# IMPROVING PRIVACY AND SECURITY USING LATTICE CRYPTOGRAPHY IN WBAN SYSTEMS

Anupama S[1], Sudheesh S.R[2], Hari S[3]
[1]Student, Master of Technology, Dept. of ECE, [2,3]Asst. Prof., Dept. of ECE,
Mount Zion College of Engineering Kadammanitta, Pathanamthitta, Kerala, India

***Abstract: Wireless communication technology and its applications are important in the case of health-care applications. The advantage and benefits of wireless system became attractive in all kinds of fields. This is mainly due to elimination of the complications of wired connection. The improvement in wireless technology, the Wireless Body Area Network (WBAN) is become more attractive in medical fields.***

***The WBAN uses medical sensors, which are continuously monitors and collect the physiological information of patient's health. In order to send this information to a medical server, it must takesplace data aggregation. In this real-time data transmission, the system must have data security and data privacy [6]. So as to improve privacy with higher data aggregation this proposed scheme develops a lattice cryptographic system. The lattice privacy preserving data aggregation provides more integrity, authentication and consumer privacy.***

***Keywords: WBAN, Real time data transmission, Cryptographic system, Aggregation, Lattice privacy preserving scheme.***

## I. INTRODUCTION

The Wireless Body Area Network (WBAN) [1] is a combination of tiny wearable devices referred to as medical sensors attached to a patient's body in remote health monitoring systems. The WBAN is used to monitor patient's physiological parameters such as temperature, blood pressure, and electrocardiography (ECG) [3]. Medical sensors continuously monitor and collect patient's data and send them to a remote medical server through a local processing unit (LPU) like a PDA/mobile. The WBAN consists of medical sensors and which have scarce resources in terms of memory, energy, and storage also, that communicates wirelessly with an LPU.

The LPU has more resources than sensors but is still limited; as it uses the battery and communicates wirelessly with the medical server. The medical server is very powerful in terms of energy, computational power, and storage. As such, the WBAN is deployed in a hostile environment, where sensors may be incapable of providing reliable functions or can be easily compromised by malicious adversaries; thus sensitive health data may be subject to privacy issues, or data misuse may also occur. In order to overcome the above-stated issues of security and privacy [2] regarding medical health data during transmission and data aggregation in WBAN [5], I propose a lightweight lattice privacy scheme for a remote health monitoring system. With this proposed scheme, it can identify the necessary security and privacy requirements in the WBAN. In particular, I point out the necessity for an end-to-end secure data transmission from medical sensors to the remote medical server in the WBAN. The main contributions of this paper can be summarized below:

- I propose a Robustic and lightweight lattice privacy scheme for remote health monitoring systems. It ensures data confidentiality, data privacy and data authenticity by combining simple encryption scheme and aggregate signature scheme in WBAN[7].
- This scheme uses data aggregation technique at the LPU in WBAN, to reduce the overall communication cost in our proposed scheme.
- I have conducted a security analysis to state and prove the correctness of the proposed scheme.

## II. SYSTEM AND SIGNAL MODEL

Proposed scheme guarantees consumers privacy and messages authenticity and integrity, with reduced communication and computation complexity. In this paper, I propose a lightweight lattice-based homomorphic [9] privacy-preserving data aggregation scheme for health monitoring systems. Compared to existing system, the proposed system offers end to end consumer`s privacy. It also prevents any illegal access and modification of messages. Lattice based algorithm improved the network privacy along with the node energy. The system divided the entire network into small grids and a particular grid is chosen for transmission and security analysis. It is having mainly three phases.

- Initialization: It this phase includes how many bits we are taken for processing. Some security parameters are included here [4].
- Health data generation: It has some keys and is mainly based on lattice algorithm. Also performing message encryption in it.
- Verification: It is an authentication technique. Here, check whether it is able to decrypt or not. Successful decryption can be possible by this system. The block diagram of the system having two phases is shown in Fig. 1.

  

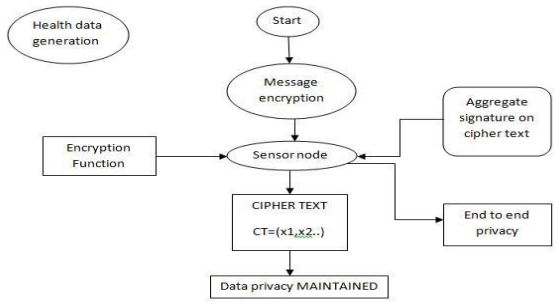


Fig.1: Block diagram of the system (including two phases)

## III. RESULTS AND DISCUSSIONS

Proposed system results shows better performance compared to existing system results and is more advantageous. The green line in the graph represents the existing system output, whereas red line represents the proposed approach. The routing overhead is relatively very small in proposed approach as compared to existing in fig. 2.

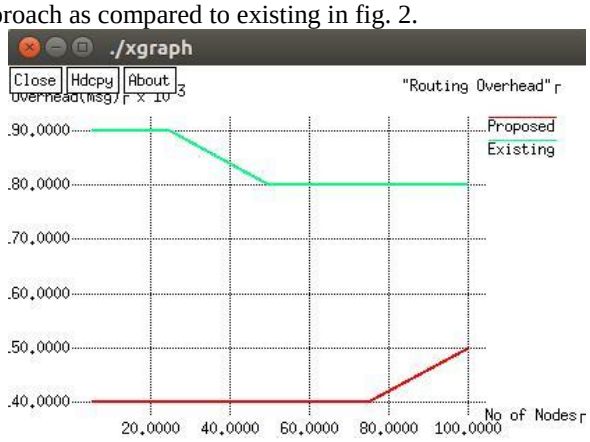


Fig. 2: Routing overhead

Throughput means that the number of bits transmitted per seconds. It shows the efficiency of the system. The efficiency of the lattice based system is higher than that of DBDH and is shown in Fig. 3. Number of packets transmitted per time can be shown in Fig. 4.

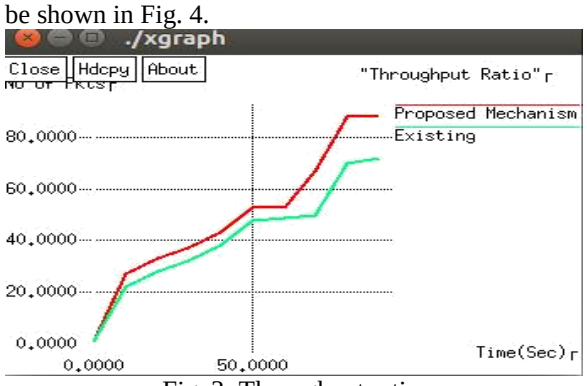


Fig. 3: Throughput ratio

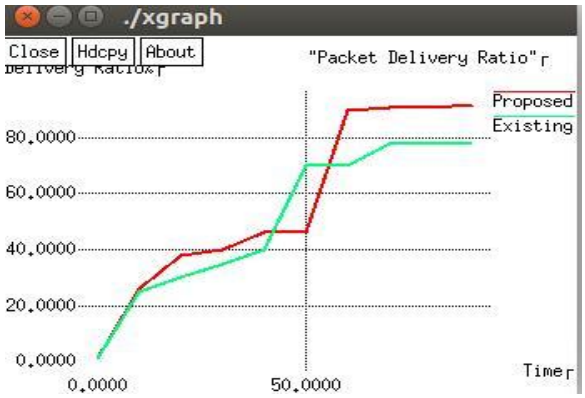


Fig. 4: Packet delivery ratio

The lifetime of a network is important in the case of wireless body area network systems. The life time indicates how long the network is going on for data transmission and is shown in Fig. 5.

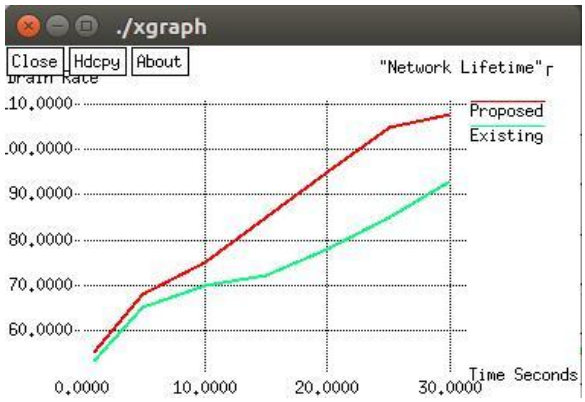


Fig. 5: Network lifetime

The delay is the major disadvantage of the existing approach. It can be decreased in the proposed system as nodes increases. It is shown in Fig. 6.

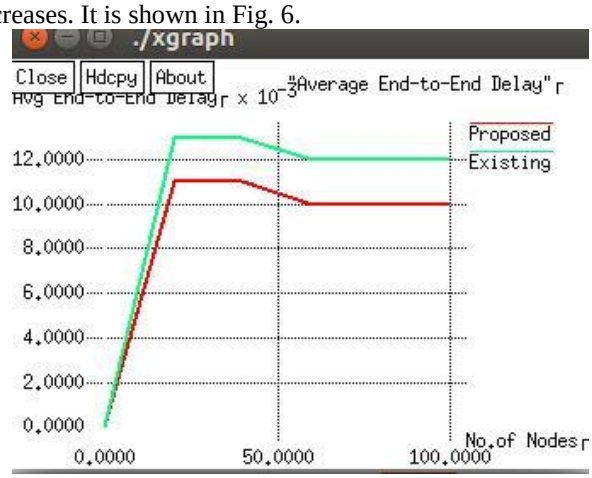


Fig. 6: Average End-to-End Delay

## IV. CONCLUSION

In this paper, I have proposed a Secure Privacy-scheme based lattice cryptography for remote health monitoring systems to improve aggregation efficiency and preserve data privacy. This paper formalizes the system model and security model for the remote health monitoring system. The utilization of privacy homomorphism makes this scheme

  

feasible for applicability in a cloud-assisted WBAN and simple arithmetic operations are used here. Here I considered and implemented a light weighted homomorphic aggregation scheme with more efficient to further reduce communication and computational overhead and improve the efficiency of the proposed scheme.

REFERENCES

[1] Anees Ara, Student Member, IEEE, Mznah Al-Rodhaan, Yuan Tian and Abdullah Al-Dhelaan "A Secure Privacy-Preserving Data Aggregation Scheme based on Bilinear ElGamal Cryptosystem for Remote Health Monitoring Systems“ , 2016 IEEE.

[2] S. Lim, T. H. Oh, Y. B. Choi, and T. Lakshman, “Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring,” Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference on. pp. 327– 332, 2010.

[3] J.-L. Beuchat, J. E. González-Díaz, S. Mitsunari, E. Okamoto, F. Rodríguez Henríquez, and T. Teruya, “High-speed software implementation of the optimal ate pairing over Barreto-Naehrig curves,” Lect. Notes Comput. Sci. (including Subser.Lect. Notes Artif.Intell. Lect. Notes Bioinformatics), vol. 6487 LNCS, pp. 21– 39, 2010.

[4] J. Ren, G. Wu, and L. Yao, “A sensitive data aggregation scheme for body sensor networks based on data hiding,” Pers. Ubiquitous Comput., vol. 17, no. 7, pp. 1317–1329, 2013.

[5] J. Sun, X. Zhu, and Y. Fang, “Preserving Privacy in Emergency Response Based on Wireless Body Sensor Networks,” Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. pp. 1– 6, 2010.

[6] J. Zhou, Z. Cao, X. Dong, and X. Lin, “Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions, and future directions,” IEEE Wirel. Commun., vol. 22, no. 2, pp. 136–144, Apr. 2015.O. Kocabas, T. Soyata, and M. K. Aktas, “Emerging Security Mechanisms for Medical Cyber Physical Systems,” IEEE/ACM Trans. Comput. Biol. Bioinforma., vol. 13, no. 3, pp. 401–416, May 2016.

[7] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, “Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 332–342, Feb. 2014.

[8] S. Han, S. Zhao, Q. Li, C.-H. Ju, and W. Zhou, “PPM-HDA: Privacy-Preserving 37 and Multifunctional Health Data Aggregation With Fault Tolerance,” IEEE Trans. Inf. Forensics Secure., vol. 11, no. 9, pp. 1940–1955, Sep. 2016.

[9] AsmaaAbdallah, and Xuemin (Sherman) Shen, Fellow, `A Lightweight Lattice based Homomorphic Privacy-Preserving Data Aggregation Scheme for Smart Grid`, 2015 IEEE.

  