Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Secured Servant MODLEACH Heterogeneous Routing Protocol for Large Scale Wireless Sensor Networks

[1]Fuseini Jibreel, [2]Karim Azumah, [3] Yakubu Abdul-Wahab Nawusu, [4] Diyawu Mumin, [5] Shiraz Ismail
[1345] Department of Computer Science, , [2]Statistical Sciences Department, Tamale Technical University, Ghana.

Abstract **-** A Wireless Sensor Network (WSN) consists of tiny devices called sensor nodes. These devices can sense, compute, and transmit sensed data. They are usually deployed to capture data in hostile environments and transmit it to a Base Station for analysis. However, WSNs are vulnerable to various attacks and threats, which can compromise data credibility. Security, therefore, becomes a major concern in these networks. Servant-MODELACH is a heterogeneous routing protocol that was proposed without security features, making it unsuitable for insecure environments. In this paper. Secured Servant MODLEACH (SS-MODLEACH) is proposed. The new scheme uses asymmetric cryptography with effective key management to secure captured data from sensor nodes to the Base Station. SS-MODLEACH's performance was evaluated using MatLab 2018a, and simulation results show that the new scheme effectively encrypts and decrypts data with reasonable energy consumption**.**

Keywords - Wireless Sensor Networks, Security, Attacks, RSA

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are networks of low-cost devices used in many applications to transmit sensitive data from one device to another. Deploying wireless sensor networks in sensitive environments such as nuclear facilities or battlefield surveillance is challenging due to security implications. Securing communications is crucial in such environments, given the risk of active and passive attacks [1]. Cryptography can be used for security in WSNs, but the Cryptographic algorithms should be designed to use less memory, power and energy so the network lifetime can be increased [2]. Cryptography techniques can be classified into three types: Symmetric Cryptographic techniques, Asymmetric Cryptographic techniques and Hybrid Cryptographic techniques [3]. Symmetric cryptography uses a shared secret key for encryption and decryption between nodes. It's popular for being hardware-friendly and energy-efficient, and since the key is not sent with the message, decryption by unauthorised parties is tough. Only those with the shared key can decrypt it. Key distribution in this scheme is a major issue – the key needs to reach the recipient securely before the actual message, and using communication channels to transmit it can be insecure. Also, it does not support non-repudiable digital signatures [4][5]. However, Asymmetric cryptography uses a private key for decryption and signing, while a public key is used for encryption and verification. The private key stays secret, but the public key can be shared openly. This boosts security since private keys are not transmitted or exposed. It is also known as public key cryptography, and it solves the key distribution problem since keys do not need to be exchanged [6]. Hybrid cryptography combines symmetric and asymmetric cryptography approaches to leverage their strengths [7]. In cryptographic systems, the symmetric key cryptography alone is not enough for WSN security due to the key distribution challenge across distant nodes. Public key cryptography (PKC), on the other hand, is needed to efficiently distribute shared symmetric keys [8][9]. The PKC's computational complexity is the major challenge for WSN nodes, but previous works suggest that it can still be viable with constrained microcontrollers [10][11]. There are two main public key schemes that are being used in these networks. These are: ECC (elliptic curve cryptography) and RSA (Rivest Shamir Addleman) [12]. ECC is popular in WSNs due to its shorter key size (160-bit for security), whereas RSA needs a larger 1024-bit key for similar security. Still, RSA's widespread use in general computing and internet apps makes it a consideration for WSN systems needing compatibility with existing RSA-based infrastructure [13]. Therefore, this research proposes a secure servant MODLEACH using RSA. Many schemes based on symmetric or public key cryptography have been employed in wireless sensor networks to secure data transmission on the networks. A lightweight and efficient RSA hybrid messaging system (SHRSA) was implemented and analysed using a four-layer authentication stack by [14]. This approach addressed the issue of slow decryption speeds in low-level systems by leveraging passwords, digital certificates, and third-party authentication. The authors in [15] proposed a key-sharing algorithm combined with RSA encryption to enhance security in cloud computing data transfers between users and the cloud. In [16], Elliptic Curve Cryptography (ECC) was implemented as a lightweight encryption solution on a popular WSN operating system, utilising the TinyECC library to execute ECC operations. In [17], an efficient and robust authentication approach leveraging elliptic curve encryption and the ElGamal signature scheme was introduced. This method can authenticate hop-by-hop message content without exceeding the built-in threshold limitations. An RSA scheme was proposed to defend against DoS attacks in networks [18].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Simulation results showed that RSA's stability against DoS attacks leads to reduced energy consumption and increased network lifetime.

II. MATERIAL AND METHODS

In this section, the new scheme called Secured Servant MODLEACH(SS-MODLEACH) is explained.

A. Proposed system

The original unsecured scheme was proposed by the authors in [19]. The scheme adopted energy conservation techniques that can provide some amount of the energy required by some aspect of RSA application. Some of the strategies include selecting cluster head based on residual energy, servant nodes being introduced to aggregate data received from the nodes, a multi-hop transmission method used to convey reports from nodes to BS and the implementation of hard and soft thresholds before data transmission. It was also argued by the authors in [20] that ECC decrypts faster but encrypts slower than RSA, while RSA encrypts faster but decrypts slower. Therefore, RSA is employed in this research work.

B. Key generationn

In the proposed system, the BS is assumed to be a resourceful node having unconstrained computational capabilities and energy supply. The BS software system has three primary components: the database, the user interface, and the RSA algorithm. Therefore, the private and public keys are generated by the BS using the RSA algorithm, and it is explained below:

i. Two random prime numbers t and w, are generated by the BS such that t≠ w. These prime numbers are generated using Equation (1)

$$\boldsymbol{pr_y = primes(h);} \quad (1)$$

Where h is a positive integer. The prime numbers are confirmed using is_prime function.

The BS uses Equations (2), (3) and (4) to determine the public and private keys.

ii. **Modulus** $\boldsymbol{n_y = t * w}$ (2)

iii. $\boldsymbol{\varphi = (t-1)*(w-1)}$ (3)

iv. Public exponent $\boldsymbol{e,\ such\ that\ 1 < e < Phi}$ **and** $\boldsymbol{\gcd(e,\varphi) = 1}$ is chosen and then

v. Private exponent $\boldsymbol{d = e^{-1} mod\ \varphi}$ is determined. (4)

Hence, the public key and the private key generated are respectively $\{\boldsymbol{e}, \boldsymbol{n_y}\}$ **and** $\{\boldsymbol{d}, \boldsymbol{n_y}\}$

C. Key Distribution

When the BS generates the keys, it transmits the public key to the cluster heads (CHs). Applying the energy dissipation model discussed by authors in [22], the energy required for the transmission of the keys in bit to the CHs is given by the Equation (5)

$$\boldsymbol{E_{BSs} = k1E_{elect} + k1E_{fs}d_{BS-CH}^{\ 2}} \quad (5)$$

Where $\boldsymbol{E_{BSs}}$ is the energy dissipated by the BS, $\boldsymbol{k1}$ is the public key being transmitted in bits, $\boldsymbol{E_{elect}}$ energy used by the electronics of the transmitter, $\boldsymbol{E_{fs}}$, is the energy used for free space and $\boldsymbol{d_{BS-CH}}$ is the gap between the BS and CH.

The CHs will also share the received key with the servant CHs in their respective clusters using the Equation (6)

$$\boldsymbol{E_{CHs} = k1E_{elect} + k1E_{fs}d_{CH-SCH}^{\ 2}} \quad (6)$$

Where $\boldsymbol{d_{CH-SCH}}$ is the intervals between the CH and SCH.

D. Encryption process

1) Encryption process

Encryption is done using the public key, $\boldsymbol{k1}$ consists of$\{n_y, e\}$ which was generated and distributed by the BS. Hence, any time the SCHs receive data from the normal sensor nodes, they encrypt data with the public keys received from the CHs using the following procedure:

i. The normal nodes capture data from the environment as a positive integer (m) including their ID such that $m < n_y$

ii. The energy required to transmit their data (k bits) to the SCHs is given by Equation (7) and (8)

H = $\boldsymbol{kE_{elect} + kE_{FS}d_{SC}^{\ 2}}$ (7)

H = $\boldsymbol{kE_{elect} + kE_{mp}d_{SC}^{\ 2}}$ (8)

Where $\boldsymbol{d_{SC}}$ is the intervals between the sensor nodes (SN) and SCH

iii. The energy required by SCHs to received and aggregated the received data, m_t bit ($\boldsymbol{D_A}$, is given by Equation (8)

$$\boldsymbol{D_{Ag}, == C1E_{elect}\left(\frac{n}{c} - 2\right) + \left(\frac{n}{C} - 1\right) kE_{DA}} \quad (8)$$

Where $\boldsymbol{c}$ is the clusters' number in the network and $\boldsymbol{E_{DA}}$ is the energy for data aggregation.

iv. It then encrypts it, $\boldsymbol{C1}$, using equation (9)

$$\boldsymbol{C1} = m_t^{\ e} mod\ n_y \quad (9)$$

v. The ciphertext $\boldsymbol{C1}$ is now sent to the CHs.

The energy required by the SCH to send the encrypted data to the CH is given by Equation (10)

$$\boldsymbol{E_{SCHs} = E_{TX}(C1, d_{to\ CH})} \quad (10)$$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Where $d_{to\ CH}$ is the distance between the SCH and CH.

Also, the energy needed by the head to convey the aggregated and encrypted report to the Sink is given by Equation (11)

$$E_{CHs} = C1E_{elect} + C1E_{FS}{d_B}^2 \quad (11)$$

Where d_B is the intervals between the CH and BS

E. Decryption process

The Sink accepts the encoded report and then decodes it using its private key {d, n_y} to get the original message. It is only the BS which has this private key to decrypt.
The energy required by the BS to receive the encrypted data is given by Equation (12)

$$E_{BS} = C1E_{elect} \quad (12)$$

The BS uses the following Equation (12) to decrypt the received data.

$$m_t = C1^d mod\ n_y. \quad (13)$$

The resourced node extracts the plaintext from the integer representative m. It checks the IDs of the sending nodes before it will decide to discard it or accept it. Figure 1 shows how the encrypted data is sent to the BS.

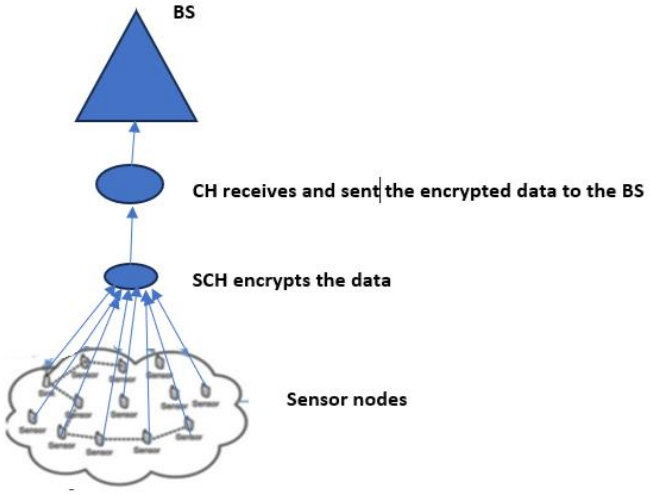

Fig. 1: Transmission of encrypted data to Base station

III. SIMULATION RESULTS AND ANALYSIS

The SS-MODLEACH model is simulated using MATLAB R2017a. This is to assess the effectiveness of the new secure algorithm. In this experiment, 200 nodes are deployed in 200*200 region and the BS was placed (100,250) away from the centre. Let's initialize the optimum probability, P_{opt} = 0.1 and assume that 40% of devices will be advanced sensors (m_y=0.2) and 20% servant nodes (q_y=0.1). The simulation parameters used are shown in Table1. However, prime numbers w and t are included in these standard values to generate the keys.

Table 1: Simulation Parameters

S/N	Parameter	Values
1	E_{elect}	50nJ/bit
2	E_{fs}	10pJ/bit/m^2
4	E_{mp}	0.0013pJ/bit/m^2
6	E_0	0.5J
7	k	4000
8	n	100
9	p_{opt}	0.1
10	w	2357
11	t	2551
12	K_e	1036250
13	m_t	1: STATISTICS.PACKETS_TO_BS(r+1)
14	m_t	***Enermies are comming***
15	E_{DA}	5nJ/bit/message

Table 2 shows the keys generated by the Base station (BS). The BS chooses two prime numbers and then generates both the public and private keys from these numbers.

Table 2: Generation of keys by the Base station

Proposed system	
Module(n):	6012707
Phi:	6007800
Public key generated:	(75913,6012707)
Private key generated:	(4433377,6012707)

Table 3 and Figure 2 show an encrypted packet from the CHs to the BS and decryption of the data by the BS at 250 rounds simulation period respectively. Thus r = 250.

Table 3: Encrypted Data

1	48	47	4	25	56	43	92	9	0	11	88	37
64	75	16	33	32	19	0	21	28	27	24	25	76
23	72	29	0	31	68	17	84	75	36	13	12	39
0	41	8	7	44	25	96	3	52	49	0	51	48
97	4	75	56	93	92	59	0	61	88	87	64	25
16	83	32	69	0	71	28	77	24	75	76	73	72
79	0	81	68	67	84	25	36	63	12	89	0	91
8	57	44	75	96	53	52	99	0	1	48	47	4
25	56	43	92	9	0	11	88	37	64	75	16	33
32	19	0	21	28	27	24	25	76	23	72	29	0
31	68	17	84	75	36	13	12	39	0	41	8	7
44	25	96	3	52	49	0	51	48	97	4	75	56
93	92	59	0	61	88	87	64	25	16	83	32	69
0	71	28	77	24	75	76	73	72	79	0	81	68
67	84	25	36	63	12	89	0	91	8	57	44	75
96	53	52	99	0	1	48	47	4	25	56	43	92
9	0	11	88	37	64	75	16	33	32	19	0	21
28	27	24	25	76	23	72	29	0	31	68	17	84
75	36	13	12	39	0	41	8	7	44	25	96	3
52	49	0	51	48	97	4	75	56	93	92	59	0
61	88	87	64	25	16	83	32	69	0	71	28	77
24	75	76	73	72	79	0	81	68	67	84	25	36
63	12	89	0	91	8	57	44	75	96	53	52	99
0	1	48	47	4	25	56	43	92	9	0	11	88
37	64	75	16	33	32	19	0	21	28	27	24	25
76	23	72	29	0	31	68	17	84	75	36	13	12
39	0	41	8	7	44	25	96	3	52	49	0	51

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The decrypted message is shown in Figure 2. Similarly, after the simulation of the decryption algorithm, the results obtained are picked from the MATLAB platform to a Microsoft word environment.

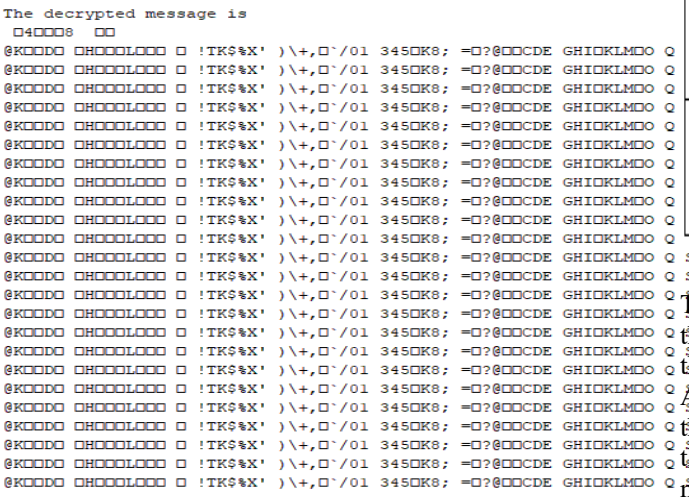

Fig. 2: Decrypted Packets by the Base station at 250 rounds

In order to illustrate the encryption and decryption process clearly, Figures 3, 4 and 5 are also generated.
Figure 3 shows new prime numbers w and t with new keys generated by the BS. In this case, encryption and decryption are done on specific data which is 5000bits of temperature and therefore, the prime numbers were chosen such that, though to increase the security of the network at the same time not depleting the energy of the nodes.

Proposed system	
Module(n): 66031513	
Phi: 66014928	
Public key generated:	(45380221,66031513)
Private key generated:	(38446789,66031513)
P= 9949	q = 6637

Fig. 3: Generation of new keys by the Base station

Figure 4 shows the encrypted 5000bits of the temperature sensed and transmitted by the SCHs nodes. The sensors first generated the ASCII equivalent of the data and finally encrypted the data before transmission.

Data transmitted: 5000bits of temperature
ASCII equivalent of the Data 53 48 48 48
The encrypted message is 31651694 57723616 57723616 57723616

Fig. 4: Encryption of data by BS using the proposed system.

The encrypted report is received by Cluster Head (CH), and then transmit the report to the BS. The BS received the report, then generate the ASCII of the message which is similar to ASCII during the encryption process. The destination node then decrypted the message as "5000" as seen in Figure 5 and then confirmed the ID of the nodes which have transmitted the message before accepting the message or rejecting it.

The decrypted message in ASCII is 53 48 48 48
The decrypted message is 5000

Fig. 5: Decryption of data by BS using the proposed system

Figure 6 displays the residual energy of the sensors without RSA. The initial energy of the sensor is 0.5J. This energy reduces gradually due to data transmission until the end of the simulation period. The existing scheme (S-MODEACH) has been able to minimize the energy exhaustion rate in the network better than the proposed algorithm (SS-MODLEACH). This is as a result of the absence of any security algorithm in the protocol.

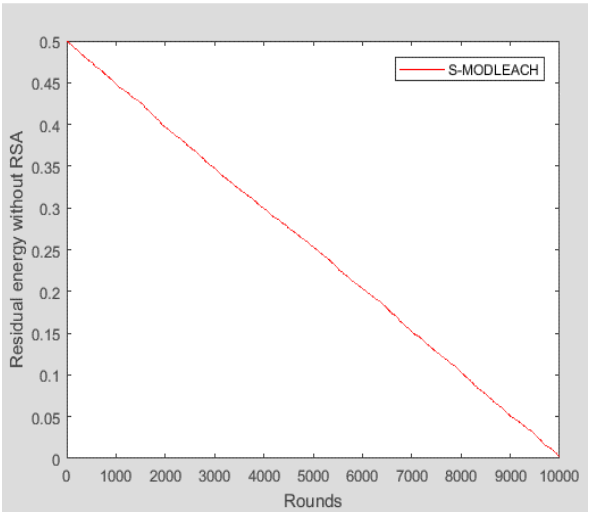

Fig. 6.: Residual Energy without RSA algorithm

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The Figure 4 shows the residual energy of the nodes with RSA per round. It can be seen that, the new scheme, SS-MODLEACH consumed energy more than the S-MODLEACH. This is because of the security algorithm in the new protocol. The normal sensor nodes used part of their energy to encrypt the captured data before transmission. As a result, most of the nodes die between 8000 and 9000 rounds. Few nodes whose energy was not exhausted showed a sudden increase in energy level but that was for a very short period. Although, adding the security algorithm has affected the lifetime of the network, the integrity, availability and confidentiality of the data transmitted are assured.

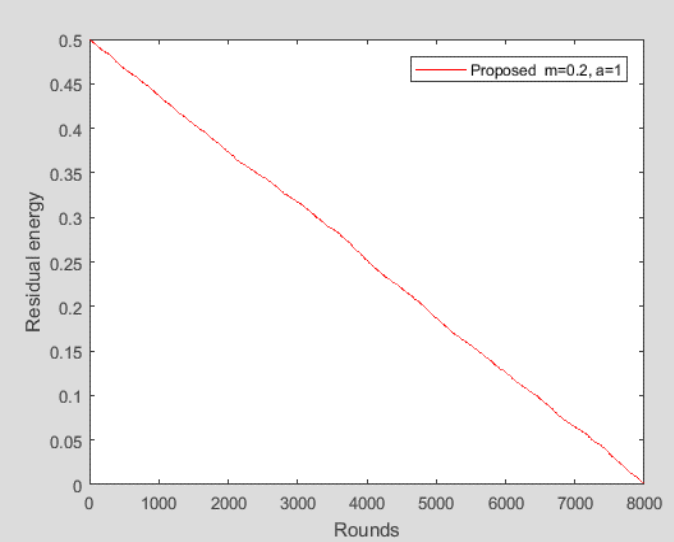

Fig. 7: Residual Energy with RSA per round

Figure 8 displays the number of death nodes without RSA. The rate of death of the nodes increases gradually until 10000 rounds where there was a sharp increase in the death of the nodes.

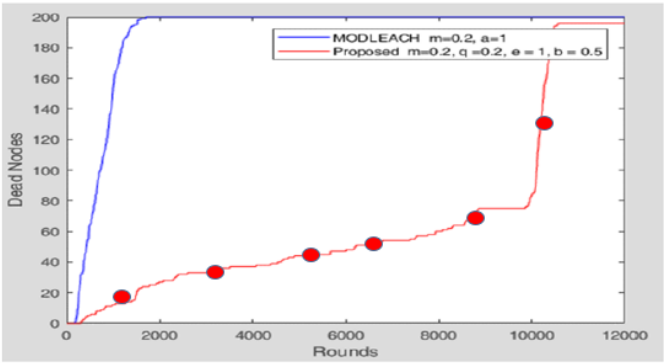

Fig. 8: Number of death nodes without RSA algorithm

Figure 9 displays the number of death nodes when the cryptographysystem was added. The rate of death of the nodes increases gradually until 8000 rounds where there was a sharp increase in the death of the nodes. The number of deaths recorded is 2000 of the nodes. This number could have been high if the energy for intracluster communication was not reduced. The reduction in this energy is as a result of the presence of servant nodes which immediately receive the encrypted data from the energy detrained nodes for onward submission to the cluster heads.

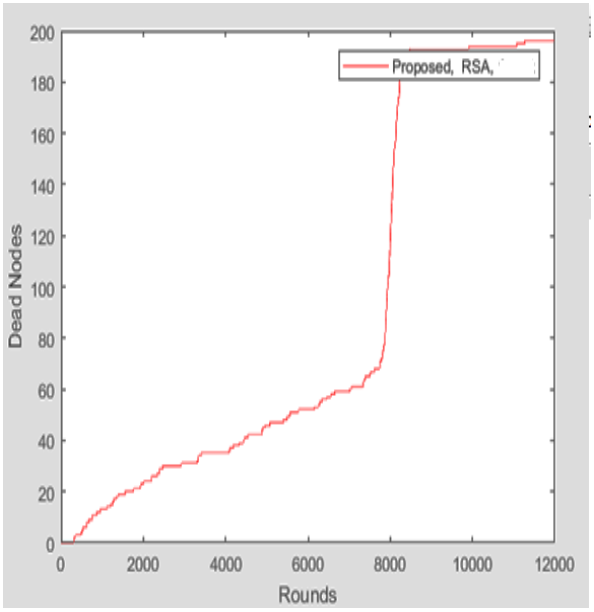

Fig. 9: Number of dead nodes with RSA algorithm per round

IV. CONCLUSION

In these results, Secured Servant MODLEACH (SS-MODLEACH) is proposed. The new protocol employed the RSA algorithm to protect the data being transmitted within the network. The normal nodes in SS-MODLEACH capture data and transmit the report to the Servant cluster heads (SCHs). The intermediate nodes, SCHs, encrypt the data using the RSA scheme since these nodes have higher energy than the normal nodes. The encrypted data is sent to the CHs, which then transmit it to the BS, which then decrypts the data. This key management technique has reduced the energy consumption that would have been witnessed without these strategies. Although the new algorithm consumed more energy than the existing scheme, as shown in Figures 6 and 7, the new protocol provides better security than the existing protocol. This makes the SS-MODLEACH suitable for any unsecured environment.

REFERENCES

[1] M. W. Khan, "SMS Security in Mobile Devices: A Survey," Int. J. Advanced Networking and Applications, vol. 5, no. 2, pp. 1873-1882, 2013.

[2] G. Saminathan and S. Karthik, "Development of an energy efficient, secure and reliable Wireless Sensor Networks Routing Protocol based on Data Aggregation and user Authentication," American Journal of Applied Sciences, vol. 10, no. 8, pp. 832-843, 2013.

[3] A. D. Daniel and E. Roslin, "WSN Security: An Asymmetric Encryption and Hash Function based Approach," Int. J. Engineering Research & Technology (IJERT), vol. 5, no. 2, pp. 312-314, 2016.

[4] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Comput. Netw., vol. 52, no. 12, pp. 2292-2330, 2008.

[5] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," Comput. Netw., vol. 51, no. 4, pp. 921-960, 2007.

[6] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557-3564, 2010.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

[7] C. Y. Chong and S. P. Kumar, "Sensor networks: Evolution, opportunities, and challenges," Proc. IEEE, vol. 91, no. 8, pp. 1247-1256, 2003.

[8] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," in Advances in Cryptology: Proceedings of CRYPTO 84, G. R. Blakley and D. Chaum, Eds. Berlin/Heidelberg, Germany: Springer, 1985, pp. 10-18.

[9] P. MacKenzie, S. Patel, and R. Swaminathan, "Password-Authenticated Key Exchange Based on RSA," in Proc. Advances in Cryptology—ASIACRYPT 2000, T. Okamoto, Ed. Berlin/Heidelberg, Germany: Springer, 2000, pp. 599-613.

[10] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: Testing the limits of elliptic curve cryptography in sensor networks," in Proc. European Conference on Wireless Sensor Networks, Bologna, Italy, 2008, pp. 305-320.

[11] C. P. L. Gouvêa and J. López, "Software implementation of pairing-based cryptography on sensor networks using the MSP430 microcontroller," in Proc. Int. Conf. Cryptology in India, NewDehli, India, 2009, pp. 248-262.

[12] N. Koblitz, "Elliptic Curve Cryptosystems," Math. Comput., vol. 48, no. 177, pp. 203-209, 1987.

[13] U. Gulen, A. Alkhodary, and S. Baktir, "Implementing RSA for Wireless Sensor Nodes," Sensors, vol. 19, no. 13, pp. 1-15, 2019.

[14] A. Bhattacharjy, X. Zhong, and X. Li, "A Lightweight and Efficient Secure Hybrid RSA (SHRSA) Messaging Scheme With Four-Layered Authentication Stack," IEEE Access, 2019.

[15] M. E. Hussain and M. R. Hussain, "Securing Cloud Data using RSA Algorithm," Suresh Gyan Vihar University, 2018.

[16] N. Saqib and S. S. Shekhawat, "Securing Wireless Sensor Networks Using Elliptic Curve Cryptography," Int. J. Eng. Trends Technol., vol. 56, no. 1, 2018.

[17] M. Manjusha, A. Prof, M. Laxmi, B. Rananavare, and A. Prof, "A Robust Message Authentication Scheme In Multihop WSN Using Elliptical Curve Cryptography And Elgamal Signature," Int. J. Eng. Research & Technology (IJERT), vol. 2, no. 7, 2013.

[18] R. Fotohi, S. F. Bari, and M. Yusefi, "Securing Wireless Sensor Networks Against Denial-of Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol," Faculty of Computer Science and Engineering, Shahid Beheshti University, Tehran, Iran, 2018.

[19] F. Jibreel, M. I. Daabo, A. W. Yusuf-Asaju, and K. A. Gbolagade, "Servant-MODLEACH Energy Efficient Cluster Based Routing Protocol for Large Scale Wireless Sensor Network," The 12th Int. Multi-Conference on ICT Applications, vol. XII, pp. 1-6, 2018.

[20] D. Mahto, "RSA and ECC: A Comparative Analysis," vol. 12, no. 19, pp. 9053-61, 2017.