Secure Data Transmission through Gold Coded and NTRUEncrypt Encryption Algorithm in Clustering Environment

Kumari Nishu[1], Vivek Prakash Singh[2]

[1]*M.Tech CSIT, Dept. of Computer Sciences & Information Technology, Vough Institute of Engg. and Technology, SHUATS, Allahabad, India*
[2]*M.Tech CSIT, Dept. of Computer Sciences & Information Technology, Vough Institute of Engg. and Technology, SHUATS, Allahabad, India*

---***---

Abstract*—In this paper, we present optimal path selection based on Dijkstra's algorithm. Here cluster election not done in each round it elect cluster head when energy level goes below threshold value. We proposed a secure model, which is used to fuzzy c-means based clustering algorithm to elect the cluster head, optimal path selection using Dijkstra's algorithm and NTRU encryption algorithm with Gold Code for security.*

Keywords—Wireless sensor network, Fuzzy C-Means Clustering, Dijkstra, NTRUEncrypt technique, Gold code.

1. INTRODUCTION

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. Wireless sensor network (WSN) has emerged as one of the most promising technologies for the future. This has been enabled by advances 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 protocols and algorithms must possess self-organizing capabilities [2].

2. LITERATURE SURVEY

M. Mirzaie, S.M. Mazinani [2017] This article presents an adaptive multiclustering algorithm based on fuzzy logic (Adaptive MCFL) to lessen energy consumption in wireless sensor network nodes. The Adaptive MCFL algorithm clusters sensor nodes in different rounds using different clustering algorithms, and without selecting any nodes as cluster heads in some rounds, it has been able to reduce the number of transmitted messages from each node to other nodes and to the base station, saving more energy in the network. This algorithm has been compared to some other algorithms in three scenarios. Simulation results show the reduction of energy consumption and saving more energy within the network. [3]

K. El Makkaoui et al [2016] 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. In this paper, we will study the possibility to hybridize the homomorphic encryption schemes so as to support all homomorphic properties.[4]

PeidongSha and Zhixiang Zhu [2016]design a encryption system, this encryption system 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.[5]

The next method [2015] is a fuzzy-based clustering algorithm too. In this method, as in LEACH, cluster heads are selected according to the value of the threshold. In the next step, using fuzzy parameters such as residual energy, movement of the base station, and cluster centrality, a cluster head is selected. Then, cluster heads receive data from other surrounding nodes, aggregate them, and transmit them to the cluster head. And finally the cluster head transmits the received data to base station. Results of simulation reveal that this protocol outperforms LEACH protocol in terms of energy consump- tion and network lifetime. This method uses a two-level clustering with a great impact on reducing energy consumption. [6]

Yingming Zhao et al [2014] In this paper we present an electronic voting system based on Homomorphic encryption to ensure anonymity, privacy, and reliability in the voting. Homomorphic encryption is a subset of privacy homomorphism. It is capable of computing the encrypted data directly and also encrypting the result of the operation automatically. For this reason it has a wide range of applications including secure multi-party computation, database encryption, electronic voting, etc. In this paper, we make use of the homomorphic encryption mechanism to design and implement an electronic voting system that supports the separation of privileges among voters, tellers, and announcers.

Our experimental results show the system not only ensures anonymity in voting but also presents cheating during the counting process.[7]

Liquan Chen, Hongmei Ben, Jie Huang [2014] 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 proposed 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.[8]

NingduoPeng et al [2013] propose a fast homomorphic encryption scheme for vector data. In the scheme, vector data are 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. In comparison with the prior works, the new scheme is more suitable for dealing with a large number of encrypted data in relational table.[9]

3. PROPOSED METHODOLOGY

3.1 Fuzzy C-Means Clustering Algorithm

The FCM employs fuzzy partitioning such that a data point can belong to all groups with different membership grades between 0 and 1. This algorithm works by assigning membership to each data point corresponding to each cluster center on the basis of distance between the cluster center and the data point. More the data is near to the cluster center more is its membership towards the particular cluster center. Clearly, summation of membership of each data point should be equal to one. After, each iteration membership and cluster centers are updated according to the formula [10].

3.2 Dijkstra Algorithm

The Dijkstra algorithm [11] is a well known shortest routing algorithm with high precision to get the shortest path from the origin point to object point in a network and is widely applied in many fields such as data structure, graph theory, and operational research. In many previous researches, the Dijkstra-based routing algorithms are usually employed to get the shortest distance between two nodes in a WSN, and in general, the evaluation index of distance, the weight of the connective adjacent nodes is the physical distance between those two nodes.

3.3 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.

The NTRUEncrypt public key cryptosystem, also known as the NTRU encryption algorithm [12], is a lattice-based alternative to RSA and ECC and is based on the shortest vector problem in a lattice (which is not known to be breakable using quantum computers).

3.4 Gold Code Encryption Algorithm

Gold Codes [13] 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.

Proposed Algorithm:

1. Start
2. Initialize the network
3. Form clusters by Fuzzy C- means clustering
4. If energy level is below than specified threshold then elect cluster head
5. Now find the shortest path through Dijkstra algorithm
6. Apply Gold code algorithm to generate binary bit sequence
7. Performs XOR operation
8. If sum is odd then output function is 1 otherwise 0.
9. Generate gold code of m-sequence.
10. Now, Select NTRUEncrypt algorithm for secure data transmission
11. Aggregated encrypted data towards Base station.1
12. Stop.

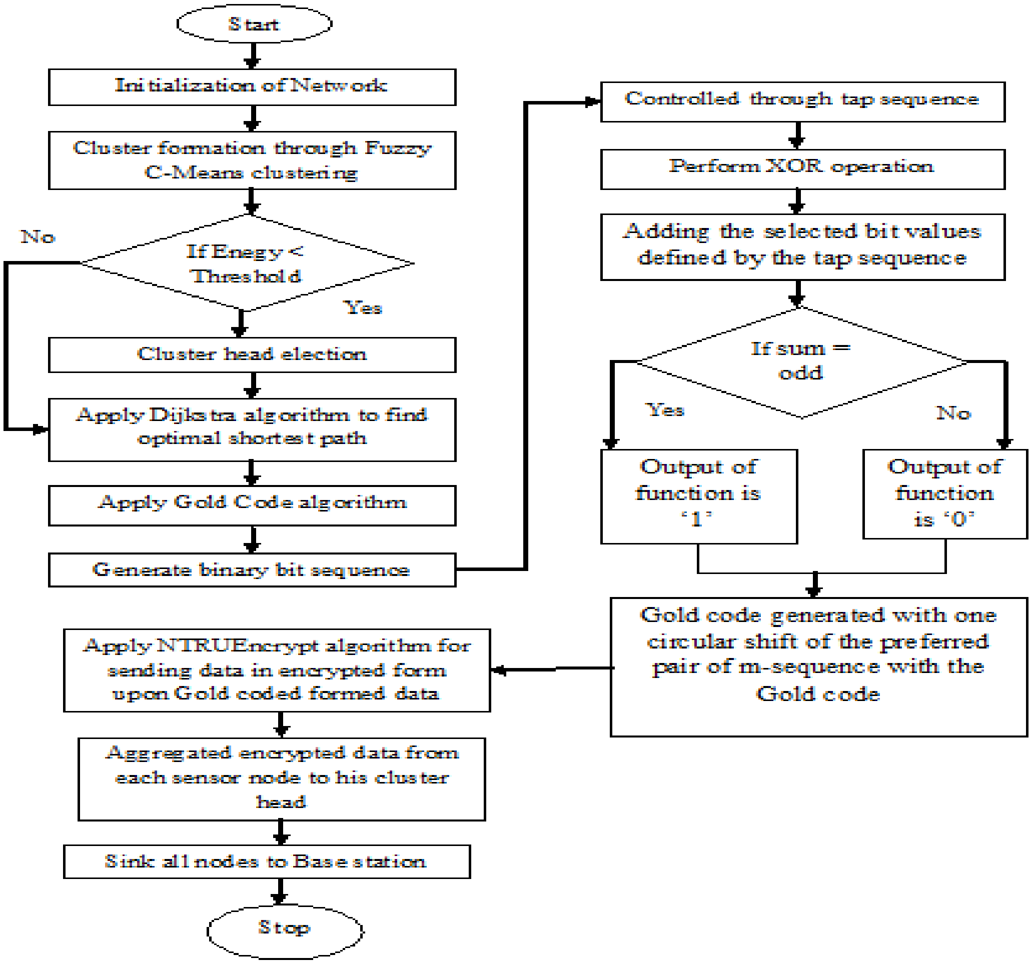
Start
Initialization of Network
Cluster formation through Fuzzy C-Means clustering
No
If Enegy < Threshold
Yes
Cluster head election
Apply Dijkstra algorithm to find optimal shortest path
Apply Gold Code algorithm
Generate binary bit sequence
Controlled through tap sequence
Perform XOR operation
Adding the selected bit values defined by the tap sequence
If sum = odd
Yes
No
Output of function is '1'
Output of function is '0'
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 from each sensor node to his cluster head
Sink all nodes to Base station
Stop

Fig. 3.1 Flowchart of Proposed Work

4. RESULT ANALYSIS

In the result analysis, the experiment of proposed work performed by using MATLAB tool. This firstly loaded dataset. Using Fuzzy C-Means Clustering algorithm to find optimal path and NTRU Gold Code method for secure data transmission.

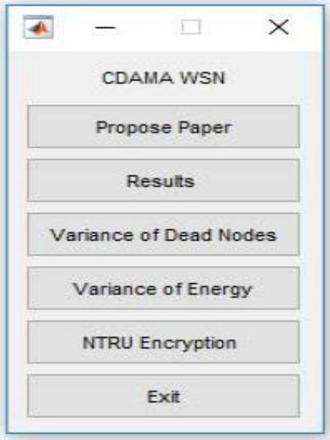

Figure 4.1: Main menu of CDAMA approach for proposed

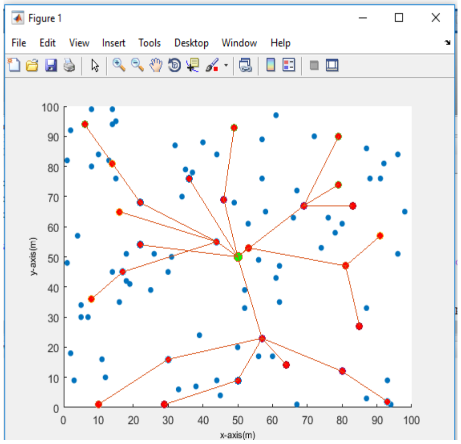

Figure 4.2: Cluster Formation towards Sink node using Fuzzy C-Mean clustering

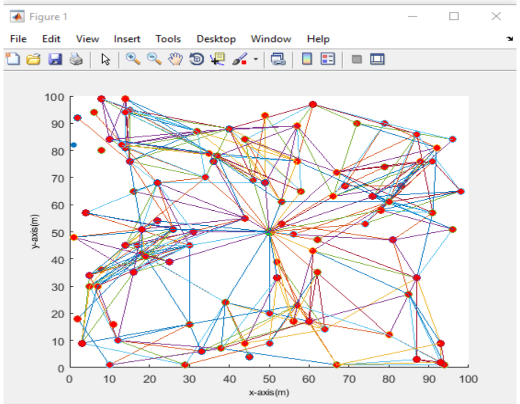

Figure 4.3: Apply Dijkstra Algorithm to optimal path

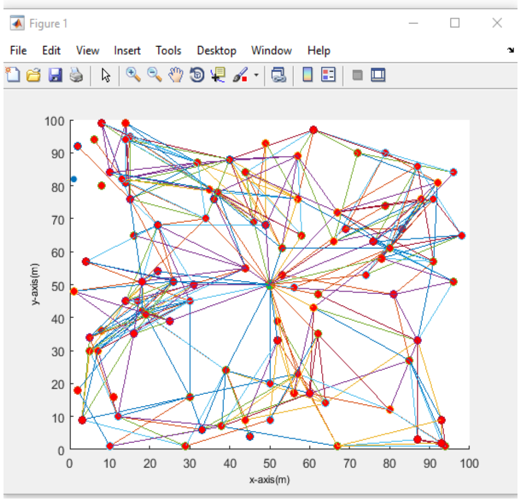

Figure 4.4: Apply Dijkstra Algorithm to optimal path

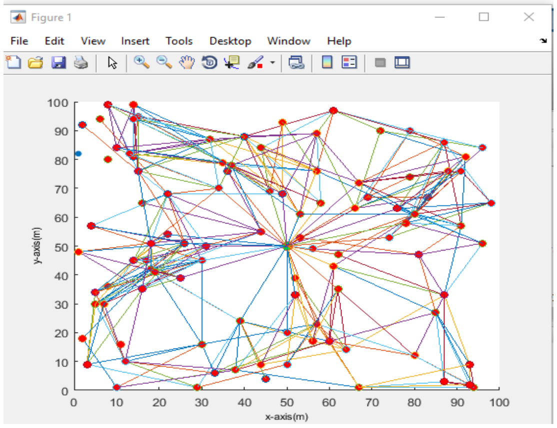

Figure 4.5: Cluster head election during dead nodes

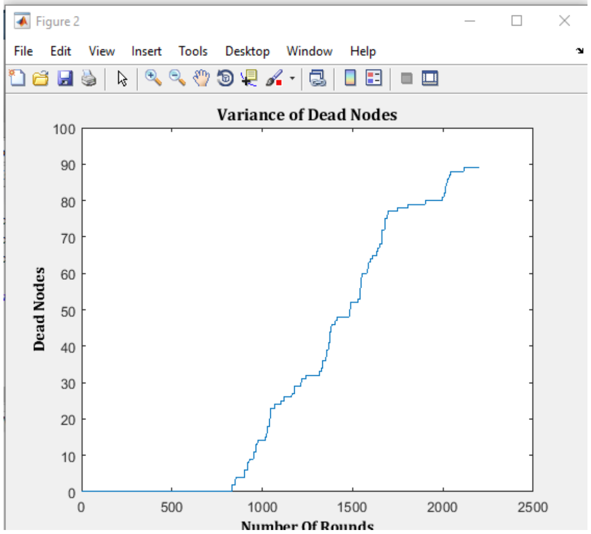

Figure 4.6: Variance of Dead Nodes

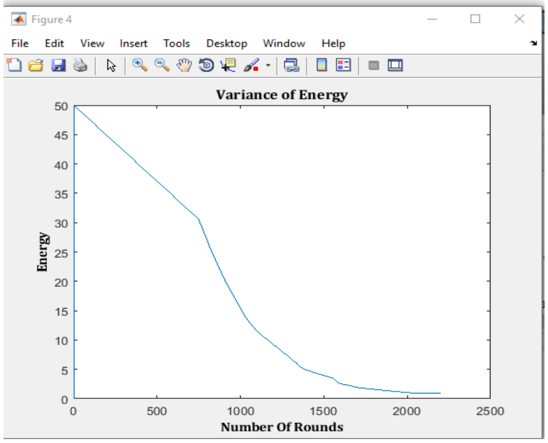

Figure 4.7: Variance of Energy

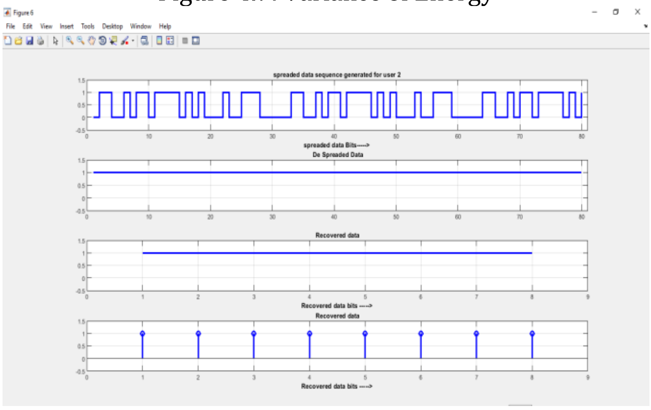

Figure 4.8: Transmitted and Received Messages through NTRU encryption and Gold Code encryption mechanism

5. CONCLUSION

Wireless Sensor Networks consists of thousands of sensing nodes, also known as motes, which are powered by battery to communicate with one another. They are deployed at remote location for continuously checking the environment to collect data. WSNs are used in many areas, i.e. surveillance, forest fire monitoring, healthcare and industrial automation. These nodes sense the environment for data and send to a sink node, also known as base station. In these networks, optimal paths need to be determined for efficient flow of data. Power optimization based on optimal path selection is a major concern/ issues in WSNs. Also, security remains the big issue in the existing approach. So, resolve these problem, we have made a secure model that enhance the security level for sending data.

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] M. Mirzaie, S.M. Mazinani, – Adaptive MCFL: An adaptive multi- clustering algorithm using fuzzy logic in wireless sensor network‖, Computer Communications 111 (2017) 56–67.

[4] 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).

[5] 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).

[6] 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 .

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

[8] 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.

[9] 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).

[10] R.Suganya and R.Shanthi, ―Fuzzy C- Means Algorithm- A Review‖, International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012, pp. 1-3.

[11] 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.

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

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