An Efficient Triple-Layered Wireless Sensor Networks

[1.]A. Swathi. [2]B. Rama Rao, [3]R. Sowjanya, [4]B. Sonia, [5]Sk. Hasmi
[1,2,3,4,5]Department of Computer Science and Engineering
[1,2,3,4,5] QIS College of Engineering and Technology, Ongole
[1]a.swathi@qiscet.edu.in,[2]ramarao.b@qiscet.edu.in, [3]sowjanya.r@qiscet.edu.in,
[4]sonia.b@qiscet.edu.in,
[5]hasmi.sk@qiscetedu.in
Corresponding Author Mail: qispublications@qiscet.edu.in

Article Info

Page Number: 528 - 535

Publication Issue:

Vol 70 No. 2 (2021)

Abstract

The established complex environment for wireless network security, which is an important feature, is the core problem with sensor networks. Cryptology is a crucial component of security in remote sensor companies. Different cryptographic techniques now in use suffer from serious deficiencies. A robust, coordinated, triple-staged, and productive cryptographic approach employing both public-key and mystery key strategies is presented in this work. Because we take into account key management using public-key based methods and provide a high level of security, the Rijndael Encryption Approach (REA), Horst Feistel's Encryption Approach (HFEA), and the more advanced Rivest-Shamir-Adleman (e-RSA) are the methods that are recommended.REA was used in the various stages of the computation, followed by REA+HFEA in stage 2 and REA+HFEA+e-RSA in stage 3. All three phases were finished simultaneously.The execution time and decoding time of the proposed method were used to evaluate the exhibition levels.In contrast to previous approaches, the proposed set of rules employs a single evaluation boundary, or calculation time.On texts with individual sizes of 6, 25, 35, 61, and 184 MegaBytes (MB), it was found that the proposed strategy gave amazingly quick generally execution as far as estimation time, with Low Encryption Time (LET) and Low Unscrambling Time (LDT) of 1.12 and 1.26, separately.By 2.9%, the proposed hybrid form outperforms AES+RSA, ECC+RSA+MD-5, AES+ECC, and AES+ECC+RSA+MD5 by 1.36 times.

Article History

Article Received*: 05 September 2021*

Revised*: 09 October 2021*

Accepted*: 22 November 2021*

Publication*: 26 December 2021*

Keywords - Wireless Sensor Networks (WSN); Rijndael encryption approach; Horst Feistel's encryption approach; Enhanced RSA**.**

I. INTRODUCTION

WirelessSensorNetwork (WSN) serves as a bridge between the most important elements of the environment and the most sensitive devices.Due to the ease with which users can provide their login information across the World Wide Web (WWW), usage of the World Wide Web (WWW) is clearly growing at a phenomenal rate.Among all of these,privateness plays out a basic part,as realities is encodedandtransmitted totherecipient while given over the WWW. .There are no intruders attempting to alter or exploit the data.No intruder will ever be able to alter or speak data.Cryptography makes it possible for data to be transmitted encrypted so that only the shipper

and collector can access the private information.There are a variety of consistent verbal trade techniques, such as secret-key and public-key, [1-5]. A few experts use a combination of these keys, which is typically referred to as an integrated cryptographic strategy.Despite their drawbacks, secret and public-key cycles offer advantages [6].Public-key calculations are widely acknowledged to be appropriate in expressions of utility, whereas Secret-key calculations are commonly known to be appropriate in expressions of significant value [7].In terms of speed, framework, and equipment, public-key calculations are more expensive [8].Despite the fact that there are a few possibilities in which each calculation is combined, such as cross breed calculations, the majority of applications use Secret-key calculations [9]. This is because the effective arrangement takes advantage of each calculation while ignoring its drawbacks.

When those procedures are applied to a WSN, there are numerous responses, such as sending and receiving various bundles, granting authority to hubs, killing hubs throughout the discussion process, and so on.Therefore, prior to selecting any cryptographic arrangement of rules to store the prized and profitable item in WSN, such as power, it is crucial to discover the open doors.The editors of the newspapers [11, 12] conducted a thorough analysis of this definition, with the goal of selecting the best calculation from the results.To carry out WSN, in addition to selecting the best cryptography calculation, other plan considerations must be made, such as selecting the best steering convention with the lowest energy consumption and disseminating keys between two parties while taking security considerations into account [12-16].These considerations are crucial for making WSN more useful and expanding its existence.We propose an effective, robust, triple phased, double secured, and intelligent half breed of modified RSA, Rijndael encryption methods, and Horst Feistel's encryption, with e-RSA being a public-key algorithm and AES and DES being secret-key algorithms.Following that, the remaining components of the work are presented

II Related Works

Pushpa and B. K. Chauhan (2020). [17] fostered a blended cryptography system utilizing three distinct encryption guidelines, looked at the last computation and unscrambling times to those of existing methods, and got the ideal results. Kim, H., Lee, Y., Ryu, J., and Won (2020, January). [18] examined two security dangers for the objective convention that were advanced in WSNs for the Web of Things [26] by H. Yazdanpanah et al (IoT). Both of the assaults referenced above incorporate the meeting key: the first and the second. Their tests have shown security shortcomings in the convention proposed in [26]. e-RSA is a public-key algorithm, whereas AES, DES, and Gatate, V. are secret-key algorithms. Two boundaries that have an effect on the viability of Remote Mental Radio Sensor Organizations are bundle inertness and energy consumption.Rijndael and Horst Feistel's encryption methods are efficient, dependable, triple phased, double secured, and intelligent.After that, the remaining parts of the work are shown.S. Tripathi, R. Agrawal, and R. Kumar (Walk, 2020)24] provided an explanation of the WSN steering practices in their research (2020, June). Gatate, V., and Agarkhed, J., addressed these adaptability concerns.They likewise investigated and alluded to various security encryption and unscrambling guidelines and practices that shield WSNs from weaknesses and dangers.Three authors are involved:Another significant method for managing WSNs was described in Griotti, Gandino, and Rebaudengo's (2020) article [25].The calculated analysis of the proposed cryptosystem showed that network security was

improved and that computational effort was reduced.Choosing REA, HFEA, and e-RSA over other methods has the huge advantage of requiring less restriction due to smaller key sizes, which speeds up the process. The recommended cryptographic scheme uses the processing time III PROPOSED METHODOLOGY Horst Feistel's encryption technique, the Rijndael encryption methodology, and an updated Rivest-Shamir-Adleman scheme to combine the potential benefits of both secret key and public-key computations (e-RSA).Due to the fact that the solicitation for the encryption processes is dependent on how long it takes to encrypt and decrypt, it works well for important private or remote meetings with a lot of text.The data message was encrypted using the Rijndael method for the most crucial part, Horst Feistel's encryption method for the middle part, and e-RSA for the final part after it was divided into three parts.Block-based cryptography systems A. The cryptographic system The encryption cycle has three stages, all of which happen immediately.The client sends the data message through these three sections of this framework:first, middle, and last 1) Step I:We ought to be aware that the length of the data message is denoted by z.The first third of the data message, which can range from 0 to z/31, is mixed in a state of harmony I using the REA computation. Bi is assumed to be the starting block, and its numerical value is shown by i.Mi =, 0 I z/3-1, (1) ci = REAenc(Mi, ki), where I is the secret information block's mathematical worth and ki is REA's crucial value.(2) where I is the mathematical worth of the secret information block and ki is the critical worth of REA.ci = HFEAenc(Ti, ki) (5), where I denotes the fundamental value of HFEA in the middle block and Ti denotes the coded block following REA. It is assigned to a different ciphertext view that ci manages. The initial ciphertext for which we strive to finish the REA is received by C1.2) Phase II The REA and HFEA are applied to the second third of the data message between z/3 and 2Joining the coded information C1, C2, and C3 from steps I, II, and III yields the last coded information C that the beneficiary sends.

C = C1 C2 C3 (10)
Encryption process
1. Original data= z, stubs Bj all around bits.
2. m1 = z/tri-1} bits of zero,
3. m2 ={z/tri to 2z/tri-1} highlights, and
4. m3 ={2z/tri to n-1}..tri.
5. Step 1: for(i=null; I
6. I = zero ≤ I ≤ z/tri-1,
7. ci = REAenc(i, ki);
8.}
9.C1 = ci
10.Step 2:for (i z tri;11.cien is equivalent to HFEAenc (Ti, ki)
11.C2 =ci
12.Step 3:for (i = 2z/3;)I
13.Mi = 2 I/3 1
14.Ti equals REAenc ((Ti) I, which)
15 for (j = 2z/3;j) 16.
16. Tj = HFEAenc(Ti,ki)ci

17.ci is equivalent to e-RSAenc(Tj, ki).
18.C3 = ci2
19 Add up all of the ciphertext values you got in steps I, II, and III for the background, the paragraph, and the end.
20.C = C1 C2 C3;
A. The Decryption Process After the ciphertext is obtained from the source, the decryption frame divides it into the beginning, middle, and remaining blocks. 1) The beginning block of 1/3 of the ciphertext marks the end of Phase I RDA.Ci= 0 I z/3-1, (11) where Bi is directed toward the first block of the ciphertext and Ci is used to divide it numerically.RDADec(Ci, ki) (12) is the same as Mi, where ki is the mandatory decryption time.2) Phase II RDA, HFDA has a middle-third block of ciphertext at its conclusion. With RDA's consent, clear printed material regarding the use of Mi will be sent to P1.Ci= z/3 I 2z/3-1 (13), where Bi is the middle block of the ciphertext and its numerical charge is the amount of Ci used.Stage III unscrambling rules for RDA, HFDA, and e-RSA end with an additional 1/3 block of ciphertext. Ti = HFDAdec(Ci, ki) (1), mi = RDADec(Ti, ki) (15), and ki tries to separate a section when Ti tries to decode a block after HFDA. With HFDA approval, the basic text-based content used by the mi is distributed to P2.3).The additional block of ciphertext and its numerical total attempt to exploit Ci when Bi points to.Ci is equal to 2z/3 I z-1 (16), Ti is the same as e-RSAdec(Ci, ki), Tj is the same as HFDAdec(Ti, ki), and mi is the same as RDAdec(Tj, ki).After HFDA, Tj tends to an unencrypted block, indicating the required decryption cycle, whereas Ti tends to decode the block.P3s were ultimately provided with live content that attempted to utilize miles, and RDA's strategy concurred.
The final essential message-based content P is obtained through the method for strategy for interfacing P1, P2, and P3, which can be secured from Steps I, II, and III.
Utilizing P = P1 P2 P3 (20), C, bits Bj, mixed data, you can decipher Cycle 1.everything about bits.2.Piece, protuberance, and C3 are equal.

III.Results and Discussion

At various lengths and with data messages ranging from 6 to 18 megabytes, six hybrid cryptographic computations, including the Subasree ECC Dual-RSA MD-5 technique, Kumar's AES ECC approach, Ren's DES RSA approach, Ramaraji's AES RSA approach, Bhole's ECC AES RSA MD-5 scheme, and the proposed methodology (REA HFEA e - RSA), were gathered.Each of the six methods was combined multiple times for each text size to ensure that the fastest method did not always emerge.The evaluation and decryption times of six hybrid encryption calculations with data message lengths ranging from 6 to 18 megabytes are presented.For each of the six cross-based cryptographic estimates, the corresponding graphical representation and computation time are shown in Figure 2.In figure 2, the different lengths of the data messages of the five message sizes are managed in the x-center and the consuming processor time in the y-center.A graphical representation that is nearly identical to the separation time of the six cross-based cipher computers is shown in Figure 3.In Table I and Table, respectively, the proposed model's AET and ADT of 1.12 and 1.26 are highlighted in yellow.II. The proposed cream model's efficiency is shown in Table III. This model is clearly faster than ECC RSA MD-5 (3.26/2.38) and AES ECC (3.25/2.38), respectively. (7.72/2.38) is 3.2 times faster than AES ECC RSA MD5 and 2.7 times faster than AES

RSA. However, the proposed crossover-variety model's efficiency is roughly equivalent to that of DES and RSA, i.e.,/2.38) = 1.03, which is shown in Table IV as much as possible in the proposed model.

I. Table:ADT Estimate for the Proposed Model in which the Most Recent Technology Is Very Close to the Model/Text Size MB 6 25 35 61 18 ADT ECC RSA MD-5 2.1 1.8 1.9.9 5.5 3.2 AES ECC RSA MD-5 1.8 1.5 2 1.5 2 1.76 AES ECC AES 8.8.5 ECC 5.8.12 1.3 AES RSA 2.5 2 2.5 5 3.2 AES ECC RSA MD5 3.5 3 3 5 5 3.9 Table:III The proposed HFEA model performs well.Model AET ADT ECC RSA MD-5 1.5 1.76 3.26 AES ECC 3.82 3.92 7.7 AES ECC 3.82 3.92 7.7 AES ECC 3.812.Proposed (REA HFEA e-RSA) MD5 3.82 3.9 7.72 Table IV 1.12 1.26 2.38Limits on reproduction Metric marker value sensor centers NC 300 sinks SC 1 grid area A*B 300 * 300 m2 sink position (a,b) (150 200) initially

IV. Future Enhancement

The best part, WSN security is a specialization in this study.The gatecrasher won't ever distribute evaluations about the framework being referred to in light of the fact that the arrangement works in three phases.The first phase utilized REA, the subsequent phases utilized HFEA, and the final phase utilized e-RSA. Two or three of the trans-based encryption methods that are currently available take longer to compute than the coordinated method. Even though the motivated procedure now appears to be different from the initial estimates, it performs better during estimated time breaks. The inclusion of current mole encryption techniques in the cited calculations provided the basis for these studies. The proposed cream structure stands out as a barrier to the limit of single evaluation, or computational time, which is the primary issue with these tests.In any case, the proposed Cream version's total display can only be as big as the ciphertext length, energy gain, and other restrictions.There may be phases to this review.looking at things like the energy gain from the sensor center, the range of the assembled packets, and the length of the ciphertext, etc.

References

[1] H. Hu and W. Chang, "On the Mitigation of Controllable Event Triggering Attack in WSNs," 2020 29th International Conference on Computer Communications and Networks (ICCCN), 2020, pp. 1-6, doi: 10.1109/ICCCN49398.2020.9209613.

[2] R. Chanana, A. K. Singh, R. Killa, S. Agarwal and P. S. Mehra, "Blockchain Based Secure Model for Sensor Data in Wireless Sensor Network," 2020 6th International Conference on Signal Processing and Communication (ICSC), 2020, pp. 288-293, doi: 10.1109/ICSC48311.2020.9182776.

[3] G. Xu, F. Wang, M. Zhang and J. Peng, "Efficient and Provably Secure Anonymous User Authentication Scheme for Patient Monitoring Using Wireless Medical Sensor Networks," in IEEE Access, vol. 8, pp. 47282-47294, 2020, doi: 10.1109/ACCESS.2020.2978891.

[4] Y. Zhan, B. Wang and R. Lu, "Cryptanalysis and Improvement of a Pairing-Free Certificateless Aggregate Signature in Healthcare Wireless Medical Sensor Networks," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5973-5984, 1 April1, 2021, doi: 10.1109/JIOT.2020.3033337.

[5] S. Hassayoun, S. Lahouar and K. Besbes, "SDR Bridge for a Secure Wireless Sensor Network (WSN)," 2020 IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems (DTS), 2020, pp. 1-5, doi: 10.1109/DTS48731.2020.9196201.

[6] J. Kar, K. Naik and T. Abdelkader, "A Secure and Lightweight Protocol for Message Authentication in Wireless Sensor Networks," in IEEE Systems Journal, vol. 15, no. 3, pp. 3808-3819, Sept. 2021, doi: 10.1109/JSYST.2020.3015424.

[7] K. -A. Shim, "Cryptanalysis of Two Signature Schemes for IoT-Based Mobile Payments and Healthcare Wireless Medical Sensor Networks," in IEEE Access, vol. 8, pp. 167203-167208, 2020, doi: 10.1109/ACCESS.2020.3023093.

[8] S. Li et al., "A Secure Scheme Based on One-Way Associated Key Management Model in Wireless Sensor Networks," in IEEE Internet of Things Journal, vol.s 8, no. 4, pp. 2920-2930, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3021740.

[9] P. Arpaia, F. Bonavolontà and A. Cioffi, "Security vulnerability in Internet of Things sensor networks protected by Advanced Encryption Standard," 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT, 2020, pp. 452-457, doi: 10.1109/MetroInd4.0IoT48571.2020.9138236.

[10] An Braeken, "Symmetric Key-Based Authentication with an Application to Wireless Sensor Networks," in IoT Security: Advances in Authentication , Wiley, 2020, pp.65-84, doi: 10.1002/9781119527978.ch3.

[11] X. Lin, M. Guizani, X. Du, C. -K. Chu and Y. Yu, "Advances of Security and Privacy Techniques in Emerging Wireless Networks," in IEEE Wireless Communications, vol. 27, no. 3, pp. 8-9, June 2020, doi: 10.1109/MWC.2020.9116080.

[12] J. Shen, Z. Gui, X. Chen, J. Zhang and Y. Xiang, "Lightweight and Certificateless Multi-Receiver Secure Data Transmission Protocol for Wireless Body Area Networks," in IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/TDSC.2020.3025288.

[13] X. Zhu, Y. Li and Y. Lei, "A Forwarding Secrecy Based Lightweight Authenticastion Scheme for Intelligent Logistics," 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications(AEECA), 2020, pp. 356-360, doi: 10.1109/AEECA49918.2020.9213520.

[14] Jothi AA, Srinivasan B. “A Hybrid Ciphertext-Policy With Hierarchical Attribute-Based Ring Signcryption To Enhance Security And Privacy In Body Area Networks”. 2016 International Journal of Advanced Research in Computer Science. May 1;7(3).

[15] Zhong S, Zhong H, Huang X, Yang P, Shi J, Xie L, Wang K. “Connecting Things to Things in Physical-World: Security and Privacy Issues in Mobile Sensor Networks. In Security and Privacy for Next-Generation Wireless Networks” 2019 (pp. 135-160). Springer, Cham.

[16] B. T. Asare, K. Quist-Aphetsi and L. Nana, "A Hybrid Lightweight Cryptographic Scheme For Securing Node Data Based On The Feistel sCipher And MD5 Hash Algorithm In A Local IoT Network," 2019 International Conference on Mechatronics, Remote Ssensing, Information Systems and Industrial Information Technologies (ICMRSISIIT), 2019, pp. 1-5, doi: 10.1109/ICMRSISIIT46373.2020.9405869.

[17] Pooja, Chauhan RK. “Triple phase hybrid cryptography technique in a wireless sensor network”. International Journal of Computers and Applications. 2020 Jan 8:1-6.

[18] J. Ryu, H. Kim, Y. Lee and D. Won, "Cryptanalysis of Protocol for Heterogeneous Wireless Sensor Networks for the Internet of Things Environment," 2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM), 2020, pp. 1-4, doi: 10.1109/IMCOM48794.2020.9001674.

[19] V. Gatate and J. Agarkhed, "Spectrum Aware Cryptography (SAC) in Wirelesss Cognitive Radio Sensor Networks for Delay Sensitive Applications," 2020 International Conference for Emerging Technology (INCET), 2020, pp. 1-7, doi: 10.1109/INCET49848.2020.9154027.

[20] S. Shin and T. Kwon, "A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things," in IEEE Access, vol. 8, pp. 67555-67571, 2020, doi: 10.1109/ACCESS.2020.2985719.

[21] H. A. Babaeer and S. A. Al-Ahmadi, "Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking," in IEEE Access, vol. 8, pp. 92098-92109, 2020, doi: 10.1109/ACCESS.2020.2994587.

[22] S. Reshma, K. Shaila and K. R. Venugopal, "DEAVD - Data Encryption and Aggregation using Voronoi Diagram for Wireless Sensor Networks," 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 2020, pp. 635-638, doi: 10.1109/WorldS450073.2020.9210316.

[23] C. Meshram, C. Lee, S. G. Meshram and A. Meshram, "OOS-SSS: An Efficient Online/Offline Subtree-Based Short Signature Scheme Using Chebyshev Chaotic Maps for Wireless Sensor Network," in IEEE Access, vol. 8, pp. 80063-80073, 2020, doi: 10.1109/ACCESS.2020.2991348.

[24] R. Kumar, S. Tripathi and R. Agrawal, "A Review On Security in Wireless Sensor Network," 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), 2020, pp. 304-308, doi: 10.1109/ESCI48226.2020.9167610.

[25] M. Griotti, F. Gandino and M. Rebaudengo, "Transitory Master Key Transport Layer Security for WSNs," in IEEE Access, vol. 8, pp. 20304-20312, 2020, doi: 10.1109/ACCESS.2020.2969050.

[26] H. Yazdanpanah, M. Azizi and S. M. Pournaghi, "A Secure and Improved Authentication Scheme for Heterogeneous Wireless Sensor Networks in the Internet of Things Environment," 2020 17th International ISC Conference on Information Security and Cryptology (ISCISC), 2020, pp. 36-43, doi: 10.1109/ISCISC51277.2020.9261922.

[27] P Ramprakash, M Sakthivadivel, N Krishnaraj, J Ramprasath. ”Host-based Intrusion Detection System using Sequence of System Calls” International Journal of Engineering and Management Research, Vandana Publications, Volume 4, Issue 2, 241-247, 2014

[28] N Krishnaraj, S Smys.”A multihoming ACO-MDV routing for maximum power efficiency in an IoT environment” Wireless Personal Communications 109 (1), 243-256, 2019.

[29] N Krishnaraj, R Bhuvanesh Kumar, D Rajeshwar, T Sanjay Kumar, Implementation of energy aware modified distance vector routing protocol for energy efficiency in wireless sensor

networks, 2020 International Conference on Inventive Computation Technologies (ICICT),201-204

[30] Ibrahim, S. Jafar Ali, and M. Thangamani. "Enhanced singular value decomposition for prediction of drugs and diseases with hepatocellular carcinoma based on multi-source bat algorithm based random walk." Measurement 141 (2019): 176-183. https://doi.org/10.1016/j.measurement.2019.02.056

[31] Ibrahim, Jafar Ali S., S. Rajasekar, Varsha, M. Karunakaran, K. Kasirajan, Kalyan NS Chakravarthy, V. Kumar, and K. J. Kaur. "Recent advances in performance and effect of Zr doping with ZnO thin film sensor in ammonia vapour sensing." GLOBAL NEST JOURNAL 23, no. 4 (2021): 526-531. https://doi.org/10.30955/gnj.004020 , https://journal.gnest.org/publication/gnest_04020

[32] N.S. Kalyan Chakravarthy, B. Karthikeyan, K. Alhaf Malik, D.Bujji Babbu,. K. Nithya S.Jafar Ali Ibrahim , Survey of Cooperative Routing Algorithms in Wireless Sensor Networks, Journal of Annals of the Romanian Society for Cell Biology ,5316-5320, 2021

[33] Rajmohan, G, Chinnappan, CV, John William, AD, Chandrakrishan Balakrishnan, S, Anand Muthu, B, Manogaran, G. Revamping land coverage analysis using aerial satellite image mapping. Trans Emerging Tel Tech. 2021; 32:e3927. https://doi.org/10.1002/ett.3927

[34] Vignesh, C.C., Sivaparthipan, C.B., Daniel, J.A. et al. Adjacent Node based Energetic Association Factor Routing Protocol in Wireless Sensor Networks. Wireless Pers Commun 119, 3255–3270 (2021). https://doi.org/10.1007/s11277-021-08397-0.

[35] C Chandru Vignesh, S Karthik, Predicting the position of adjacent nodes with QoS in mobile ad hoc networks, Journal of Multimedia Tools and Applications, Springer US,Vol 79, 8445-8457,2020