International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print)
Volume No.5, Issue No.7, pp : 618-621 1 July 2016

Securely Data-Gathering Cluster-Based Wireless Sensor Network Design

Ms. Sandhya Bankar , Prof. Simran Khiani
Dept. of Computer Engineering
G.H. Raisoni College of Engineering and Management SavitribaiPhule Pune University, Pune, India
Email: bankarsandhya512@gmail.com , simran.khiani@raisoni.net

Abstract: Wireless sensor network are collection of sensor for sensed data and sending to appropriate station,where data analysis is performed.The energy aware clustering is consider energy parameter but instead of that considering only energy parameter, proposing efficient clustering algorithm which provide cluster head.The effective lossless data aggregation with route formation is plus in algorithm. By introducing security algorithm which provide security as well as authentication of each node.The comparing of the systems with time and energy parameters to show the proficiency of system.
Keywords—Wireless Network, Clustering, Routing, NTRU Crypto System.

I. INTRODUCTION

Wireless sensor networks have been utilized as a part of different fields such as schools, universities, battle fields, surveillance and so forth. It has been utilized as a part of everybody's day by day life. Its necessities are expanding step by step. WSN has come in existence as a solution for some issues where human intervention to be troublesome. The quick advances in wireless organizing, implanted chip, incorporated micro-electro-mechanical systems (MEMS), and nanotechnology have empowered the advancement of low-cost, low-control, and, multifunctional sensors. Sensors are little in size and are able to do detecting, information handling, communicating with one another or with the information sinks. Sensor nodes are connected with each other through wireless medium such as infrared or radio waves it depends on applications. Internal memory is associated with each sensor node to store the information of its related event packets. A group of sensors communicating in a wireless medium form a wireless sensor network for the purpose of gathering data and transmitting it to a user (sinks). The main purpose of the WSN is to monitor and collect data by the sensors and then transmit this data to the sinks. Clustering is a key technique used to extend the lifetime of a sensor network by reducing energy consumption. Scalability of network increases with the help of clustering techniques.

The network operations of general framework of WSN is my area interest can be outlined as follows. Initially, a set of sensors, which are equipped with limited energy resource (e.g., battery) as well as sensing, processing, and communication capabilities, is deployed in a geographical region. Data collected by the sensors are forwarded to specially designated sensors, called cluster heads (CHs), which conduct some processing to aggregate their received data. CHs then forward the data to specific locations, called sinks, either directly or through other CHs.

In numerous applications of WSNs system lifetime is one of the principle concerns in system outline and operation. Sensor redeployments may be required because of a few reasons, e.g., having short of what a basic number of operational sensors with enough remaining energy in the system [4].

Therefore, the system lifetime is characterized as the quantity of periods that can be attained to with an arrangement. Topology control and routing are two principal issues in powerful outline and operation of WSNs. The nearby relationship between these choices and their connection to system lifetime are particularly underlined by the WSN particular configuration incorporate energy proficiency and computation-communication exchange off. Energy productivity is a significant concern following every sensor has limited and non-renewable energy asset. Correspondence processing exchange off alludes to the way that correspondence expends more energy than performing processing ready for. This is discriminating as it identifies with the energy effectiveness. In spite of the fact that the immediate correspondence of a sensor with a sink is suitable for the entire system, this is basically unthinkable or may require extreme energy might the system lifetime get decreased. In this way, routing plans where the data size is diminished by in-system data collection where energy is utilized for processing instead of correspondence along the ways from sensors to a sink (client) are typically favored.

In this paper further we will see: Section II talks about related work studied till now on topic. Section III current implementation details, introductory definitions and documentations and in addition formally expresses the IWI and MIWI mining undertakings tended to by this paper. Section IV show conclusions and presents a future work.

II. RELATED WORK

This project discusses the works that are more closely related to this research in the context of network topology and data routing.

In paper [1], H. Uster and H. Linestablished and implemented three mathematical models for the purpose of increasing the network lifetime. In the first two models, the degradation of total energy usage in the network and the degradation of the maximum energy usage at a sensor node might occurs some problem of quick energy drainage. In the third proposed model, minimizethe weighted sum of the total energy consumption and the range of remaining energy distribution in the network improve efficiency of energy and

ISSN:2319-6890)(online),2347-5013(print)
1 July 2016

increase network lifetime.Authors do not ensure proper solution method to improve quality of their heuristic algorithm.

SudarshanVasudevan, Micah Adler, Dennis Goeckel (Vasudevan et al., 2013) [2], presents gainful neighbordisclosure algorithms for remotesensor networks. The neighbor revolution calculations don't oblige examinations of node thickness and permit alternative operation. Moreover, algorithms grantnodes to start operation at various times, authenticated nodes are used to distinguish the end of the neighbor detection stage.Explicitly compelling is the topic of whether the criticism based designs, which are demand ideal in the single-bounce case, can be connected with the multi-bounce framework setting while beating the ALOHA like algorithm.

In this paper [3], author implements UHEED, an unequal clustering algorithm which alleviates this issue and which indicates to a more uniform remaining energy in the network and increases the network lifetime.

In this paper [4] author represents a hierarchical network structure with multiple sinks at which the data collected by the sensors are gathered through the cluster heads are adopted. A Mixed Integer Linear Programming (MILP) model to optimally determine the sink and CH locations as well as the data flow in the network is considered. Data gatheringinwireless sensor networks (WSNs) are worked unattended in several applications.

In this paper [5],author distinguishes between neighbor discovery during sensor network initialization and continuous neighbor discovery. They efforts on the latter and view it as a joint task of all the nodes in every connected segment.

Al-Turjman et al. [6], propose a mixed integer linear program (MILP) with the destination of reducing the aggregate network energyconsumptionwhereascontainingnecessities on defect resilience at the same time. In that study, sensors are estimated to forward their data to the sink through particular hand-off nodes that are equipped with higher strength sources.

This paper [7], ensures the availability of a bidirectional route between each sensor node and a base station, which offers both broadcast from a base station and data collection to the base stations.Obviously, the amount of relay nodes needed to ensure this weaker integration won't surpass the amount of relay nodes needed to ensure the more grounded network planed in this paper.

In this paper [8] author make an effort issue by deploying Relay Nodes (RNs) aimed for restoring connectivity. Although finding the minimum relay count and positions is NP-Hard, efficient heuristic methodologies have been expected. The infinite 3-Dimensional (3-D) seek space which specifically corrupts network performance in practice.

Liu et al. [9] recommend a distributed energy-efficient protocol EAP for the general situation. In EAP, every CH is probabilistically chosen concentrated around its amount of the remaining energy to the normal residual energy of all the nearby sensors inside its cluster range. For advance change in network lifetime, EAP presents the thought of ``intracluster scope" that permits a halfway set of sensors.

Table 1

Title	Method Used	Advantages	Disadvantages
Data agregation and routing in wireless sensor networks: Optimal and heuristic algorithms [3].	present solutions for the data gathering and routing problem with in-network aggregation in WSNs.	It improves system lifetime with acceptable levels of latency in data aggregation and without sacrificing data quality	Lack of Security.
An energy-aware routing protocol in wireless sensor networks [9].	Introduces a simple but efficient approach, namely, intracluster coverage to cope with the area coverage problem.	It has far better performance than HEED when node density goes higher than 0.01nodes/m2 .	Need to improve the network lifetime.
Integrated topology control and routing in wireless sensor network design for prolonged network lifetime [4].	A hierarchical network structure with multiple sinks at which the data collected by the sensors are gathered through the cluster heads are adopted.	This model effectively utilizes both the position and the energy-level aspects of the sensors while selecting the CHs and avoids the highest-energy sensors.	Need to improve the security.
Energy efficient communication protocol for wireless micro-sensor networks [11].	Propose LEACH (Low-Energy Adaptive Clustering Hierarchy), a clustering-based protocol that utilizes randomized rotation of local cluster base stations (cluster-heads) to evenly distribute the energy load among sensor	To distribute energy dissipation evenly throughout the sensors, doubling the useful system lifetime for the networks we simulated.	Communication cost is more.

III. IMPLEMENTATION DETAILS

In this section discussed about the proposed system in detail. In this section discuss the system overview in detail, proposed algorithm, mathematical model of the proposed system,

A. System Overview

The following figure 1 shows the architectural view of the proposed system.

ISSN:2319-6890)(online),2347-5013(print)
1 July 2016

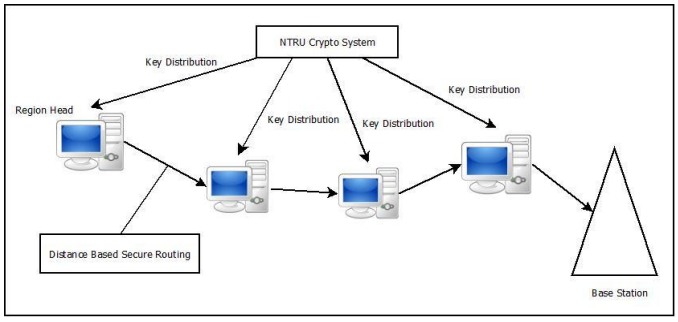

Figure 1: System Architecture

- *Clustering Process:*The process of clustering is performed in which nodes are divided into group of clusters. Number of clusters is generated in the network.
- *Cluster Head Selection:*After generating the group of clusters, cluster head is selected from each group of clusters. Cluster head selection is done on the basis of energy and distance parameters. Each node has assigned initial energy at the time of network deployment.
  1. Cluster head should be in same cluster
  2. Cluster head should have maximum energy
  3. It should minimum distance from base station
  4. It should have maximum number of neighbor
  5. It should aggregate all data from cluster member without data loss.
- *Key generation and distribution:*Base station generates the key and distributes the keys toeach node.
- *Data Encryption:*Data is generated at each node. After generating the data, data is encrypted at each node by using the NTRU algorithm.
- *Data aggregation:*The process of data aggregation is done by the cluster head. And send data to the base station.
- *Route Generations:*The routes are generated from each cluster head to the base station.In this distance based technique to generate the path. Each node calculates the optimal path to the destination.
- *Data Decryption*Base station receives the data from each cluster head and decrypts the data by the appropriate key.

B. ***Algorithm***

In this section discuss the algorithm of the proposed system and algorithm for addition of graphical element into slide.

Algorithm 1:NTRU Crypto System

In the above NTRU(Nth Degree Truncated Polynomial Ring Units) algorithm describes the steps of the proposed system. In which initially network is generated with sensor nodes, after that performing the process of clustering in which number of nodes is divided into number of clusters, cluster head is selected on the basis of three parameters, key distribution is performed at each node through base station, route is generated from Cluster Head to the base station. Encrypt the data by using the NTRU algorithm with the private key. Cluster member send the data to the cluster head in all clusters. The data is aggregated at the cluster head using appending technique. Send the data to the base station. Base station decrypts the data with the appropriate keys. By proposing this we are improving time as well as energy efficiency and providing secure network.

B. ***Steps of NTRU:***

1. Key Generation
   K= {PK, CK}Where, K is a set of keys,
   PK= Private KeySK= Secret Key
   The Pair (sk, pk) is generated by sampling value $\acute{f}$ from distance Gaussian distribution$D_{Z^n,\sigma}$.
   To generate the key pair two polynomials f and g, with degree at most \ N-1 and with coefficients in {-1,0,1} are required.
   P is a positive integer specifying a ring Z=pZ
   Compute secret key f by:
   $f = p.\acute{f} + 1$ …….. (1)
   Compute public key h by:

$h = \frac{pg}{f} \in R_q^{\times}$ ……. (2)

2. Encryption of data M.
   M= {m1, m2, …,mn}
   Where, M is the encrypted data.
   two random values s, e ← Υα and computes ciphertext as
   $C = hs + pe + M \in Rq$……(3)
   where h is the public key
3. Decryption of data by Base Station.
   C is decrypted by using secret key f as:

$$\acute{C} = f.C \in Rq \text{…….. (4)}$$

$$M = \acute{C} \bmod p \text{ ……(5)}$$

C. ***Mathematical Model***

System S is represented as S= {N, B, C, CH, K, F, LD, DR}
1. Deploy nodes
N= {N1, N2, ... ,Nn }
N is set of all machines which are considered as deployed nodes.
2. Create Base Station
B= {B1, B2, ……,Bn}
Where, B is a set of all base stations.
3. Create clusters
C= {C1, C2, ...,Cn}
4. Select the Cluster Heads in Each Cluster
CH = {CH1, CH2,....,CHn}
Where, CH is a set of all cluster heads.
To estimate energy dissipation in transmitting x_{pq} (bits) of data from node p to q, the path loss model $vD_{pq}^{a}\ x_{pq}$ where $v\ (J/bit/m^a)$ is constant and D_{pq} is the distance between p and q, and $2 \leq a \leq 4$.
5. Generate the the keys for authentication
K = {K1, K2,....,Kn}
Where, K is a set of all Keys.
6. Send the data from cluster members to cluster Head and from here to base station
F= {f1, f2, f3, ...fn}
Where, F is a set of all data files transmitted.

D. *Experimental Setup*

The system is built using Java framework (version jdk 8) on Windows platform. The Netbeans (version 8.1) is used as a development tool. The system doesn't require any specific

ISSN:2319-6890)(online),2347-5013(print)
1 July 2016

hardware to run, any standard machine is capable of running the application.

IV. RESULT AND DISCUSSION

A. *Results*

In Figure 2 shows the comparison graph for package drop ratio of existing and proposed system.
Packet drop=number of packet send - number of packet received

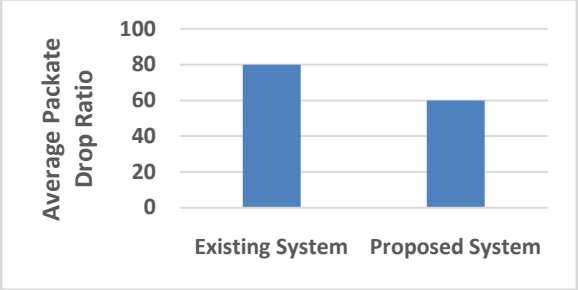

Figure 2: Average packet drop ratio graph comparison

Figure 3 shows the comparison graph for energy consumption ratio of existing and proposed system.

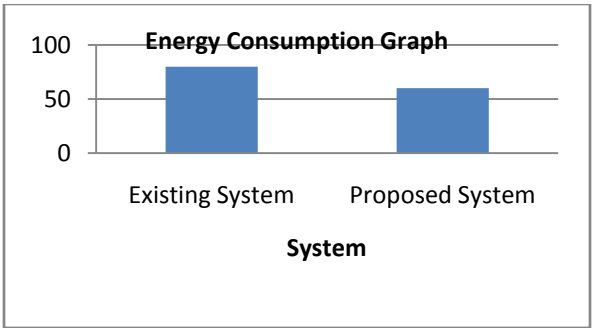

Figure3: Energy Consumption Graph Comparison

Figure 4 shows the comparison graph for Network Lifetime graph of existing and proposed system.

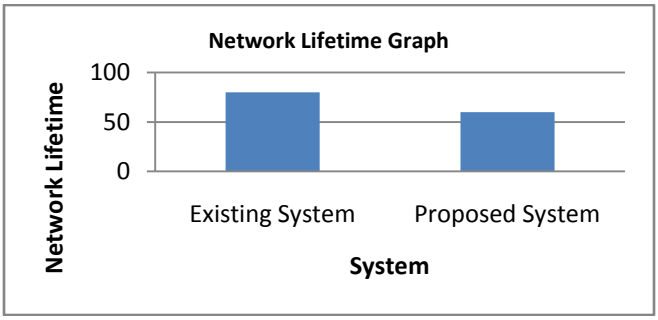

Figure 4: Network Lifetime Graph Comparison

V. CONCLUSION AND FUTURE SCOPE

In this introduced system which increases the network lifetime of network in the wireless network system. This system proposed the method by which cluster head is selected on the basis of three parameters, from which the network consumes its energy and increase the network lifetime of the wireless sensor network. System also introduced the method for Secure Data Sending. Finally generate the results which conclude that the proposed system is increase the network lifetime and is more Secure. In future we can work on relocation of sink node.

ACKNOWLEDGMENT

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We are thankful to the authorities of SavitribaiPhule University of Pune and concern members of cPGCON2016 conference, organized by PCCOE, Pune, for their constant guidelines and support. We are also thankful to the reviewer for their valuable suggestions. We also thank the college authorities for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and familymembers.

REFERENCES

i. *Jiao Zhang,FengyuanRen Shan GaoHongkun Yang and Chuang Lin "Dynamic Routing For Data Integrity and Delay Differentiated Services in Wireless Sensor Network "IEEE International Conference on Mobile Computing,vol14,NO.2,Feb 2015*

ii. *AnkitThakkar,KrtanKotecha "Cluster Head Election for Energy and Delay Constraint Application of Wireless Sensor Network",IEEE,2013.*

iii. *H. Lin and H. Uster, "Exact and Heuristic Algorithm for Data-Gathering Cluster- Based Wireless Sensor Network Design Problem",IEEE International Conference on sensor Journal, vol. 22, no.3, June 2014.*

iv. *Kyung-Ah Shim,"A Secure Data Aggregation Scheme Based On Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Network" IEEE International Conference On Parallel and Distributed system,Aug 2015,Vol26,NO.8.*

v. *S. Vasudevan, M. Adler, D. Goeckel, and D. Towsley, "Efficient algorithms for neighbour discovery in wireless networks," IEEE Feb. 2013,vol. 21, no. 1, pp. 69-83.*

vi. *H. A˜ ster and H. Lin, "Integrated topology control and routing in wireless sensor network design for prolonged network lifetime," IEEE 2011, Ad Hoc Newt., vol. 9, no. 5, pp. 835-851.*

vii. *R. Cohen and B. Kapchits, "Continuous neighbor discovery in asynchronous sensor networks," IEEE Feb.2011 vol. 19, no. 1, pp. 69-79.*

viii. *S. Misra, S. D. Hong, G. Xue, and J. Tang, "Constrained relay node placement in wireless sensor networks: Formulation and approximations," IEEE International Conference On Sensor Network,Apr.2010, vol. 18, no. 2, pp. 434-447.*

ix. *F. Al-Turjman, H. Hassanein, and M. Ibnkahla, "Connectivity optimization for wireless sensor networks applied to forest monitoring", in Proc. IEEE International Conference On wireless Sensor Network, Jun. 2009, pp. 1-6.*

x. *M. Liu, J. Cao, G. Chen, and X.Wang, "An energy-aware routing protocol in wireless sensor networks,"IEEE International Conference On Sensors, 2009,vol. 9, no. 1, pp. 445-462.*

xi. *J. N. Al-Karaki, R. Ul-Mustafa, and A. E. Kamal, "Data agregation and routing in wireless sensor networks: Optimal and heuristic algorithms, ComputerNetw" IEEE International Conference On Networking,2009, vol. 53, no. 7, pp. 945-960.*