DOI 10.29042/2018-3759-3763

Helix Vol. 8(5): 3759- 3763

Design of Wireless Sensor Network Based on Cluster for Securely Data Gathering

[1]Ms. Sandhya Bankar, [2]Prof. Simran Khiani, [3]Dr. C.G.Dethe

[1,2]Department of Computer Engineering, G.H.R.C.E.M, Wagholi, Pune

[3]Director ASC, Nagpur

Email: bankarsandhya512@gmail.com, simran.khiani@raisoni.net

Received: 09th July 2018, Accepted: 14th August 2018, Published: 31st August 2018

Abstract

The wireless sensor network organizes the collection of the sensor for detected information and sending to the suitable station, where information examination is performed. The clustering is not only considering energy parameter but also proposing other parameters like distance, no of neighboring nodes. And depending on the parameters cluster head has calculated. Security is most common issue in wireless sensor network. By introducing an NTRU crypto Security Algorithm, as well as clustering techniques, are improving the lifetime of the wireless sensor network. By using NTRU algorithm does not prone to attack and most secure algorithm for encryption and decryption process.

Keywords: Wireless Network, Clustering, Routing, NTRU Crypto System.

Introduction

A wireless sensor organize has been utilized as a part of a few regions of work like schools, universities, battlefields, surveillance and so on. The need of WSN is expanding each day. It turned into a response to the issues in which human intercession can make some inconvenience. The brisk advances in wireless organizing implanted chip, incorporated micro-electro-mechanical systems (MEMS) and in addition, nanotechnology has boosted the headway of minimal effort, low-cost, low-control, and furthermore multifunctional sensors. Sensors are a little size and can recognize, handling of data, communicating with one another or with the data sink. Sensors nodes are connected to each node by means of wireless innovation like infrared or radio waves on the basis of an application. Sensor nodes or internal memory of associated event packets for storing data. Collections of sensors communication all wireless medium form WSN for the reason of collecting information as well as forwarding it to the client or sinks. Clustering technique is utilized for improving the lifetime of a sensor network by minimizing energy utilization. Network scalability ascends with the assistance of clustering methods. This is the reason; the life of framework is portrayed as the measure of periods that can be accomplished with an arrangement. The primary issue in outline and also in operation of WSNs are routing and topology control. The main problems in outline as well as in operation of WSNs are topology control as well as routing. The adjacent connection between these choices and their relationship with system lifetime are particularly underlined configuration incorporate energy proficiency and computation-communication exchange off. Energy productivity is a huge concern taking after each sensor has limited and non-renewable energy resource. Correspondence preparing trade-off suggests the way that correspondence uses more energy than performing handling prepared for. This is discriminating as it relates to the energy efficiency. Notwithstanding the way that the prompt correspondence of a sensor with a sink is reasonable for the whole framework, this is fundamentally inconceivable or may require great energy may the framework lifetime get reduced. Thusly, routing plans where the information size is reduced by in-system information gathering where energy is used for processing rather than correspondence along the routes from sensors to a sink (client) are normally supported.

Related Work

This section talks about the works that are all the more firmly identified with this examination with regards to network topology and information routing.

In paper [1], H. Uster and H. Lin designed and developed 3 mathematical models with the goal to give one more method to be developed in every round of a deployment for the reason of maximizing network life. Authors are not sure of exact solution technique which is utilized for minimizing the solution quality of proposed heuristic algorithm.

In paper [2], authors have given gainful neighbor disclosure algorithms for remote sensor networks which solve distinctive common sense limitations of the present techniques. Observations exhibits a gap

between the lower and upper bounds on the running time for neighbor disclosure.

In this paper [3], authors have developed UHEED, an unequal clustering algorithm this alleviates this problem and that shows to a more uniform remaining energy in the network as well as maximizes network lifetime.

In paper [4] author given a hierarchical network structures having multiple sinks which collects information by the sensors are collected by the cluster heads are adopted. A Mixed Integer Linear Programming (MILP) model to optimally determine the sink as well as CH locations also the flow of information in the network is taken in account. Information collection inside wireless sensor networks (WSNs) is the work which is not attended over long time horizons to gather data in different applications. Typically, sensors have limited energy as well as are subject to the elements in the terrain.

In paper [5], author given the difference in neighbor discovery while sensor network initialization and continuous neighbor discovery. They efforts on the after as well as view it as a combined work of every nodes in each linked segment. Every sensor works on a simple protocol in a synchronize effort to minimize power utilization without raising the needed time to find hidden sensors.

In paper [6], authors have given a mixed integer linear program (MILP) with the destination of minimizing the collective network energy utilization wherein having necessities on defect resilience at the same time. In that study, sensors are predicted to send the information to the sink via specific hand-off nodes which is having higher strength sources.

This paper [7] makes sure the availability of a bidirectional route in every sensor node as well as a base station that gives both broadcasts from a base station as well as information gathered to the base stations. The observation of obliged relay nodes conditions with this weaker connection need might be a heading of future extension.

In paper [8], authors have given a distributed energy-efficient protocol EAP for the common cases. In EAP, each CH is probabilistically selected on its level of the available energy to the normal residual energy of all the nearby sensors in its cluster range. This is as different to HEED that just selects CHs concentrated on sensors own specific available energy. For advance modification in network lifetime, EAP gives the idea of "intra-cluster scope which allows a halfway set of sensors to be dynamic in clusters while having up a normal scope.

In paper [9] author have given a Lattice based cryptography is attractive for its quantum computing resistance and efficient encryption/decryption process. However, the big data problem has perplexed lattice based cryptographic systems with the slow processing speed. This paper intends to analyze one of the major lattice-based cryptographic systems, Nth-degree truncated polynomial ring (NTRU).

Implementation Details

In this section we will go through proposed system in detail. In this section discuss the system overview in detail, proposed algorithm, and mathematical model of the proposed system.

System Overview

The following figure 1 shows the architectural view of the proposed system. The description of the system is as follows:

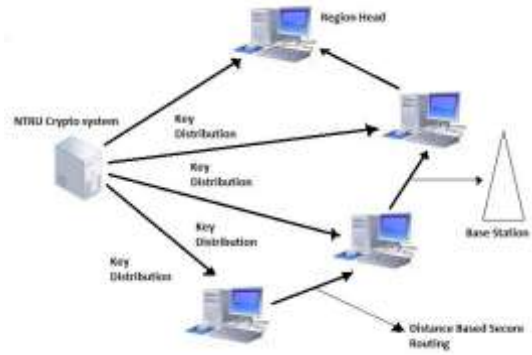

Fig.1: System Architecture

Clustering Process

The clustering process is done in those nodes which are scattered into the group of clusters. Number of clusters is generated in the network.

Cluster Head Selection

After establishment of clusters, cluster head is picked from each group of clusters. Cluster head selection is accomplished depending on energy and distance parameters. Every node has given initial energy at the time of network formation. When node is sensing as well as forwarding the data, energy is gets utilized based on the size of information also on distance to the destination. As cluster head comes in common communication it is must have huge energy compared with all other nodes and its distance to the base station must be optimal.

For cluster Head Selection:

- Cluster head should be present in the same cluster group.
- Cluster head must have exactly the highest energy
- It should have less distance between base station and cluster head.
- It should have more number of neighbor nodes

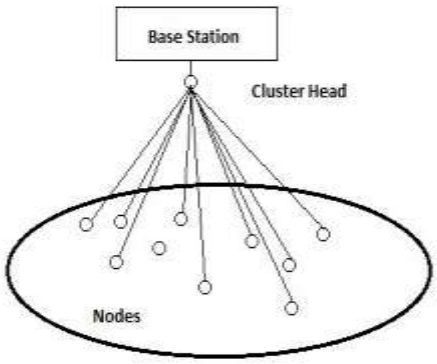

Fig 2. Cluster Head Model in WSN

Cluster head selection is done on the basis of parameters like distance, energy.
Calculation of distance between two points, as shown in the below formula,

$$dist\big(t(x,y),(a,b)\big) = \sqrt{(x-a)^2 + (y-b)^2}$$

If points (x,y) and (a,b) are in 2-dimensional space, then the Euclidean distance between them calculated.
Calculate the consumed energy, available of energy of sensors using below equation:

$$consumed\ energy = len * 50 + 0.1$$

len = Distance between CH to BS
Remaining Energy =
(Available Energy - Consumed Energy)

1. The procedure of Cluster formation is given below: Initially Base Station requests for ID of every node, node energy level as well position from each node that's called client. Search the distance of each cluster nodes from Base Station using Euclidean distance formula

2. Base station will chooses k nodes as cluster head which will have maximum energy and very closer to the node.

3. The whole cluster node passes the information to cluster head node which will finally forwards the data of entire sensor network to Base Station

The way of data communication will formed from cluster head to base station.

Key Creation and Distribution:
Base station creates the key and assigns the keys to every node.

Data Encryption:
Data is gathered at each node. Once collection of data I finished, data is encrypted at every node by making use of the NTRU algorithm.

Data Aggregation:
The process of data aggregation is done by the cluster head and forward data to the base station.

Route Generations:
The routes are created to the base station from every cluster head. In this way using distance based methods to create the path. Every node computes the optimal path to the destination by computing number of hops in between and choosing the minimal hop path.

Data Decryption
Base station receives the information from every cluster head as well as decrypts the information by the proper key.

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

Algorithm: NTRU Crypto System
In the above given NTRU (Nth Degree Truncated Polynomial Ring Units) algorithm explains the steps of the proposed system. In that basic network is created with sensor nodes, after that performing the process of clustering in which number of nodes is divided into number of clusters, cluster head is chosen depending on three parameters, key distribution is done at every node via base station, route is created from Cluster Head to the base station. Encrypt the information by making use of the NTRU algorithm with the private key. Cluster member transmit the information to the cluster head in all clusters. The information is collected at the cluster head utilizing appending method. Forward the information to the base station. Base station decrypts the information with the specific keys. By proposing this we are maximizing time and energy efficiency also providing secure network. The RSA provides the highest security to the business application and If an

application is required with the highest decryption priority DES is more suitable but In An asymmetric key cryptographic system provides high security in all ways. Encryption, decryption and complexity are high in NTRU.

Advantage of NTRU

1) Doesn't prone to attack
2) Most secured type of algorithm
3) Secured in Encryption and decryption process

NTRU Algorithm

Key Creation K= {PK, SK}
Where, K is a set of keys,
PK= Private Key, SK= Secret Key
The Pair (sk, pk) is created by sampling value f' from Distance Gaussian distribution$Dz^n\sigma$
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.f + 1

Compute public key h by:

$$h = \frac{pg}{f} \in Rq$$

Encryption of data M. M= {m1, m2,,mn}
Where, M is the encrypted data.
Two random values s, «and computes cipher text as
C = hs + pe + M
Where, h is the public key

Proposed System Algorithm

NTRU Algorithm:

1) Generate the network with number of nodes.
2) Divide the network in to number of clusters.
3) Analyze each nodes energy, distance from base station, number of nodes in transmission range.
4) Based on above parameters select the cluster head.
5) Select the appropriate cluster head for each cluster
6) Generate and distribute the key pairs at each node using NTRU algorithm.
7) Distribute The Valid Key Pairs generated by NTRU to The intended nodes securely.
8) Generate The Data At Each Cluster Member.
9) Encrypt the sensed data at each node
10)Send the data to the cluster head.
11)Aggregate the data at the cluster head using appending technique.
12)Form the routes from each cluster head to the base station.
13)Send the data from cluster head to Base station.
14)Decrypt the data at the base station with valid keys.

NTRU Disadvantages

With NTRU, there's a tradeoff to be made in terms of the parameter q. The larger q is, the larger keys and ciphertexts are; the smaller it is, the greater the chance that a valid ciphertext will fail to decrypt. An attacker learns information from these decryption failures, so it's important to stop this happening. For sufficiently large q, there will be no decryption failures at all, and in fact some sets of NTRU parameters have had this property.

Mathematical Model

System S is represented asS= {Input, Process, Output}

Input:

Sensing Information
I = {I1, I2,…..,In}
I is a set of input represent sensing information. Process:

Process:

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.
   One important parameter in performance of WSN energy consumption.
5. Generate 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.

Output: Data routing to base station.

Results and Discussion

In this section we will discuss and conclude the results of proposed system. In Fig. 3 shows the comparison graph for package delivery ratio of existing and proposed system. In the existing system package delivery ratio is more as compare to the package delivery ratio in the proposed system because by selecting the optimal paths that can effectively send

the data. Also packet drop ration can calculate, Packet drop=number of packet send - number of packet received.

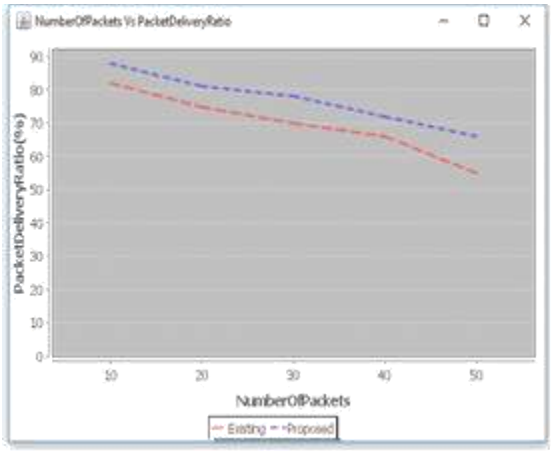

Fig. 3: Average Packet Delivery Ratio Graph Comparison

Fig. 4 shows the comparison graph for Network Lifetime graph of existing and proposed system. The selecting the optimal paths and selecting the high energy cluster heads leads to better network lifetime in the proposed system.

Remaining Energy = Energy Available – Energy Consumed

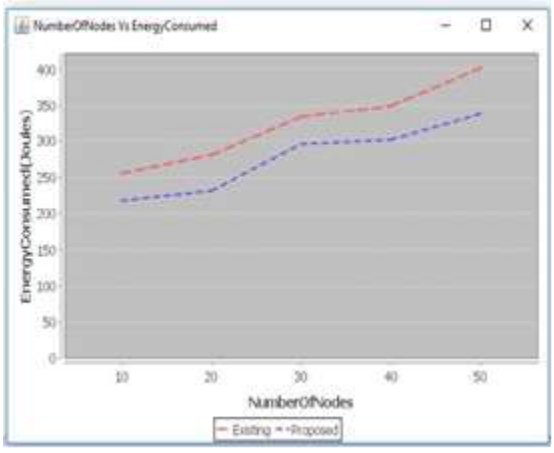

Fig. 4 Network Lifetime Graph Comparison

Conclusion and Future Scope

In this paper introduce the system that maximizes the network lifetime in the wireless network system. This system gives the technique using this cluster head is chooses to depend on three parameters, the network uses its energy, distance, neighboring nodes and authenticate the cluster head. This process will maximize the network lifetime of the wireless sensor network. The system also implemented for Secure Data Forwarding. By introducing NTRU crypto security algorithm, the data encryption and decryption are done securely. NTRU is one of the best security algorithms. It does not prone to attack. At last, creates the outcome that shows that the proposed system maximizes the network lifetime of the system as well as is more secure. In future, we can work on the relocation of sink node.

References

[1] Jiao Zhang,Fengyuan Ren Shan Gao Hongkun 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

[2] 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.

[3] Ankit Thakkar, Krtan Kotecha Cluster Head Election for Energy and Delay Constraint Application of Wireless Sensor Network,IEEE,2013.

[4] 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.

[5] 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.

[6] 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.

[7] H. A Uster 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.

[8] 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.

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

[10] Tianyu Bai, Spencer Davis, Juanjuan Li and Hai Jiang: Analysis and Acceleration of NTRU Lattice-Based Cryptographic System, Computer Netw. International conference 2017.

