IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Efficient Concealed Data Aggregation For Multi-Application in Wireless Sensor Networks

[1*]Vivek Prakash Singh, [2*]H. M. Singh, [3*]R. Dileep Kumar and [4*]Km. Nishu
Department of Computer Science & Engineering
SHUATS, Prayagraj, U.P., India

Abstract—In the field of Wireless Sensor Networks (WSNs), Concealed Data Aggregation (CDA) technique is widely investigated for implementation of secure communication over the network. The major advantage in using CDA is that it can perform data aggregation directly on encrypted data prepared for transmission without decrypting them. In this paper, a new approach for Concealed Data Aggregation with the help of NTRU and Gold Technique has been proposed for multi-application environment. NTRU is the only post quantum public key cryptosystem suitable for practical implementation and it performs aggregation on encrypted data without decrypting data due to which the complete process is more secure and effective interns of time complexity. Proposed Efficient Concealed Data Aggregation for Multi-application support enhances systems capability achieving higher throughput.

Keywords**—**Concealed Data Aggregation(CDA), CDA for Multi-Applicationa, NTRUEncrypt technique, Gold code.

I. INTRODUCTION

Wireless sensor network (WSN) has emerged as one of the most promising technologies for the future. Wireless sensor networks (WSNs), as distributed networks of sensors with the ability to sense, process and communicate, have been increasingly used in various fields including engineering, health and environment, to intelligently monitor remote locations at low cost. Sensors in such networks are responsible for four major tasks: data aggregation, sending and receiving data, and in-network data processing. The innovation in technology and availability of small, inexpensive, and smart sensors resulting in cost effective and easily deployable WSNs. However, researchers must address a variety of challenges to facilitate the widespread deployment of WSN technology in real-world domains [1]. A WSN is a network that is made up of hundreds or thousands of sensor nodes which are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or pre-determined, so that it leads to random deployment in inaccessible terrains or disaster relief operations. On the other hand, this poses a challenge that sensor network devices, protocols and algorithms must possess self-organizing capabilities [2] like data aggregation, routing, data security etc. Although data aggregation could significantly reduce transmission, it is vulnerable to some attacks. For instance, compromising a CH will allow adversaries to forge aggregated results as similar as compromising all its cluster members. To solve this problem, several studies, such as the delay aggregation, SIA, ESPDA, and SRDA, have been proposed. In this paper, the proposed scheme, called ECDAMA, provides CDA between multiple groups. Basically, we also suppose three practical application scenarios for ECDAMA, all of which can be realized by only ECDAMA. The first scenario is designed for Network Formation in WSNs. In practice, sensor nodes having different purposes, e.g., smoke alarms and thermometer sensors may be deployed in the same environment. If we apply conventional concealed data aggregation schemes the ciphertexts of different applications cannot be aggregated together; otherwise, the decrypted aggregated result will be incorrect. The only solution is to aggregate the ciphertexts of different applications separately. As a result, the transmission cost grows as the number of the applications increases. By ECDAMA, the ciphertexts from different applications can be aggregated into “only” one ciphertext. The second scenario is designed for finding the optimal path towards base station using enhanced “Dijksta algorithm”. In comparison to conventional schemes, ECDAMA finds an optimal path for better communication. And re-clustering of nodes takes place at regular intervals as sensor nodes involved in aggregation and transmission, become weaker. The last scenario is designed for secure communication in efficient manner by using NTRUEncrypt that takes less operation modules, more secured and effective in terms of time complexity.

II. Homomorphic Encryption and Related Work

Homomorphic Encryption

Homomorphic encryption is a form of encryption that allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. A cryptosystem that supports *arbitrary computation* on ciphertexts is known as fully homomorphic encryption (FHE) and is far more powerful. Such a scheme enables the construction of programs for any desirable functionality, which can be run on encrypted inputs to produce an encryption of the result. Since such a program need never decrypt its inputs, it can be run by an untrusted party without revealing its inputs and internal state. Elliptic curve cryptosystem is a semi homomorphism cryptosystem supporting only additive and multiplicative operations. Whereas NTRU is a fully homomorphic cryptosystem supporting any desirable operations.

NTRU Encryption Algorithm - NTRU is an open source public-key cryptosystem that uses lattice-based cryptography to encrypt and decrypt data. It consists of two algorithms: NTRUEncrypt, which is used for encryption, and NTRUSign, which is used for digital signatures. Unlike other popular public-key cryptosystems, it is resistant to attacks using Shor's algorithm and its performance has been shown to be significantly better. Unlike RSA and Elliptic Curve Cryptography, NTRU is not known to be vulnerable to quantum computer based attacks.

Gold Code Encryption Algorithm -Gold Codes [11] are sequences of 0's and 1's. Gold codes based on XOR and Shift registers. Linear feedback shift registers (LFSR) are called state machines, whose components and functions are:

- The **shift register** - shifts the bit pattern and registers the output bit and
- The **feedback function** - computes the input bit according to the tap sequence and inserts the computed bit into the input bit position.

The output sequence of bits forms pseudo-random binary sequences, which are completely controlled by the tap sequence. A tap sequence defines which bits in the current state will be combined to determine the input bit for the next state. The combination is generally performed using module-2 addition (⋆ - XOR). This means that adding the selected bit values defined by the tap sequence, if the sum is odd the output of the function is one; otherwise the output is zero.

Related Work

K. El Makkaoui et al [3] proposed a fully homomorphic encryption scheme which supports both multiplicative and additive homomorphic operations. Since then, several fully homomorphic encryption schemes have been proposed. However, the fully homomorphic encryption schemes are still undergoing experimentation and improvement. The hybridization of homomorphic encryption schemes seems to be an effective way to overcome their limitations and to benefit from their resistance against the confidentiality attacks. Peidong Sha and Zhixiang Zhu [4] designed an encryption system that, firstly discriminates whether the values of the public key and private key generated during the encryption process contain prime number, then combines with the Pascal's triangle theorem and RSA algorithm model and inductive methods to construct a new cryptosystem that meets homomorphic computation of some operations on cihpertexts (e.g., additions, multiplications), Thus the new cryptosystem satisfies fully homomorphic encryption in cloud computing. Liquan Chen, Hongmei Ben, Jie Huang [7] propose a re-encryption optimization scheme over the given arbitrary function, which designs a depth threshold value and do function decomposition while the depth value of given function is deeper than the designed depth threshold value. Then, an encryption depth optimization fully homomorphic encryption (EDO-FHE) scheme is constructed. Based on analysis results, the complexity of the EDO-FHE scheme is far less than the DGHV scheme. It greatly improved the efficiency of the fully homomorphic encryption scheme, while the security is also proved based on the approximate GCD problem. And Ningduo Peng et al [8] propose a fast homomorphic encryption scheme for vector data. In the scheme, vector data is transformed to specific bit strings such that addition of two plaintexts could be completed by just a simple XOR operation over the corresponding ciphertexts. Experiments show that the new scheme is about 30% faster than the current fastest homomorphic encryption scheme.

III Proposed Work

The main objective of this research work is to develop efficient concealed data aggregation method that support multi-applications in wireless sensor network. Fully homomorphic fast encryption technique named as NTRU cryptosystem used to perform data aggregation in ciphertext and Gold Code technique is used to combine data of multiple applications. The highlighting advantages of NTRU cryptosystem are-

- No integer factoring nor discrete logs
- Seems to resist practical attacks
- Seems to resist quantum attacks

The proposed efficient CDAMA method performs secure and fast sinking of multi-application data in three basic steps as shown in Fig. x

A. Network Clustering
B. Tree Structure Formation
C. Efficient Concealed Data Aggregation with Multi-application.

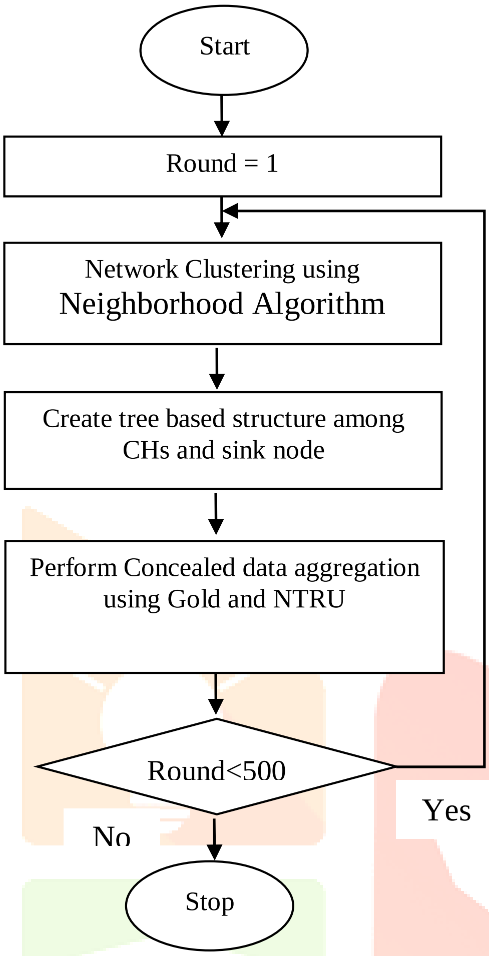
Start
Round = 1
Network Clustering using Neighborhood Algorithm
Create tree based structure among CHs and sink node
Perform Concealed data aggregation using Gold and NTRU
Round<500
Yes
No
Stop

Figure 3.3.1 Proposed Flowchart

A. Network Clustering

Firstly, the network is clustered using neighbor clustering. In neighbor clustering, cluster head election is not done in each round when cluster energy below than threshold then election is performed. Clustering divided into three parts:

- If distance is less than 450 and greater than 1000 then on the basis of distance and number of neighbor.
- If distance between them then choose energy and cluster head distance.

B. Tree Structure Formation

Secondly, tree structure is formed using energy efficient based dijkstra algorithm. It chooses the node under pre-specified threshold radius. After that find the optimal shortest path over the cluster head.

C. Efficient Concealed Data Aggregation with Multi-application

Finally, all aggregator node is ready to send data to sink node in a secure way. For that, efficient concealed data aggregation is used for secure transmission, and during transmission we used NTRU encryption and gold code algorithm. After selection of cluster head by using neighborhoods clustering techniques then apply Dijkstra algorithm to find optimal shortest path over the clusters heads then gold cold algorithm to generate binary bit sequence by controlled through tap sequence due to the output sequence of bits from pseudo-random binary sequences, which are completely controlled by the tap sequences because a tap sequence defines which bits in the current state will be combined to determine the input for the next state. Then perform XOR operation because the combination is generally performed using module-2 addition (*, XOR) this means that adding the selected bits values defined by the tap sequence, if the sum is odd the output of the function is one: otherwise output is zero then m-sequence message is generated now apply NTRUEncrypt algorithm on this m-sequence message for sending data in encrypted form then aggregated encrypted data from each sensor node to his cluster head then sink all nodes to base station. The proposed CDAMA technique performs operation in two phases, Gold Code sequence set up and NTRUEncrypt Homomorphic.

The proposed scheme, called CDAMA with NTRUEncrypt, provides Concealed Data Aggregation (CDA) between multiple groups. In Sensor Node (SN) having different purposes, e.g., smoke alarms, temperature, heat sensors may be deployed in the same environment. So, by the existing concept of CDAMA, we studied that ciphertext from different applications can be encapsulated into “only” one ciphertext. But at the same time it is difficult to differentiate at the Cluster Heads. So, to differentiate multiple groups with this CDAMA with NTRUEncrypt as shown in figure no. 3.3.2 technique we perform Gold sequence Code which has ability to differentiate multiple groups at the Base station.

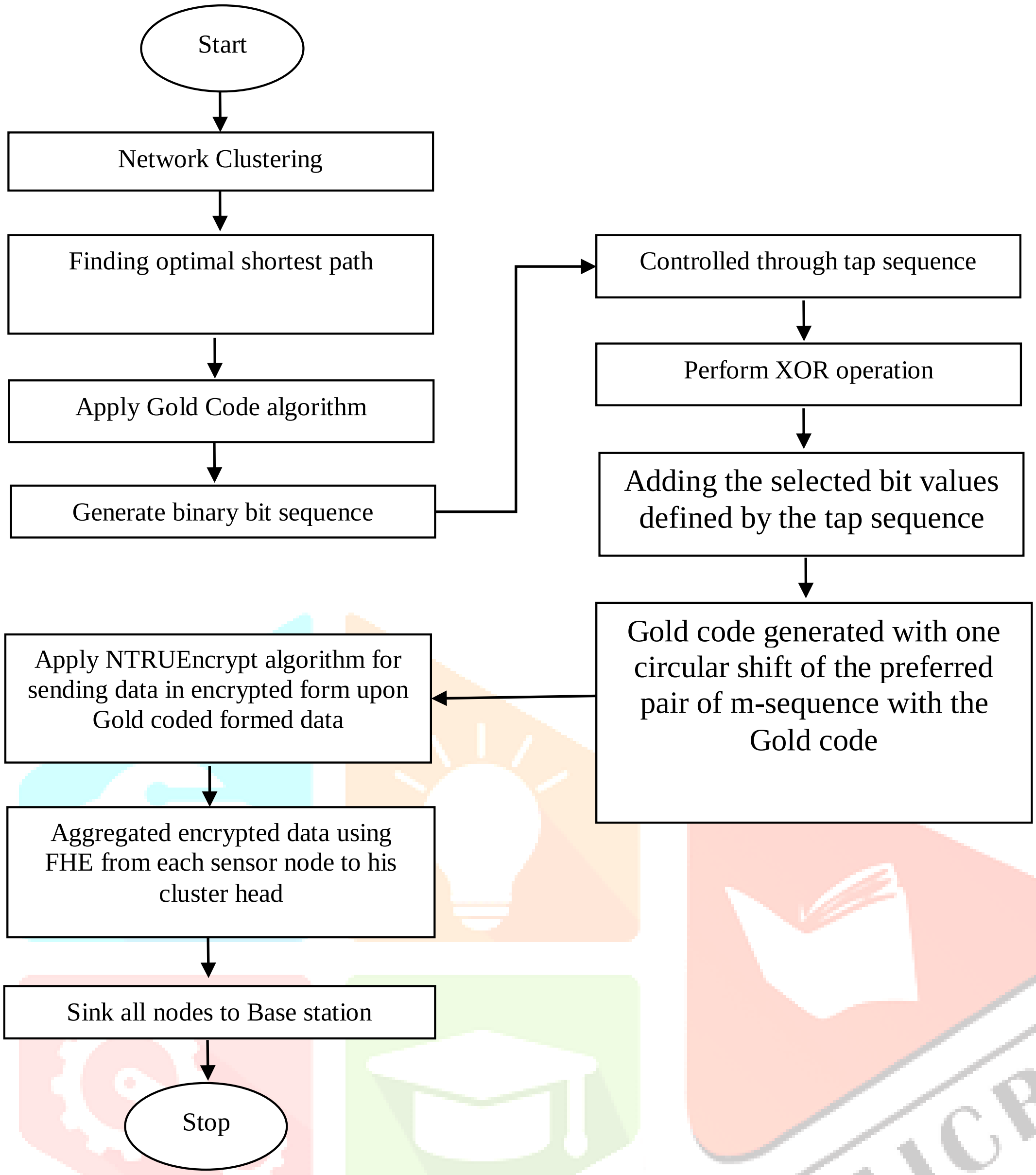
Start
Network Clustering
Finding optimal shortest path
Apply Gold Code algorithm
Generate binary bit sequence
Controlled through tap sequence
Perform XOR operation
Adding the selected bit values defined by the tap sequence
Gold code generated with one circular shift of the preferred pair of m-sequence with the Gold code
Apply NTRUEncrypt algorithm for sending data in encrypted form upon Gold coded formed data
Aggregated encrypted data using FHE from each sensor node to his cluster head
Sink all nodes to Base station
Stop

Figure no. 3.3.2 Flowchart of NTRU

Gold codes is fully based on XOR and shift register as shown figure no. 3.3.3. Gold codes convert the input into the binary sequence by using some polynomial parameters, then it

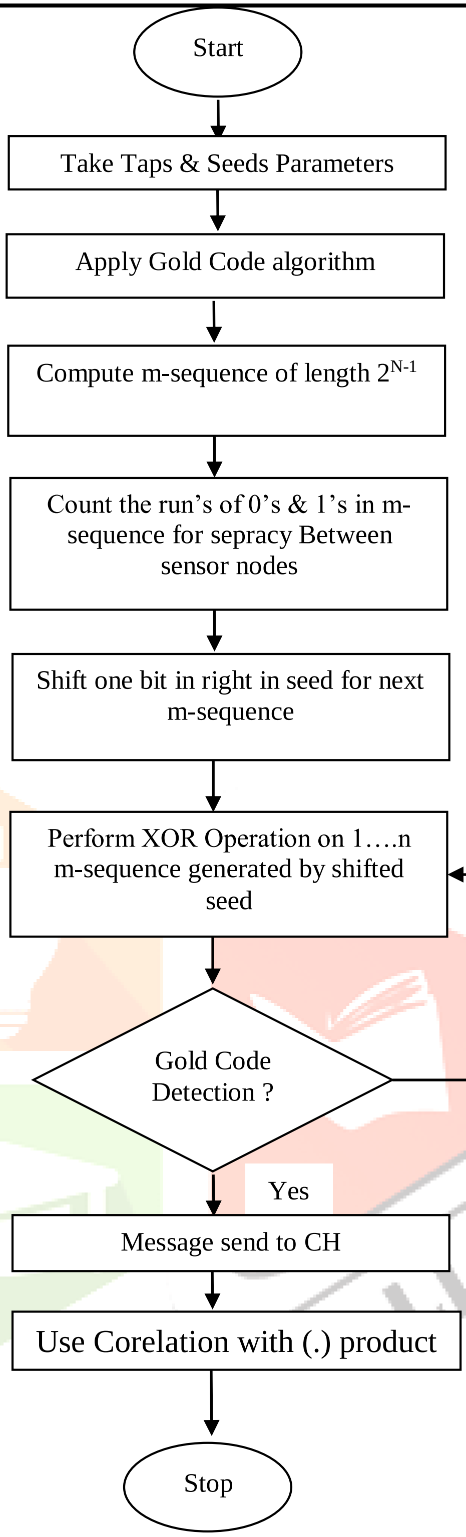
Start
Take Taps & Seeds Parameters
Apply Gold Code algorithm
Compute m-sequence of length 2^N-1
Count the run's of 0's & 1's in m-sequence for sepracy Between sensor nodes
Shift one bit in right in seed for next m-sequence
Perform XOR Operation on 1….n m-sequence generated by shifted seed
Gold Code Detection ?
No
Yes
Message send to CH
Use Corelation with (.) product
Stop

Figure no. 3.3.3 Flowchart of Gold Code

finds the LFSR, LFSR taps are described by a characteristic polynomial, which is generated by the binary sequence,(e.g., 1 + x3 + x5) Taps in columns 3 and 5, 1 is not a tap but corresponds to the input to the first bit x0), the initial contents of the LFSR are called the seed, always use 00001 to first LFSRs, then we got first maximum length shift register sequence (MLSRs), it is repeated after 2^N-1 steps, in next step we shift our seed to the Right 00010 with binary bits of next applications and perform the operation as earlier then we got another MLSRs after that we did the runs of 0's and 1's to maintain the consistency between the multiple groups, and perform XOR operations on MLSRs generated by different taps then we get Gold code where each code is quite different than others, for Gold sequence detection first read the bit sequence and then used correlation : all possible dot product then highest correlation indicates detected Gold code. After Gold Sequence code done, all SNs forward the results to the corresponding Clusters heads then all messages is encrypted via NTRUEncrypt homomorphic algorithms, to increase the security and improve network lifetime, cluster networks force the intermediate nodes to perform aggregation, i.e., to be aggregators (AG). By the use this algorithm NTRUEncrypt the preferred pair of m-sequence with Gold code to ciphertext, after encrypting the plaintext to ciphertext then NTRU perform aggregation using on the base station through the Fully Homomorphic Encryption (FHE) technique, on the cluster head take two ciphertext C1 & C2 as a input then call FHE technique for C1 and C2 perform modular addition on C1 & C2 and get C3 (C1+C2=C3) then we again check for the next corresponding ciphertext with C3 and then forward to the Cluster Heads. Because NTRU is inherently follow the properties of Privacy Homomorphism (PH). In figure no.3.3.4, the proposed work is explained by the example of ECDAMA with NTRU and Gold.

Proposed Algorithm:

1. Start
2. Initialize the network
3. Form clusters using Neighbor clustering Technique and Recognize cluster head
4. If energy level of cluster head is below specified threshold, then re-elect cluster head using n^{th} nearest node as cluster head using distance parameter.
5. Now find the shortest path of cluster heads to base station through Dijkstra algorithm
6. a)Apply Gold code algorithm to generate binary bit sequence of signals generated by sensor nodes which may generate signals of different application
   b)Performs XOR operation between bits to maintain uniqueness between signals
   c)If sum is odd then output function is '1' otherwise '0'.
   d)Generate gold code of m-sequence.
7. Apply NTRUEncrypt algorithm to encrypt code for secure data transmission
8. Aggregate encrypted data toward cluster head
9. Using Shortest path identified forward aggregate data to Base station
10. Stop.

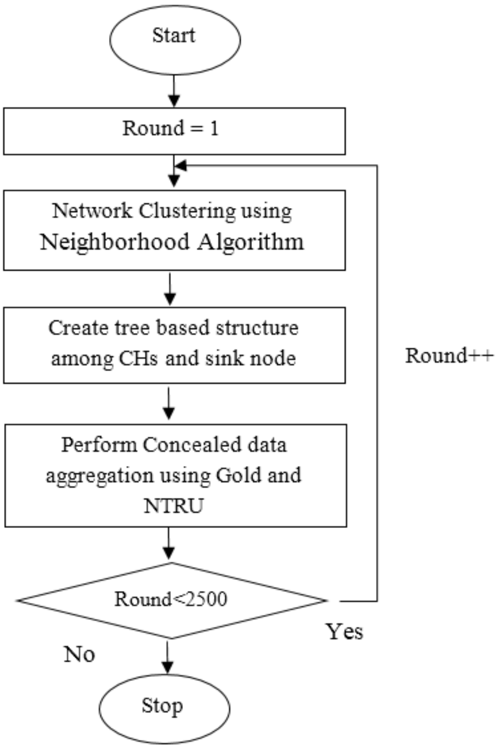
Start
Round = 1
Network Clustering using Neighborhood Algorithm
Create tree based structure among CHs and sink node
Perform Concealed data aggregation using Gold and NTRU
Round<2500
Yes
No
Round++
Stop

Fig. 3.1 Flowchart of Proposed Work

III. RESULT ANALYSIS

In the result analysis, the experiment of proposed work performed by using MATLAB tool. Firstly perform Neighbor clustering to create clusters then Dijkstra algorithm to find optimal path and NTRU Gold Code method for secure data transmission.

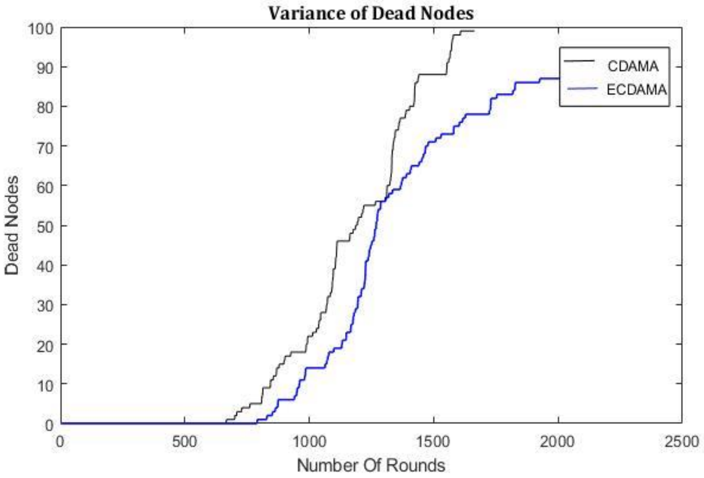

Figure 3.1: Variance of Dead Nodes

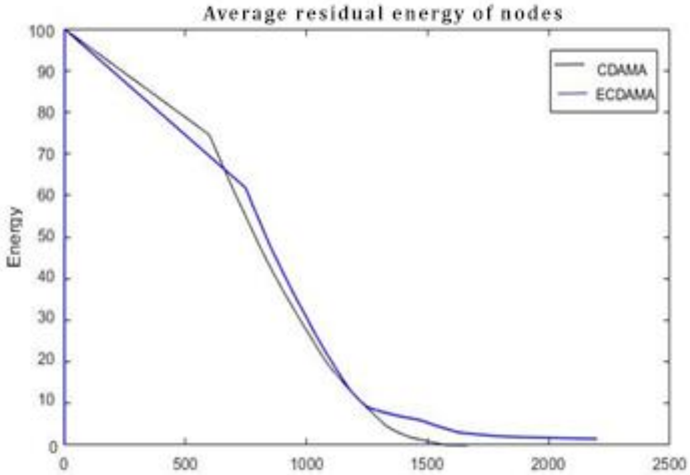

Figure 3.2: Average residual energy of nodes

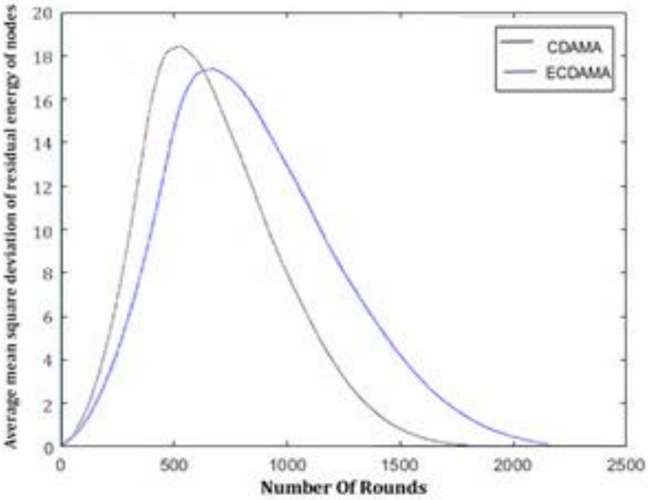

Figure 3.3 Average mean square deviation of residual energy of nodes

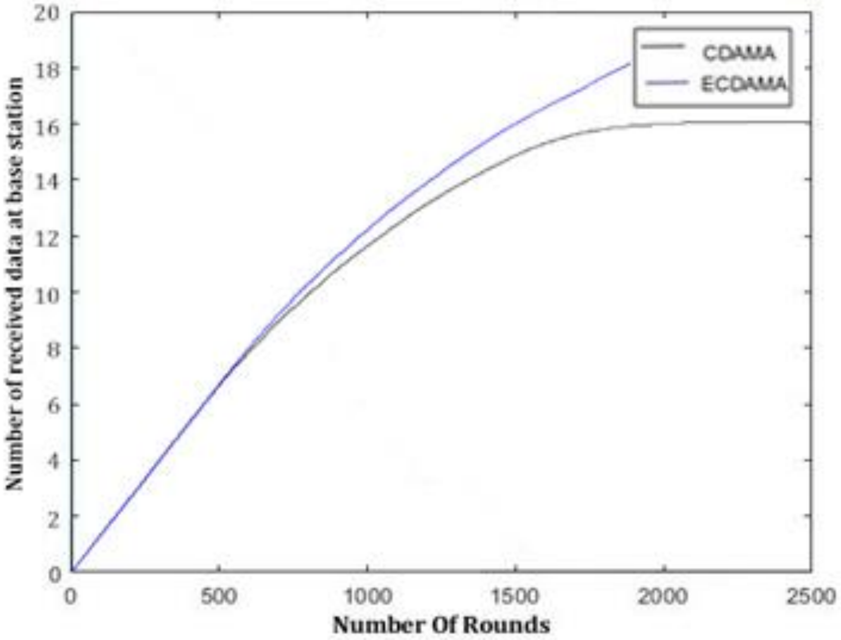

Figure 3.4 Number of received data at base station

IV. Conclusion

The current system for data aggregation in sensor networks, CDAMA technique, uses ECC approach which do not ensure security combined with high rate data transmission. Power optimization based on optimal path selection is a major concern/ issues in WSNs. Therefore, after the detailed study of pros and cons of CDAMA, it has been proposed a secure model that enhance the security level for sending multiple data in WSNs with higher transmission rate. To achieve high security NTRUEncrypt algorithm in combination with Gold Code, has been used and Dijkshtra's algorithm has been applied in finding shortest path between cluster heads and base station. A comparative experiments conducted to analyze CDAMA and ECDAMA approaches and results are assessed using MATLAB graphs.

References

[1] Rawat, P., Singh, K. D., Chaouchi, H., & Bonnin, J. M., "Wireless sensor networks: a survey on recent developments and potential synergies", The Journal of Supercomputing, 68(1), 2013, pp.1–48.

[2] R.Mehala and Dr.A.Balamurugan, "An Efficient Data Aggregation Scheme and Cluster Optimization in Wireless Sensor Networks", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 3, March 2015, pp. 1706-1712.

[3] El Makkaoui, K., Beni-Hssane, A., & Ezzati, A. (2016). Can hybrid Homomorphic Encryption schemes be practical? 2016 5th International Conference on Multimedia Computing and Systems (ICMCS).

[4] Sha, P., & Zhu, Z. (2016). The modification of RSA algorithm to adapt fully homomorphic encryption algorithm in cloud computing. 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS).

[5] P. Nayak , D. Anurag , A fuzzy logic based clustering algorithm for WSN to ex- tend the network lifetime, IEEE Sens. J. 16 (1) (2015) 137–144 .

[6] Zhao, Y., Pan, Y., Wang, S., & Zhang, J. (2014). An anonymous voting system based on homomorphic encryption. 2014 10th International Conference on Communications (COMM).

[7] Chen, L., Ben, H., & Huang, J. (2014). An Encryption Depth Optimization Scheme for Fully Homomorphic Encryption. 2014 International Conference on Identification, Information and Knowledge in the Internet of Things.

[8] Ningduo Peng, Guangchun Luo, Ke Qin, & Aiguo Chen. (2013). A fast additively symmetric homomorphic encryption scheme for vector data. Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC).

[9] Zhang et al., "An Energy Saving Routing Algorithm Based on Dijkstra in Wireless Sensor Networks", Journal of Information & Computational Science, 10:7 (2013), pp. 2087–2096.

[10] https://en.wikipedia.org/wiki/NTRUEncrypt.

[11] http://sepwww.stanford.edu/data/media/public/docs/sep136/claudio1/paper_html/node3.html