Elliptic Curve Cryptography Based Security And Cluster Based Routing In WBAN

Mrs. R. Latha[1], K. Abirami Sundhari[2], B. Haripriya[3],G. Kalaiarasi[4]

[1, 2, 3, 4] Dept of ECE

[1, 2, 3, 4] Muthayammal Engineering College, Rasipuram

Abstract- *The emergence of wireless body area network (WBAN) technology has brought hope and dawn to solve the problems of population aging, various chronic diseases, and medical facility shortage. The increasing demand for real-time applications in such networks, stimulates many research activities. WBANs are a variant of Wireless Sensor Networks (WSNs) which consist of a few tiny sensors implanted inside the body or located on the body to typically observe physiological signals emanating from different body organs, body motions as well as the surrounding environment. The network is designed in such a way that the coordinating device communicates with implanted and on-body sensors as well as with the access point which further transmits the collected information to a base station. The collected information from the nodes are transferred to the cluster head(CH) during routing, The collected information is encrypted using elliptic curve cryptography and the encrypted data is saved in the server and accessed by the application provider by decrypting the data.*

***Keywords*-** Wireless Body Area Network(WBAN), Elliptic Curve Cryptography(ECC)

I. INTRODUCTION

Elliptic curve cryptography (ECC) is a smart way to keep secrets safe using some special math tricks. Imagine Bob wants to send secret medical information to Alice. They use a special code that has two keys - one to lock the information and another to unlock it. But there's a twist: the keys are different! One key is for locking, and the other is for unlocking. This is like Bob having a special padlock to lock the information and Alice having a different key to open it. Now, imagine there are little devices, called nodes, that collect the medical info. These devices are like little robots running on batteries. They can't recharge, so it's super important to use their energy wisely. There's a clever plan called LEACH that helps manage their energy so they can work efficiently. LEACH is like a boss telling the robots how to organize themselves so they don't waste energy. Each little robot has three jobs: first, it collects the medical info, then it processes it, and finally, it sends it to where it needs to go. These jobs are like steps in a recipe for making a cake - first, you gather ingredients, then you mix them, and finally, you bake the cake. When we put all these ideas together, we see how ECC, the special code, and LEACH, the energy-saving plan, work together to keep secrets safe and make sure our little robots can do their jobs without running out of energy.

II. IDENTIFY,RESEARCH AND COLLECT IDEA

To ensure secure and efficient data transmission in WBANs, this research focuses on integrating Elliptic Curve Cryptography (ECC) and cluster-based routing. ECC provides robust encryption methods with shorter key lengths, making it suitable for resource-constrained WBAN devices. Cluster-based routing optimizes energy consumption by organizing sensors into clusters with a designated cluster head responsible for data aggregation and transmission.

III. WRITE DOWN YOUR STUDIES AND FINDINGS

A. Elliptic Curve Cryptography (ECC) in WBAN Security

Elliptic Curve Cryptography (ECC) serves as a cornerstone for ensuring robust security measures within Wireless Body Area Networks (WBANs). In the context of WBANs, ECC offers a powerful cryptographic solution that effectively addresses the critical need for secure data transmission, particularly concerning sensitive health information. The key advantage of ECC in WBANs lies in its ability to provide a high level of security with relatively smaller key sizes compared to conventional cryptographic systems. This efficiency is particularly vital for WBANs, where resource-constrained wearable devices necessitate optimized computational and storage requirements.

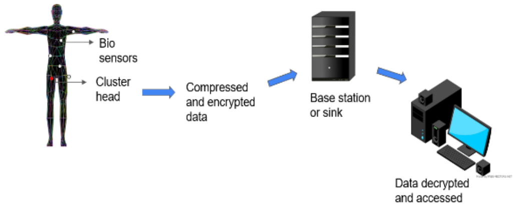


Fig 1: WBAN Security

Elliptic Curve Cryptography (ECC) is a secure way to send messages between two people using two keys: a public key (shared openly) and a private key (kept secret). It uses a special type of math with elliptic curves to make encryption strong. With ECC, messages can be safely encrypted by anyone with the public key, but only the person with the private key can decrypt and read them. This method is efficient and provides strong security for sending sensitive information like medical data.

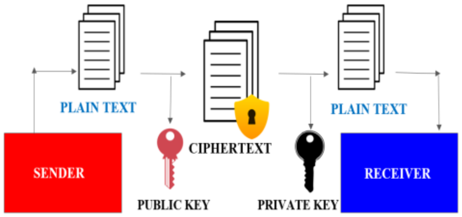


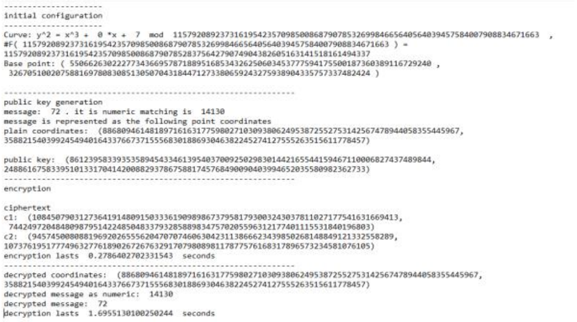
Fig 2. Asymmetric Key Cryptography

B. Cluster-Based Routing in WBAN

Cluster-based routing aims to optimize energy consumption and data flow in WBANs by organizing sensors into clusters. Each cluster has a designated cluster head responsible for data aggregation, processing, and communication with the base station or access point. This hierarchical structure facilitates organized and streamlined data flow, enhancing the network's efficiency and reliability, particularly in resource-constrained environments.

IV. RESULTS AND DISCUSSION

Elliptic curve cryptography (ECC) is a method for securing communication by using unique points on a special curve as keys. It's like having a secret code that only the right person can decode. ECC is great because it's fast and doesn't need a lot of power, which makes it perfect for small devices like phones or IoT gadgets. Also, when using ECC, it's important to organize data properly and handle small errors carefully to make sure everything works smoothly and securely.



```
---------------------
initial configuration
---------------------
Curve: y^2 = x^3 +  0 *x +  7  mod  115792089237316195423570985008687907853269984665640564039457584007908834671663  ,
#F( 115792089237316195423570985008687907853269984665640564039457584007908834671663 ) =
115792089237316195423570985008687907852837564279074904382605163141518161494337
Base point: ( 55066263022277343669578718895168534326250603453777594175500187360389116729240 ,
 32670510020758816978083085130507043184471273380659243275938904335757337482424 )

--------------------------------------------------------------
public key generation
message:  72 . it is numeric matching is  14130
message is represented as the following point coordinates
plain coordinates:  (88680946148189716163177598027103093806249538725527531425674789440583554459 67,
35882154039924549401643376673715556830188693046382245274127555263515611778457)

public key:  (86123958339353589454334613954037009250298301442165544159467110006827437489844,
24886167583395101331704142008829378675881745768490090403994652035580982362733)
--------------------------------------------------------------
encryption

ciphertext
c1:  (108450790312736419148091503336190989867379581793003243037811027177541631669413,
 74424972048480987951422485048337932858898347570205596312177401115531840196803)
c2:  (94574500808819692026555620470707460630423113866623439850268148849121332558289,
107376195177749632776189026726763291707980898117877576168317896573234581076105)
encryption lasts  0.2786402702331543  seconds
--------------------------------------------------------------
decrypted coordinates:  (88680946148189716163177598027103093806249538725527531425674789440583554459 67,
35882154039924549401643376673715556830188693046382245274127555263515611778457)
decrypted message as numeric:  14130
decrypted message:  72
decryption lasts  1.6955130100250244  seconds
```

Fig 3: Encrypting a message using Elliptic Curve Cryptography

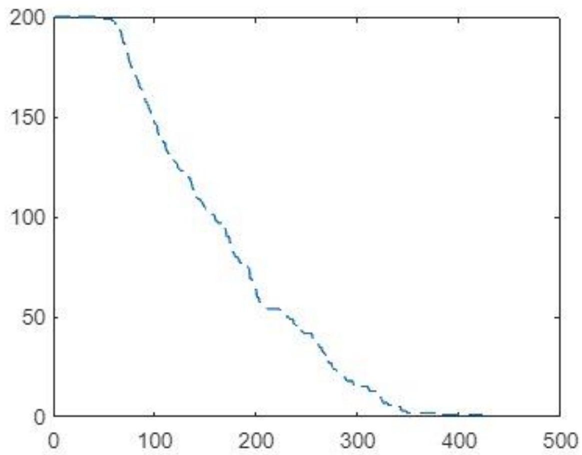
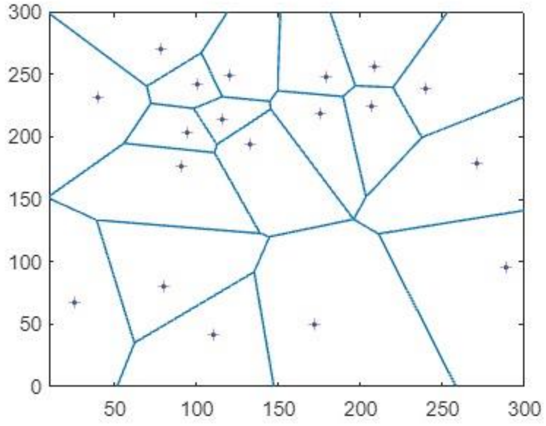


Fig 4: Cluster Formation



V. GET PEER REVIEWED

The proposed integration of ECC and cluster-based routing in WBANs underwent rigorous peer review by experts in the field to ensure the validity, reliability, and quality of the research findings. Feedback from peer reviewers was incorporated to refine the research methodology, enhance the research outcomes, and address potential limitations.

VI. IMPROVEMENT AS PER REVIEWER COMMENTS

Based on the constructive feedback received from the peer reviewers, several improvements were made to the research methodology, findings, and discussion. Clarifications were sought for ambiguous comments, and necessary amendments were made to ensure the research's integrity, quality, and contribution to the field of WBANs.

VII. CONCLUSION

Encrypting data using elliptic curve cryptography is a good way to keep it safe when sending it over a network. ECC is fast and secure, making data transfer quick and efficient. Networks that use a central node, called a cluster head, for managing communication are more organized and use less energy. Prioritizing some sensor nodes can help save even more energy and make the network work better. This could be a good idea to consider for improving networks in the future.

REFERENCES

[1] B. Liu, J. Zhang and Z. Zhu, "Research on Cluster-Based Routing Protocol for Wireless Sensor Networks," 2022 IEEE 5th International Conference on Information Systems and Computer Aided Education (ICISCAE), Dalian, China, 2022, pp. 958-963, doi: 10.1109/ICISCAE55891.2022.9927578.

[2] E. Lara, L. Aguilar and J. A. García, "Lightweight Authentication Protocol Using Self-Certified Public Keys for Wireless Body Area Networks in Health-Care Applications," in IEEE Access, vol. 9, pp. 79196-79213, 2021, doi: 10.1109/ACCESS.2021.3084135.

[3] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-efficient communication protocol for wireless microsensor networks,”2000.

[4] A. Al-Shaikh, H. Khattab, and S. Al-Sharaeh, “Performance comparison of LEACH and LEACH-C protocols in wireless sensor networks,” Journal of ICT Research and Applications, vol. 12, no. 3,2018.

[5] A. Yousaf, F. Ahmad, S. Hamid, and F. Khan, “Performance Comparison of Various LEACH Protocols in Wireless Sensor Networks,” 2019.

[6] A. O. Abu Salem and N. Shudifat, “Enhanced LEACH protocol for increasing a lifetime of WSNs,” Personal and Ubiquitous Computing,vol. 23, no.5–6, 2019.

[7] Y. Tong, “Research and improvement of energy balance in wireless sensor network based on LEACH,” in Journal of Physics: Conference Series, 2021, vol. 1738, no. 1.

[8] S. E. Pour and R. Javidan, “A new energy aware cluster head selection for leach in wireless sensor networks,” IET Wireless Sensor Systems,vol. 11, no. 1, 2021.

[9] P. K. Chithaluru, M. S. Khan, M. Kumar, and T. Stephan, “ETH-LEACH: An energy enhanced threshold routing protocol for WSNs,”International Journal of Communication Systems, vol. 34, no. 12, 2021.

[10] B. Shen, S. Y. Zhang, and Y. P. Zhong, “Cluster-based routingprotocols for wireless sensor networks,” Ruan Jian Xue Bao/Journal of Software, vol. 17, no. 7, 2006.