sa2120241710.22105/SA.2021.281500.1061.

[2] S. Naveneethan, E.S. Madhan, and K. Ayyaswamy, “Identifying and Eliminating the Misbehavior Nodes in the Wireless Sensor Network”, Springer, Singapore, 2021, pp. 393-403, doi: 10.1007/978-981-16-7088-6_36.

[3] S. Sadeghi, N. Soltanmohammadlou, and F. Nasirzadeh, “Applications of wireless sensor networks to improve occupational safety and health in underground mines,” in *Journal of Safety Research*, Springer, Vol. 83, ISSN 0022-4375, pp. 8–25, 2022, doi: 10.1016/j.jsr.2022.07.016.

[4] M. Tropea, M. G. Spina, F. De Rango, and A. F. Gentile, “Security in Wireless Sensor Networks: A Cryptography Performance Analysis at MAC Layer,” in *Future Internet*, Vol. 14, No. 5, pp. 1-20, 2022, doi: 10.3390/fi14050145.

[5] D. J. Kadhim, “A Proposed Solution for Route Reply Storm Problem to Improve DSR Protocol Performance in Wireless Sensor Networks,” in *IOP Conf Ser Mater Sci Eng*, Vol. 1076, No. 1, p. 012058, 2021, doi: 10.1088/1757-899x/1076/1/012058.

[6] J. Matematika, D. Ilmu, P. Alam, L. Wilayah, Y. S. Santoso, and S. Santoso, “Message Security Using a Combination of Hill Cipher and RSA Algorithms,” 2021, doi.org/10.54076/jumpa.v1i1.38.

[7] S. K. Jaiswal and A. K. Dwivedi, “A Security and Application of Wireless Sensor Network: A Comprehensive Study,” in *2023 International Conference on IoT, Communication and Automation Technology,* ICICAT 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICICAT57735.2023.10263644.

[8] D. Kandris and E. Anastasiadis, “Advanced Wireless Sensor Networks: Applications, Challenges and Research Trends,” in *Multidisciplinary Digital Publishing Institute (MDPI)*,2024, doi: 10.3390/electronics 13122268.

[9] F. H. El-Fouly, M. Kachout, R. A. Ramadan, A. J. Alzahrani, J. S. Alshudukhi, and I. M. Alseadoon, “Energy-Efficient and Reliable Routing for Real-time Communication in Wireless Sensor Networks,” in *Engineering, Technology and Applied Science Research*, Vol. 14, No. 3, pp. 13959–13966, 2024, doi: 10.48084/etasr.7057.

[10] K. Sathish, C. V. Ravikumar, A. Srinivasulu, A. Rajesh, and O. O. Oyerinde, “Performance and Improvement Analysis of the Underwater WSN Using a Diverse Routing Protocol Approach,” in *Journal of*

TABLE VII
COMPARISON

Method	Result	Advantage	Disadvantage	Encryption Time (ms)	Key Size (bits)	Decryption Success Rate (%)
Hill 2*2	Simple and fast computations	Highly efficient, lightweight applications, simple encryption	Smaller key space, less secure	0.002-0.005	Matrix 2*2	98
Hill 3*3	Moderate complexity due to a larger matrix	Balanced efficiency and security, medium-level encryption	Larger key space, moderately secure	0.005-0.010	Matrix 3*3	97
Hill 4*4	High complexity requires more processing	Suitable for high-security needs, it offers stronger encryption	Lower efficiency, even larger key space, and highest complexity	0.010-0.020	Matrix 4*4	96
Ali Cipher	Moderate complexity	Balanced efficiency and security, medium-level encryption	Simple algorithm with medium-level secure	0.008-0.015	sentence (character(position))	100
HillAil Cipher	Very High Complexity	Extremely secure, suitable for very high-security needs, advanced encryption	Large key space, lower efficiency due to high complexity	0.015-0.030	sentence (character(position)) *sentence (character(alphabet(position)))	99

Computer Networks and Communications, Vol. 2022, pp. 1-20, 2022, doi: 10.1155/2022/9418392.

[11] A. W. K. Al-Nasir and F. S. Mubarek, "AODV, DSDV, and DSR Protocols of Routing: A Comparative Study in VANETs Using Network Simulator-2," in *Samarra Journal of Pure and Applied Science*, Vol. 6, No. 1, pp. 211–222, 2024, doi: 10.54153/ sjpas.2024.v6i1.662.

[12] E. Patnala and S. R. Giduturi, "Hybrid Dynamic Source Routing Technique and Security Implementation in Adhoc Network Topology," in *International Journal on Recent and Innovation Trends in Computing and Communication*, Vol. 11, pp. 342–353, 2023, doi: 10.17762/ ijritcc.v11i9s.7429.

[13] R. K. Hasoun, S. Faris Khlebus, and H. Kadhim Tayyeh, "A New Approach of Classical Hill Cipher in Public Key Cryptography," in *International Journal of Nonlinear Analysis and Applications*, Vol. 12, No. 2, pp. 1071–1082, 2021, doi: 10.22075/ijnaa.2022.5559.

[14] N. Nana and P. W. Prasetyo, "An implementation of Hill cipher and 3x3x3 rubik's cube to enhance communication security," in *Bulletin of Applied Mathematics and Mathematics Education*, Vol. 1, No. 2, pp. 75–92, 2021, doi: 10.12928/bamme.v1i2.4252.

[15] G. Rekha and V. Srinivas, "A Novel Approach In Hill Cipher Cryptography," in *international journal of mathematics and computer research*, Vol. 11, No. 06, pp. 3503–3505, 2023, doi: 10.47191/ ijmcr/v11i6.06.

[16] S. Arifin, D. Wijonarko, Suwarno, and E. K. Sijabat, "Application of Unimodular Hill Cipher and RSA Methods to Text Encryption Algorithms Using Python," in *Journal of Computer Science*, Vol. 20, No. 5, pp. 548–563, 2024, doi: 10.3844/jcssp.2024.548.563.

[17] S. J. Hsiao and W. T. Sung, "Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks," in *IEEE Access*, Vol. 9, pp. 72326–72341, 2021, doi: 10.1109/ACCESS. 2021.3079708.

[18] Z. Huanan, X. Suping, and W. Jiannan, "Security and application of wireless sensor network," in *Procedia Computer Science*, Elsevier B.V., 2021, pp. 486–492, doi: 10.1016/j.procs.2021.02.088.

[19] U. Panahi and C. Bayılmış, "Enabling secure data transmission for wireless sensor networks based IoT applications," in *Ain Shams Engineering Journal*, Vol. 14, No. 2, Article ID 101866, 2023, doi: 10.1016/j.asej.2022.101866.

[20] D. Sudha and A. Kathirvel, "An Intrusion Detection System to Detect and Mitigating Attacks Using Hidden Markov Model (HMM) Energy Monitoring Technique," in *Stochastic Modeling and Applications*, Vol. 26, No. 0972–3641, pp. 467–476, 2022.

[21] R. Upadhyay, U. R. Bhatt, and H. Tripathi, "DDOS Attack Aware DSR Routing Protocol in WSN," in *Physics Procedia*, Elsevier B.V., 2016, pp. 68–74. doi: 10.1016/j.procs.2016.02.012.

[22] A. A. Zaidan, B. Bahaa, S. A. Hameed, and O. O. Khalifa, "Novel Approach for Secure Cover File of Hidden Data in the Unused Area within EXE File Using Computation between Cryptography and Steganography," in *International Journal of Computer Science and Network Security (IJCSNS)*, Vol. 9, No. 5, pp. 294–300, 2009, https://www. researchgate.net/publication/241509578.

[23] H. Y. Lin and Y. R. Jiang, "A multi-user ciphertext policy attribute-based encryption scheme with keyword search for medical cloud system," in *Applied Sciences (Switzerland)*, Vol. 11, No. 1, pp. 1–14, 2021, doi: 10.3390/app11010063.

[24] J. S. Jolin, A. Theophilus, and A. Kathirvel, "Two-factor Mutual Authentication with Fingerprint and MAC Address Validation," in *International Journal of Computer Network and Information Security*, Vol. 16, No. 6, pp. 56–68, 2024, doi: 10.5815/ijcnis.2024.06.05.

[25] G. Nath, "Performance improvement of unicast reactive routing protocols in MANETs", in *Open Access Journal of Mathematical and Theoretical Physics*, Vol. 4, No. 1 pp. 1-7, 2023, doi: 10.15406/oajmtp.2023.04.00059.

[26] D. Sudha and A. Kathirvel, "The Performance Enhancement Of AODV Protocol Using GETUS," in *International Journal of Early Childhood Special Education (INT-JECSE)*, Vol. 15, No. 2, pp. 115-125, 2023, doi: 10.48047/INTJECSE/V15I2.11.

[27] B. Jeevana, S. Harshita, and A. Kathirvel, "MMF Clustering: A On-demand One-hop Cluster Management in MANET Services Executing Perspective," in *International Journal of Novel Research and Development*

(IJNRD), Vol. 8, No. 4, pp. 127–132, 2023, https://www.ijnrd.org/viewpaperforall.php?paper=IJNRD2304318

[28] Dr. A. K. D. Sudha, "The Effect of Etus in Various Generic Attacks in Mobile Adhoc Networks to improve the Performance of AODV Protocol," in *International Journal of humanities, Law and Social Sciences Published biannually by New Archaeological & Genological Society*, Vol. 9, No. 2348–8301, pp. 128–135, 2022.

[29] J. S. Jolin, A. Theophilus, and K. Ayyaswamy, "Two-factor Mutual Authentication with Fingerprint and MAC Address Validation," in *International Journal of Computer Network and Information Security*, Vol. 16, No. 6, pp. 56–68, 2024, 10.5815/ijcnis.2024.06.05.

[30] K. Ayyaswamy, "Utilizing Idle Time for Job Clusters Reduces Inventory and Total Job Completion Time for Single Machine Scheduling," in *Advances in Robotic Technology*, Vol. 2, No. 1, pp. 1–5, 2024, doi: 10.23880/art-16000119.

[31] A. K. Naren, A. Kathirvel, K. Nirmaladevi, and B. Santhoshi, "Overview of 5G Technology: Streamlined Virtual Event Experiences," in *Advances in Robotic Technology*, Vol. 2, No. 1, pp. 1–8, 2024, doi: 10.23880/art-16000109.

[32] K. Ayyaswamy, V. M. Gobinath, V. Sathya, N. Kathirvel, and Raj A. Anthony: "The Role of Robotics in Smart Manufacturing: Increasing Efficiency and Reducing Costs*",* The Quantum AI Era of Neuromarketin, IGI Global, 1st ed., 2024, doi: 10.4018/979-8-3693-7673-7.ch014.

[33] K. Ayyaswamy, A. K. Naren, and Raj A. Anthony: "New Perspectives on the Contribution of ChatGPT With AI in the Modern Era", Enhancing Research for Academicians in Higher Education, IGI Global, 1st ed., 2025, doi: 10.4018/979-8-3693-4496-5.ch013.

[34] W. Stallings, and L. Brown: "Computer Security Principles and Practice", Pearson Education, 3rd ed., 2015, https://thuvienso.hoasen.edu.vn/handle/123456789/11970.

[35] C. D. Schou, and D. P. Shoemaker: "Information Assurance for the Enterprise: A Roadmap to Information Security", McGraw Hill, 1st ed., 2006.

Haneen Mohammed Hussein received an M.Sc. degree in Computer and Control Engineering from Baghdad University, Baghdad, Iraq, in 2019. Currently, she is working in the Division of Construction and Projects at Mustansiriyah University, Baghdad, Iraq. Her research interests include Networking, Data Security, software engineering, and Artificial intelligence.

Ali Qasim Hanoon received an M.Sc. degree in the Faculty of Information Technology at Zarqa University, Zarqa, Jordan, in 2023. Currently, he is working at Qand Company, Baghdad, Iraq. His research interests include Computer Security, Networking, and Artificial intelligence.

Afrah Thamer Abdullah received an M.Sc. degree in Power and Electrical Machine Engineering, from Mustansiriyah University, Iraq, in 2019. Currently, she is working in the Division of Construction and Projects at Mustansiriyah University, Baghdad, Iraq. Her research interests include electrical power systems, renewable energy integration, and artificial intelligence