An Efficient and Secured Triple-Layered Wireless Sensor Network with Machine Learning Techniques

Reem Atassi[1,*], Aditi Sharma[2,3]

[1]Faculty of Computer Information System, Higher Colleges of Technology, UAE

[2]IEEE Senior Member, Post-Doc Fellow, Intelligent Cryptographic systems/IOT-Cloud in Robotics, Nazarbayev University, Kazakhstan

[3]Department of Computer Science, School of Engineering and Digital Sciences

Emails: ratassi@hct.ac.ae; aditi11121986@gmail.com

Abstract

Replacement of physical labor and repetitive tasks by the agents is an attractive issue in the Smart Environment (SE). SE is distinguished by its ability to be controlled from a distance, to facilitate the connection between devices through middleware, to gather and share data from sensors, to improve the intelligence of devices, and to make decisions. To be effective, SE design must make use of information and networks that already exist in the actual world. Effective SE design is complicated by several difficulties, including monitoring, data collecting, assessment, evaluation, prediction of important data, and meaningful presentation. For SE, the most important step is gathering information from a variety of sensors in various locations. Wireless sensor networks provide an underlying architecture for the coordinated collection of data from many sensors that have common characteristics (WSN). An essential aspect of sensor networks is their inability to function in the currently complicated environment for wireless network security. In the realm of remote sensor businesses, cryptology is an essential part of safety measures. Several of the prevalent cryptographic methods have significant flaws that prevent them from being fully reliable. In this paper, we provide a unified, three-stage cryptographic procedure that combines public-key and secret-key techniques for maximum security. Due to consideration of Public-key management and high degree of security, Rijndael Encryption Approach (REA), Horst Feistel's Encryption Approach (HFEA), and the more sophisticated Rivest-Shamir-Adleman (e-RSA). Time spent in both execution and decoding of the suggested approach was utilized to rank the quality of displays. The suggested set of rules uses a single evaluation boundary or computation time, which is different from the methodologies used before. Low Encryption Time (LET) and Low Unscrambling Time (LDT) values of 1.12 and 1.26 were observed on texts ranging in size from 6 to 184 MB, respectively. Comparisons show that the suggested hybrid form is 2.9% more efficient than AES+RSA, 1.36 times more efficient than ECC+RSA+MD-5, 1.36 times more efficient than AES+ECC, and 1.36 times more efficient than AES+ECC+RSA+MD-5.

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

1. Introduction

Connecting critical environmental factors with ultra-sensitive sensors is the primary function of Wireless Sensor Networks (WSN). World Wide Web (WWW) use is certainly rising at a spectacular

DOI: https://doi.org/10.54216/IJWAC.060201
Received: September 03, 2022 Accepted: November 18, 2022

pace due to the convenience with which users may enter their login credentials throughout the WWW. Among them, confidentiality plays a crucial role since information sent via the Internet must be encoded before being sent to the intended receiver. Intruders aren't trying to exploit or change the data in any way. There will never be a breach where an unauthorized person may change or hear information. Thanks to cryptography, sensitive material may be sent in an encrypted form, accessible only to the sender and the recipient. Several reliable verbal exchange methods exist, including secret-key and public-key [1-5]. The usage of several keys is known as an integrated cryptographic technique and is only used by a select few specialists. Both secret-key and public-key cycles have benefits [6] while having downsides. Generally speaking, it is accepted that public-key calculations are suitable when expressing practicality, but secret-key calculations are generally accepted when expressing significance [7]. Public-key computations are more costly because of slower speeds, a more complex infrastructure, and specialized hardware [8]. Some applications may utilize a hybrid approach, such as cross-breed computations, although Secret-key calculations are still widely used [9]. This is because the optimal setup makes the most of every computation while minimizing or avoiding their downsides.

There are several possible reactions when those methods are implemented in a WSN, including sending and receiving different bundles, delegating power to hubs, and destroying hubs at various points in the conversation. Therefore, it is essential to find the available avenues before settling on any cryptographic arrangement of rules to store the precious and lucrative item in WSN, such as power. Newspaper editors [11, 12] analyzed this definition in depth in order to choose the most accurate computation. In order to implement a WSN, it is not enough to just choose the most secure cryptographic computation; additional planning considerations, such as the most energy-efficient steering convention and the safest method of key distribution between parties, must also be considered [12-16]. These factors are essential for increasing WSN's utility and spreading its reach. We propose a hybrid of the public-key algorithm e-RSA, the secret-key algorithms AES and DES, and Horst Feistel's encryption that is both efficient and safe. The RSA and Rijndael encryption techniques are updated, and the hybrid is triple-phased, double-secured, and intelligent. Subsequently, the remaining parts of the work are provided.

1.1 Route Maintenance

Once the destination node has issued the RREP message, packet transmission is started using the best available path as determined by the route cache. Communication is sent "hop by hop," or from one node to the next. If a single node in the transmission route fails, the transmission will fail. There is no way for the preceding nodes to learn that the node after them has failed. A routing error (RERR) message will be sent from the failing node to the sending node in this case. With this message, the origin node may restart the pathfinding procedure. Because nodes are in constant motion throughout the transmission period, there are constant interruptions. In order to find a new route, the originating node will retransmit the RREQ message if it has relocated. A mistake in a relay node causes it to transmit a RERR message to the node before it.

A sensor network is an unmanaged, static ad hoc network made up of hundreds of sensor nodes. Each sensor node has a sensing component, a CPU with limited computational capability, a wireless transceiver and antenna with a relatively small range, and a battery that can only provide so much juice. Each node in a sensor network keeps an eye on some aspect of the environment nearby, processes the data it collects, and sends it on to a centrally located base station.

Longevity improvement in WSNs may be accomplished in part via improved energy efficiency. If unnecessary data transmission is avoided along a productive path, energy use may be reduced. Methods for cutting down on power consumption include various forms of routing, clustering, and data aggregation. For conventional methods, discovering neighbors and choosing cluster heads uses more energy than actually having such conversations does. The main problems of the conventional methods are time synchronization, the existence of idle nodes, and route failure. A pair of protocols, Energy Efficient Sleep Scheduling (EE-SS) and Cross-Layer LEACH (CL-LEACH) are developed to achieve energy efficiency through data aggregation and routing, respectively, in order to solve the aforementioned problems. For choosing the heads of clusters and the gateways between them, the Hierarchical Clustering by Gateway Election (HCGE) is presented. The approach relies on the RSSI for gateway selection and the residual energy for choosing cluster heads. Despite this, the proposed work offers great performance while also increasing the lifespan of WSNs via more efficient use of energy.

DOI: https://doi.org/10.54216/IJWAC.060201
Received: September 03, 2022 Accepted: November 18, 2022

2. Related Work

In the paper, Pushpa and B. K. Chauhan (2020), the best results were obtained when [17] promoted a mixed cryptography system using three different encryption recommendations and compared the final calculation and unscrambling timings to those of current approaches. In a study conducted by Kim, Lee, Ryu, and Won (2020, January). H. Yazdanpanah et al. [18] analyzed two security threats to the objective convention proposed in their paper "WSNs for the Web of Things" [26]. IoT Attacks 1 and 2 both use the meeting key. The testing they conducted revealed vulnerabilities in the suggested convention for ensuring data security [26]. While AES, DES, and Gatate, V. are all secret-key algorithms, e-RSA is public-key. Remote Mental Radio Sensor Organizations are limited in their usefulness by two factors: bundle inertness and energy expenditure. The ciphers developed by Rijndael and Horst Feistel are not only smart, but also fast, secure, and use three different phases of encryption. The remaining sections of the presentation follow after that. In their study, researchers S. Tripathi, R. Agrawal, and R. Kumar (Walk, 2020)[24] outlined how WSN steering procedures are often carried out (2020, June). These worries about flexibility were addressed by Gatate, V., and Agarkhed, J. They also looked into and made allusions to a number of other encryption and decryption best practices that help keep WSNs safe from vulnerabilities and threats. This work is the collaborative effort of three authors: In their paper [25], Griotti, Gandini, and Rebaudengo (2020) introduced another important approach to controlling WSNs. A mathematical examination of the suggested cryptosystem revealed its efficacy in boosting network security while simultaneously reducing the computational burden. Less restriction is needed when using REA, HFEA, and e-RSA as opposed to other techniques owing to reduced key sizes, which speeds up the process. Processing time is used by the suggested cryptographic algorithm.

3. Proposed Methodology

Combining the advantages of both secret key and public-key calculations, as in Horst Feistel's encryption method, the Rijndael encryption technology, and the most recent iteration of the Rivest-Shamir-Adleman scheme (e-RSA). This method is ideal for confidential, distant, or high-stakes meetings that include a lot of text due to the fact that the encryption and decryption times are factored into the request. After splitting the data message into three sections, the most vital section was encrypted using the Rijndael technique, the intermediate section was encrypted using Horst Feistel's encryption method, and the last section was encrypted using e-RSA. Systems of encryption based on blocks A. The method of encryption Three distinct but simultaneous phases make up the encryption cycle.

The primary objective of this study is to provide a practical method for estimating the costs of energy use in WSNs. Figure 1 depicts our methodology and describes the general process of our planned study. At first, the network model is built, and the sensors node is installed along the pipeline. The next step is to analyze the data and compile it into a report detailing the energy use. The effectiveness of the suggested paradigm is finally proven.

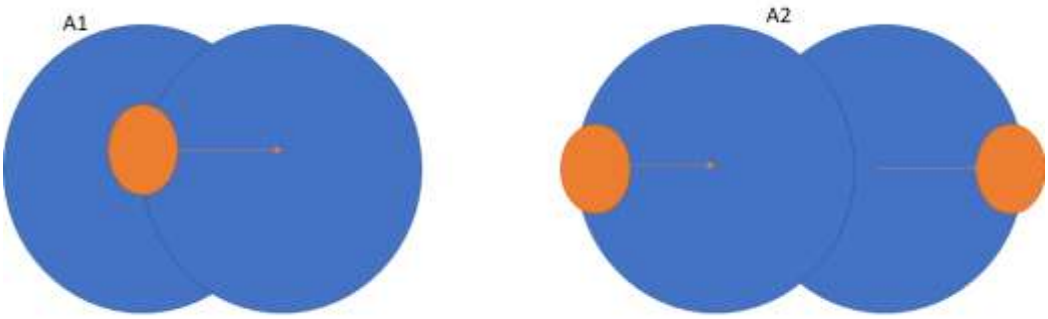

Figure 1: Possible interactions of neighbor nodes

To calculate this, we need to compare the areas where the communication coverages of two randomly chosen neighbors overlap. Their coverage and transmission areas will overlap if the two

DOI: https://doi.org/10.54216/IJWAC.060201
Received: September 03, 2022 Accepted: November 18, 2022

nodes are within communication range. The most severe examples of this situation are shown in Figure 1. To calculate the power required by a network for detecting harmful gases, the COA-LEACH energy model was developed. The COA-LEACH energy model is broken down into the following five stages:

1) All network nodes are awake during CORN P cycles, anticipating a CORN packet from another node. Energy is also needed at this stage, with p being proportional to the total number of packets.
2) Periodic resynchronization of nodes is performed to prevent clock drift. There is constant transmission of the CORN packet from all nodes, but only a small percentage of them really get it to their intended destinations. It's because of packet loss and collisions. Sending and receiving the CORN packet at this phase also requires some amount of energy.
3) Each node in a CORN network does neighbor finding during each N P cycle. Not all network nodes will conduct the discovery procedure simultaneously since some will get disoriented at the moment of channel conflict. As a result, the periodic neighbor finding is slowed down by collision.
4) Assuming a constant rate of consumption, the total energy used may be calculated as (1)

$$E_{\text{Total}} = E_{\text{Data}} + E_{\text{Neighbor\_Discouery}} + \varphi_1 \quad (1)$$

In Equation (1) E_{Total} denotes the total energy consumed by the network, E_{Data} is the amount of energy consumed for transferring the data packet and the E is the amount of energy consumed for detecting the neighbor discovery. φ is a constant.

5) A threshold value is set to decide whether the range for communication should be selected or discarded. The threshold value can be derived using Equation (2).

$$\text{Threshold} = \sqrt{\frac{\ln\left(1-P\left(\left(\text{conn}\right)^{\frac{1}{n}}\right)\right)}{-\lambda\pi}} \quad (2)$$

The probability of a network's connections, denoted by *P(conn)* in the equation above, is proportional to its density, shown by Equation 2. Once the power consumption rises over a certain limit, the channel is no longer usable for communication. In any case, the data transfer range may be adjusted.

Algorithm 1: Encryption of Proposed work

Encryption Process-
Original data = *z*, stubs B_j all around bits.
$m_1 = \{z/tri - 1\}$ bits of zero,
$m_2 = \left\{\frac{z}{tri}\ to\ \frac{2z}{tri} - 1\right\}$ highlights, and
$m_3 = \left\{\frac{2z}{tri}\ to\ n - 1\right\}$..tri.
Step 1: for(*i*=NULL; *I*)
$I = zero \leq I \leq z/tri - 1,$
$ci = REAenc(i, ki);$
C1 = ci
Step 2:for (*i z tri*);11.cien is equivalent to HFEAenc *(Ti, ki)*
C2 =ci
Step 3:for (i = 2z/3;)I
Mi = 2 I/3 1
Ti equals *REAenc ((Ti) I*, which)
for $(j = 2z/3; j)$ 16.
$Tj = HFEAenc(Ti, ki)ci$
ci is equivalent to *e-RSAenc(Tj, ki).*
$C3 = ci2$
Add up all of the ciphertext values you got in steps I, II, and III for the background, the paragraph, and the end.
$C = C1\ C2\ C3;$

A. The Decryption Process: After the ciphertext is obtained from the source, the decryption frame divides it into the beginning, middle, and remaining blocks.

DOI: https://doi.org/10.54216/IJWAC.060201
Received: September 03, 2022 Accepted: November 18, 2022

3.1 Data Aggregation

In typical WSNs, the sensor nodes are resource-controlled and battery-limited. Data should be aggregated to avoid an overwhelming amount of traffic in the network for achieving the conservation of energy and network resources. The main objective of the data aggregation process is the elimination of redundant data transmission and enhancement in the lifetime of energy in WSN. Data aggregation is the process of collecting information from multiple sensor nodes and combining such collected data. The collected data is sent to the base station. Data aggregation is a widely used technique for solving the disintegration and overlap problems in data-centric routing in WSN. Data received from the multiple sensor nodes is aggregated as if they are about the same attribute of the phenomenon when they reach the same routing node on the way to the sink. The data traffic in the WSN can be reduced by transferring the data only when the intensity of the toxic gas reaches a maximum level (the level is predefined depending on the industry and country).

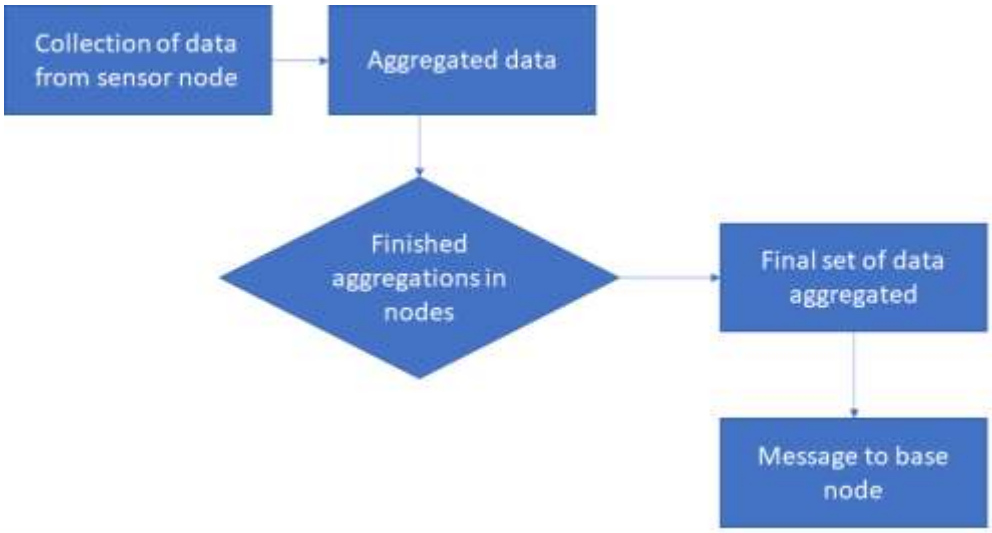

Figure 2: Flow chart of Data Aggregation

This requires aggregation of data. The main goal of the data aggregation is to collect data relating to the toxic gas intensity for improving the network lifetime. The general workflow of the data aggregation is shown in Figure 3.5. Initial information on the intensity of the toxic gas is received from the sensor node and in-network aggregation of the information is performed. It is checked whether aggregation of the sensor information received from all the sensor nodes is performed or not. If aggregation is completed, then the final set of aggregated data is obtained. Otherwise, the collection of toxic gas intensity information is performed again. Finally, the aggregated data is sent to the base station. In our work in-network aggregation is considered for gathering information through a multi-hop network and processing the data at the intermediate 83 nodes. In-network, aggregation is the process of collecting and routing information through a multi-hop network. The sensor with the most critical information aggregates the data packets and sends the aggregated data packets to the sink. Each sensor transmits its signal strength to its neighbors. When the signal strength of the neighbor is high, the sender stops the transmission of the packets. The node having the highest strength becomes the data aggregator, after receiving the packets from all the neighbors. There are two types of approaches for in-network aggregation. In a network, aggregation with size reduction is the process of combining and compressing data received by the sensor node from its neighbors for the reduction of the length of the data packet to be sent to the base station. The number of bits transmitted in the network is reduced and energy conservation is achieved by using this approach. In-network, aggregation without size reduction is the process of combining the data packets received by different neighbors into a single data packet but without processing the value of data. This process also reduces energy consumption and increases the network lifetime. Aggregation of the data is required before the data reaches the base station for reducing the energy utilization in a network. The compromised nodes can perform malicious actions that affect the aggregation results. Here, the packets received from different sources are merged at the intermediate node, and the data redundancies are avoided. The redundant data packets are removed by the intermediate nodes,

DOI: https://doi.org/10.54216/IJWAC.060201
Received: September 03, 2022 Accepted: November 18, 2022

thereby reducing the number of packets routed toward the destination. This implicitly reduces the network traffic and number of packets to be processed at the destination node. Data aggregation results in the energy-saving effect since the sensor nodes require only a minimum volume of energy for sending data directly to the base station. The energy gain due to data aggregation is high in 84 the network having a large number of sensor nodes. This is due to the optimization of the number of hops from the nodes to the base station. The lifetime of the network is improved and data latency is reduced. With the help of data aggregation, the robustness and accuracy of information obtained by the entire network are improved. Data aggregation is performed for eliminating redundancy in the data collected from the sensor nodes. The traffic load in the network is reduced.

4. Experimental Results and Simulation Environment

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.

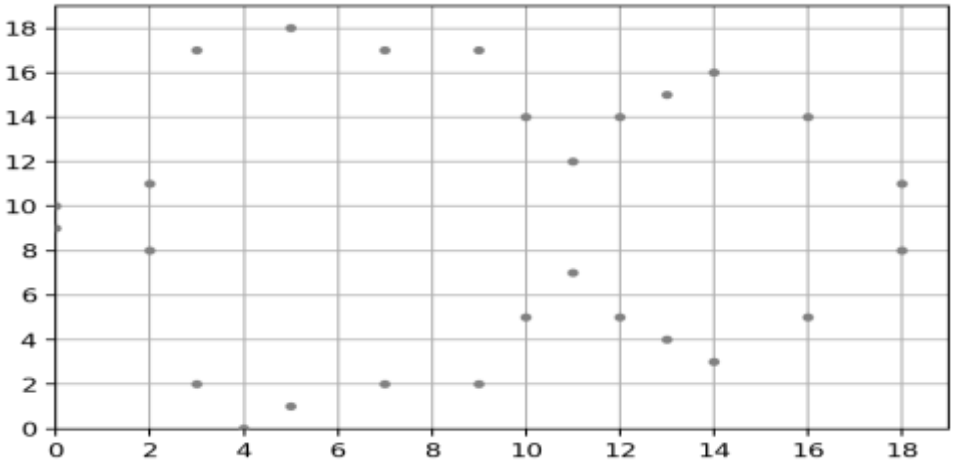

Figure 3: Initial Point Allocation

The evaluation and decryption times of six hybrid encryption calculations with data message lengths ranging from 6 to 18 megabytes are presented.

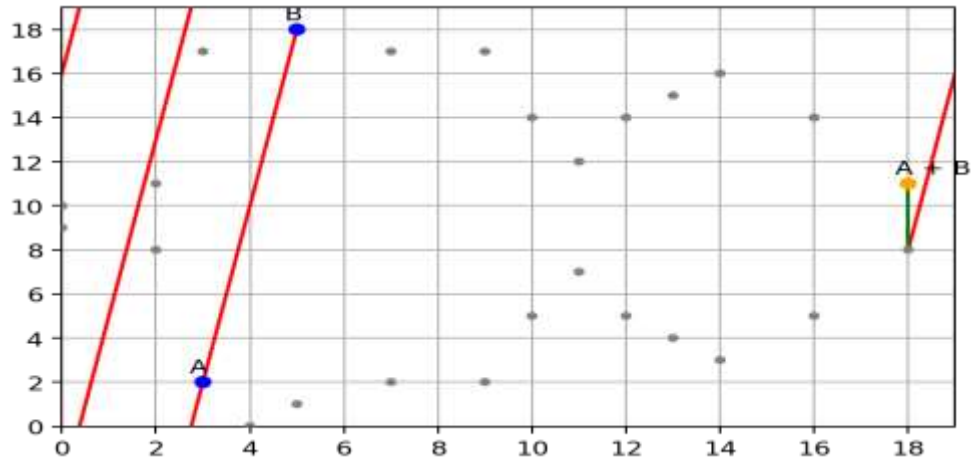

Figure 4: Data aggregation at Each node

For each of the six cross-based cryptographic estimates, the corresponding graphical representation and computation time are shown in Figure 3.

DOI: https://doi.org/10.54216/IJWAC.060201
Received: September 03, 2022 Accepted: November 18, 2022

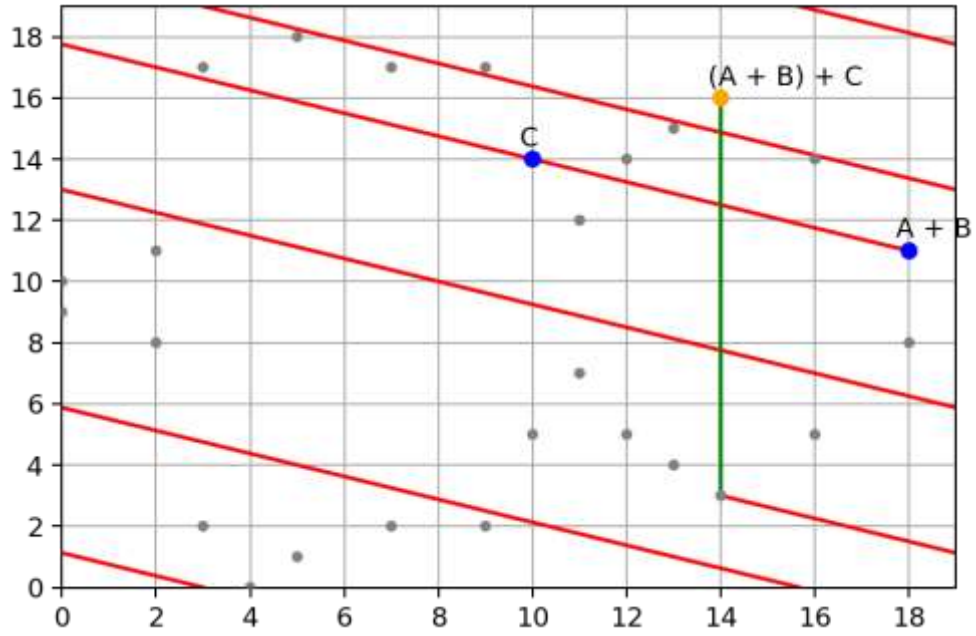

Figure 5: Data Aggregation at point 2

In figure 5, the different lengths of the data messages of the five message sizes are managed in the x-center, and the consuming processor time is in the y-center.

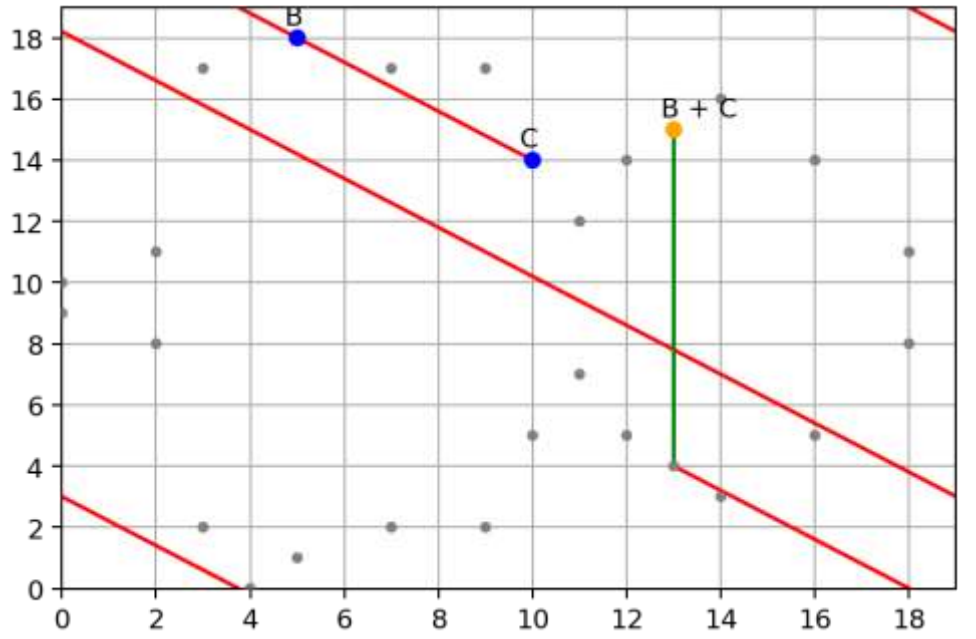

Figure 6: Data Aggregation at point 3

A graphical representation that is nearly identical to the separation time of the six cross-based cipher computers is shown in Figure 6

DOI: https://doi.org/10.54216/IJWAC.060201
Received: September 03, 2022 Accepted: November 18, 2022

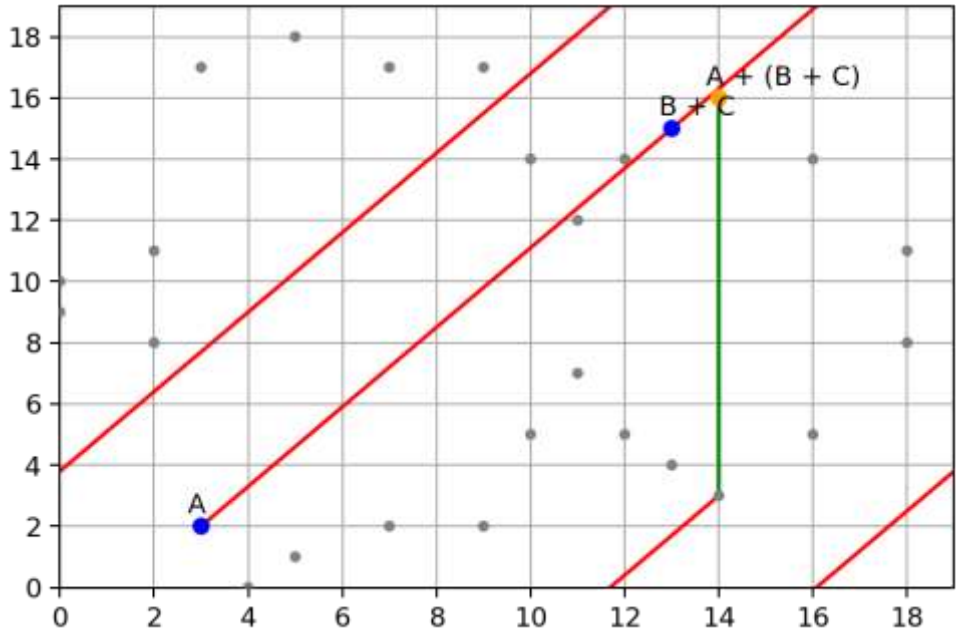

Figure 7: Data Aggregation at point 4

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 Figure 7 as much as possible in the proposed model.

5. Conclusion

In this research paper WSN security is the major concern for Smart Environment. Due to the three-stage nature of the system being discussed, the gatecrasher will never publish assessments of it. The initial implementation made use of REA, the following implementations made use of HFEA, and the final implementation made use of e-RSA. There are presently only two or three trans-based encryption algorithms, and each of them takes much longer to calculate than the coordinated approach. The inspired technique has changed from its original estimations, yet it still outperforms them throughout the projected time off. These analyses were based on previously published computations that uses current mole encryption algorithms. The main problem with these tests is the limit of single evaluation or computing time, and the suggested cream structure stands out as a barrier to that limit. The maximum possible visual output of the suggested Cream variant is limited by factors such as the length of the ciphertext, the amount of energy gained, and other constraints. This investigation may consist of many stages. checking out the sensor's energy gain, the concatenated packets' reach, and the ciphertext's length.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

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.

DOI: https://doi.org/10.54216/IJWAC.060201
Received: September 03, 2022 Accepted: November 18, 2022

[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.

DOI: https://doi.org/10.54216/IJWAC.060201
Received: September 03, 2022 Accepted: November 18, 2022

[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.

DOI: https://doi.org/10.54216/IJWAC.060201
Received: September 03, 2022 Accepted: November 18, 2022