Secure Strategy for High Speed Transmission & Efficient Collection of Data in WSN Research

Kamal Kr. Gola[1], Bhumika Gupta[2], Zubair Iqbal[3]

Abstract— Wireless Sensor Networks (WSNs) consist of small nodes with sensing, computation and wireless communications capabilities. Wireless sensor networks utilize large numbers of wireless sensor nodes to collect information from their sensing terrain. Once they are deployed, it becomes impossible to replace or recharge its battery. So the battery power of the sensor node is very important. As we know that Energy efficient routing is one of the key issues in wireless sensor network because all the nodes are battery powered, so failure of one node affects the entire network that's why Energy saving is always crucial to the lifetime of a wireless sensor network. Many routing protocols have been proposed to maximize the network lifetime and decrease the energy consumption. But these algorithms do not provide any security at that time when the data has to be sent to the node as well as to the base station and also do not define how to collect high speed data in efficient way. We proposed an algorithm to provide these two services. The main purpose of the proposed algorithm is to reducing the time in the collection process of data in the wireless sensor networks and also provide the security at the time of transmission(among the node and node to base station) using.

Index Terms— WSN, energy efficient, cluster head, data aggregation, shortest path algorithm, Base station, Security Algorithm, QOS Parameters, RDM, Re-Clustering.

1 INTRODUCTION

Wireless sensor network (WSN) is widely considered as one of the most important technologies for the twenty-first century.[1] In the past decades, it has received tremendous attention from both academia and industry all over the world. A WSN typically consists of a large number of low-cost, low-power, and multifunctional wireless sensor nodes, with sensing, wireless communications and computation capabilities.[2][3] These sensor nodes communicate over short distance via a wireless medium and collaborate to accomplish a common task, for example, environment monitoring, military surveillance, and industrial process control.[4] The basic philosophy behind WSNs is that, while the capability of each individual sensor node is limited, the aggregate power of the entire network is sufficient for the required mission. In many WSN applications, the deployment of sensor nodes is performed in an ad hoc fashion without careful planning and engineering. Once deployed, the sensor nodes must be able to autonomously organize themselves into a wireless communication network. Sensor nodes are battery-powered and are expected to operate without attendance for a relatively long period of time. Due to the severe energy constraints of large number of densely deployed sensor nodes, it requires a suite of network protocols to implement various network control and management functions such as synchronization, node localization, and network security. The traditional routing protocols have several shortcomings when applied to WSNs, which are mainly due to the energy-constrained nature of such networks.[4] Furthermore, these inconveniences are highlighted when the number of nodes in the network increases. A large number of research activities have been carried out to explore and overcome the constraints of WSNs and solve design and application issues.

2 ENERGY EFFICIENT ROUTING PROTOCOLS IN WS

2.1 Low-energy adaptive clustering hierarchy (LEACH)

LEACH [5] is the first and most popular energy-efficient hierarchical clustering algorithm for WSNs that was proposed for reducing power consumption. In LEACH, the clustering task is rotated among the nodes, based on duration. Direct communication is used by each cluster head (CH) to forward the data to the base station (BS). It uses clusters to prolong the life of the wireless sensor network. LEACH is based on an aggregation (or fusion) technique that combines or aggregates the original data into a smaller size of data that carry only meaningful information to all individual sensors. LEACH divides the a network into several cluster of sensors, which are constructed by using localized coordination and control not only to reduce the amount of data that are transmitted to the sink, but also to make routing and data dissemination more scalable and robust. LEACH uses a randomize rotation of high-energy CH position rather than selecting in static manner, to give a chance to all sensors to act as CHs and avoid the battery depletion of an individual sensor and dieing quickly. The operation of LEACH is divided into rounds having two phases each namely (i) a set-up phase to organize the network into clusters, CH advertisement, and transmission schedule creation and (ii) a steady-state phase for data aggregation, compression, and transmission to the sink.

- [1]*Kamal Kumar Gola is currently pursuing masters degree program in computer science & engineering in Uttarakhand Technical University, India, PH-9456893676. E-mail: kk_gola1503@gmail.com*
- [2]*Bhumika Gupta is currently working as Assistant Professor in Department of Computer science & Engineering GB Pant Engineering College, Pauri Garhwal, Uttarakhand, India.*
- [3]*Zubair Iqbal is currently working as Assistant Professor in Department of Computer science & Engineering Moradabadad Institute of Technology, Moradabad, Uttar Pradesh,India, PH-9997869683. E-mail: zubairiqbal17@gmail.com*

2.2 Power-Efficient Gathering in Sensor Information Systems (PEGASIS)

PEGASIS [6] is an extension of the LEACH protocol, which forms chains from sensor nodes so that each node transmits and receives from a neighbor and only one node is selected from that chain to transmit to the base station (sink). The data is gathered and moves from node to node, aggregated and eventually sent to the base station. The chain construction is performed in a greedy way. Unlike LEACH, PEGASIS avoids cluster formation and uses only one node in a chain to transmit to the BS (sink) instead of using multiple nodes. A sensor transmits to its local neighbors in the data fusion phase instead of sending directly to its CH as in the case of LEACH. In PEGASIS routing protocol, the construction phase assumes that all the sensors have global knowledge about the network, particularly, the positions of the sensors, and use a greedy approach. When a sensor fails or dies due to low battery power, the chain is constructed using the same greedy approach by bypassing the failed sensor. In each round, a randomly chosen sensor node from the chain will transmit the aggregated data to the BS, thus reducing the per round energy expenditure compared to LEACH.

2.3 Hybrid Energy-Efficient Distributed Clustering (HEED)

HEED [7] extends the basic scheme of LEACH by using residual energy and node degree or density as a metric for cluster selection to achieve power balancing. It operates in multi-hop networks, using an adaptive transmission power in the inter-clustering communication. HEED was proposed with four primary goals namely (i) prolonging network lifetime by distributing energy consumption, (ii) terminating the clustering process within a constant number of iterations, (iii) minimizing control overhead and (iv) producing well-distributed CHs and compact clusters. In HEED, the proposed algorithm periodically selects CHs according to a combination of two clustering parameters. The primary parameter is their residual energy of each sensor node (used in calculating probability of becoming a CH) and the secondary parameter is the intra-cluster communication cost as a function of cluster density or node degree (i.e. number of neighbors).

2.4 Power Efficient Data Gathering and Aggregation Protocol

Power Efficient Data Gathering and Aggregation Protocol [8] based on idea of minimum spanning tree. It minimized the long distance transmission among the sensor node and base station as well as minimized the distance between the sensor nodes. It is also a clustering algorithm, but it is more efficient as compare to LEACH and PEGASIS in terms of energy saving in sensor nodes. Another advantage is it enhances the life time of network even if base station is inside the field where as this condition can not applicable to either LEACH or PEGASIS.

2.5 Top down Approach

A Delay-aware data collection was done by Cheng et al. 2011 [9]. In their work they gave two approaches for data collection, one is Top-down and another one is bottom up approach. In bottom up approach the network structure is not that much energy efficient while transmitting the data to base station because in their network structure large numbers of nodes are involve in transmit their data to a longer distance so large amount of energy is consumed. In our research work we try to overcome this problem by reducing the transmission distance among nodes by forming a different network structure among the nodes and to transmit data as fast as possible as well.

3 ATTACKS ON ROUTING

Since the concept of sensor networks originates from the wireless ad-hoc networks, many attacks on wireless ad-hoc Networks can be adapted for sensor networks. Sybil attack is such an example.[10] Karlof and Wagner[11] show another types of attacks and furthermore they propose two novel attacks – HELLO floods and sinkholes. Denial of Service attacks on sensor networks are studied by Stankovic and Wood.[12] We present a brief summary of major attack Classes here.

3.1 Bogus routing information

The basic method how to influence routing is to change the routing information. An Adversary spoofs, alters or replays routing information. By these methods he can create loops in routing, increase Latency, extend the paths or attract the traffic to the chosen node.

3.2 Selective forwarding

Selective forwarding is a variant of the DoS attack. Malicious node forwards only chosen packets and drops the rest. Attacker has to be included in the path of the data flow to mount selective forwarding. To do so, he can use can use Sybil attack or sinkhole attack. The ultimate variant of this attack is called a Black hole attack. In such case, all the packets are dropped. However node behaving like a Black hole can be easily detected by the neighboring nodes, considered as dead and excluded from the routing path. Therefore dropping only some messages may be more beneficial for the attacker.

3.3 Sinkhole attack

The goal of the sinkhole attack is to attract as much of the traffic as possible to the malicious node. The principle of this attack is that the malicious node tries to look very attractive for other nodes with respect to the routing algorithm. This goal can be achieved, for example, by spoofing the route advertisement or by providing a high-quality path to the base station using wormhole attack. Sinkhole can be further used for selective forwarding, which is very efficient and easy in that case.

3.4 HELLO flood attack

In some protocols, nodes announce themselves to the neighbors by broadcasting the HELLO packets. Node receiving such packet concludes that the broadcasting node is his neighbor and is within the normal radio range. A laptop class attacker can use a powerful radio to send HELLO packets to nodes, which are far more distant than the normal radio range from him. These nodes will send their messages to oblivion trying to reach the neighbor, which is not in their radio range.

3.5 Wormhole attack

Wormhole is a low-latency out-of-band channel used to connect two distant part of the network. Wormhole attack exploits the routing race conditions. This means that message, which should normally traverse multiple nodes, traverse only single one and hence is delivered in a much less time. Time of the delivery can be important for the routing scheme, especially if the influenced message contains routing information. The attacker can send replayed packets through the wormhole to persuade two distant nodes that they are neighbors. He can, for example, create wormhole between the base station and a node at the opposite side of network, thus instead of multiple hops the node appears to be only single hop from the base station. Therefore it becomes a sinkhole for his neighbors providing low-latency route to the base station.

3.6 Acknowledgement spoofing

Acknowledgement spoofing focus on the algorithms using link layer acknowledgements. An attacker spoofs these acknowledgements to persuade the node, that its dead neighbor is alive or that the weak link is reliable. The impact is similar to selective forwarding; chosen packets are lost with high probability.

3.7 Sybil attack

In the Sybil attack, the attacker simulates multiple nodes and advertises multiple identities to the rest of the network. By this, he can cripple even the robust multipath routing algorithms, because the bulk of the paths (even all) may pass through him. In geographic routing, attacker's node can be virtually at more locations simultaneously and thus influence routing algorithm. Sybil attack in general means serious threat not only for routing, but also for other algorithms such as voting algorithm or distributed storage.

3.8 Denial of Service

Denial of Service represents more or less general class of attacks, which can be mounted on several ISO/OSI layers of wireless sensor network, including the network layer. Almost all above attacks, especially selective forwarding and HELLO floods, can result in the denial of service.

4 THE SYSTEM MODEL

4.1 Network Model

The protocol assumes that 40 sensor nodes are distributed randomly in the network area of diameter 100m. In addition to data aggregation, each node of the network has the capability to transmit data to other sensor nodes as well as to BS. The aim is to transmit the aggregated data to base station with minimum loss of energy which in fact increase system life time in terms of rounds. In this paper we consider sensor network environment where:

i) Each node periodically senses its nearby environment & likes to send this data to BS.
ii) Base Station is placed at a fix location.
iii) Sensor nodes are homogeneous & energy constrained.
iv) Sensor nodes are dynamic & are uniquely identified time to time.
v) Data fusion & aggregation is used to reduce the size of message in the network. We assume that combining n packets of size k results in one packet of size k instead of size nk.

4.2 Radio Model

We use the same radio model as discussed in [13]. In this model, a radio dissipates Eelec = 50 nJ/bit to run the transmitter or receiver circuitry and Eamp = 100 pJ/bit/m2 for the transmitter amplifier. The radios have power control and can expend the minimum required energy to reach the intended recipients. The radios can be turned off to avoid receiving unintended transmissions. An r2 energy loss is used due to channel transmission [14]. The equations used to calculate transmission costs and receiving costs for a k-bit message and a distance d are shown below:

Transmitting
Etr (k,d) = Eelec(k) +Eamp (k,d)
= kEelec+kEampd2
Receiving
ERx(k) = ERx-elec(k)
ERx(k) = Eelec*k
Receiving is also a high cost operation, therefore, the number of receives and transmissions should be minimal. LEACH and PEGASIS use the same constants (Eelec, Eamp, and k) for calculating energy costs; therefore the proposed protocol achieves energy savings by minimizing the distance and the number of transmissions and receives for each node. In our simulations, we used a packet length k of 2000 bits. It is assumed that the radio channel is symmetric so that the energy required to transmit a message from node i to node j is the same as energy required to transmit a message from node j to node i for a given signal to noise ratio (SNR).

5 PROBLEM STATEMENT

In this work, our main focus is to provide Security in WSN (wireless sensor networks) as well as to provide the strategy to collect the high speed data in efficient manner so that we can increase the network lifetime and decrease the energy consumption. As we know that all the sensor node are in direct communication range of each other and can transmit to and receive data from the other sensor node as well as to and receive the data from base station. The nodes periodically sense the environment and have always data to send in each round of communication. At the time of transmission of data, an attacker may change the whole data or can hack the data which create the problem. To overcome this problem we are using the concept of public and private key (Modified RSA Digital Signature Scheme). [15]

Sensor Node Information

X	Y	C_id	N_id	RE	Energy	TH	Distance
	TE	LOC	PU	PR	DS	RDM	RT

Where x and y are coordinates that represents the location of

the node in the network.
C_id=Cluster _id, N_id=Node_id, RE=Residual Energy TH=ThresholdValue,TE=Transmission Energy, LOC=Location of the nearest node to which data will be transmitted, PU=Public Key, PR=Private Key, DS=Digital Signature, RDM= Route discovery message, RT=Route Table.

6 PROPOSED ALGORITHM

Cluster Head Selection and Cluster Formation

1- All nodes will broadcast a message which contains node_id, transmission range, location and energy status in the network. With the help of this message each node must know about the node _id, transmission range and energy status of all other node in the network. Threshold will be defined by base station.

2- FFind the neighbor of each node that is come under transmission range. Distance between Node is calculated by given formula

$$\sqrt{(X2-X1)^2 + (Y2-Y1)^2} <= T\_Range$$

Where T_Range=8

3- Find the degree of node (ND) for each node that is calculated by total number of neighbours. ND=

$$\sum_{k=0}^{n} \text{Number of neighbours of each node}$$

4- FFor every node, compute the sum of distances with all its neighbors using given formula.

SV=

$$\sum_{k=0}^{n} \text{Distance of all neighbours of each node}$$

5- Compute the average energy of every node using given formula. Initially EEAV=1J

$$EEAV=1/NV \sum_{k=0}^{n} RE$$

6- Where, RE is the residual energy of all the neighboring nodes.

7- Calculate the value of location function LOS, for each node using given equation.

$$LOS= [(\alpha*ND) + (\beta*EEAV) + (\gamma*(1/SV))]$$

Where $\alpha + \beta + \gamma = 1$

α =0.3, β=0.3 and γ=0.3 are the weighting factors for the corresponding system parameters.

8- Select the node with the highest LOS as the cluster Head with the condition that all the neighbours of the selected Cluster Head are not allowed to take part in the election procedure. Now cluster head broadcast message of its selection within the cluster.

9- Repeat step 1 to 8 for all the remaining nodes till the Cluster and Cluster Head get forms.

Data Transmission within Cluster

10- After cluster formation, node having lowest location value will transmit their data to its nearest node with the condition that nearest node should be in same cluster, if the nearest node is in the other cluster then it will find the next nearest node in the same cluster. This process will continue till all the data reaches at cluster head and sensor node also maintain route table for future use.

11- Repeat step 10 for the entire cluster.

12- The nodes that already sent their data will be kept in sleep mode so that their energy level does not decrease.

Data Transmission From Cluster Head to Base Station

13- Route discovery message, RDM is initialized by the base station to all the cluster head nodes. The base station starts a multiple path discovery phase to create a set of neighbors that are able to forward data to the base station. In this case it may be possible that multiple path will be saved to send the data to the base station in their respective route table for future use.

14- In order to avoid collision, a TDM schedule will be followed in which each path will be active for a particular time quanta , in which cluster heads forward aggregates data to the next cluster head and ultimately to the base station. The process will start from the farthest cluster head. Meanwhile cluster heads in alternate paths will be busy in intra cluster communication i.e. collecting data from their member nodes in a cluster. This process will continue in a round robin fashion. Thus, inter cluster and intra cluster transmission will go hand in hand.

Re-Clustering Process

15- If the cluster head energy level becomes less, then

re-clustering procedure will be called. In this, old CH broadcast re-clustering message with in the cluster with its remaining energy level message. The member nodes compare the value of location function within the cluster.

16-

Member node having maximum value of location function and maximum energy will be elected as new cluster head.

17-

New cluster head broadcast message of its selection. And then repeat step 10 to 16.

18-

Data aggregation function will be implemented at each level by each node cluster head.

19-

The same process will be applied again until the nodes in WSN are died.

7 Modified RSA Digital Signature Scheme

a) Key Generation Process (By Cluster Head)

i) Select p and q with the condition that p and q both prime and p does not equal to q.

ii) Calculate n=p*q

iii) Calculate Ø(n)=(p-1)*(q-1)

iv) Select integer e gcd(Ø(n),e)=1; 1<e<Ø(n)

v) Calculate d e*d=1modØ(n)

vi) Public key (e , n)

vii) Private key(d , n)

b) Signing Process (By Member Node and Cluster Head)

i) Sensor node (sender node) create signature using own private key S=Md mod n where M is sensed data.

c) Encryption Process (By Member Node and Cluster Head)

i) Before sending the data and signature to sensor node (sender node) encrypt the data using K=M(e*d)mod n

ii) Now sensor node sends the encrypted data and signature to the nearest node (Receiver node).

d) Decryption and Verifying Process (By Member Node and Cluster Head)

i) Nearest node (Receiver Node) receive the data and signature and perform the decryption and verifying process P=Ke mod n if P = S then it verify the signature.

Calculate M= Pe mod n or M= Se mod n

Protocol Description:

i) Find The Distance Between Each Node

Distance Between		X1	Y1	X2	Y2	(X2-X1)	(Y2-Y1)	$(X2-X1)^2$	$(Y2-Y1)^2$	[(X2-X1)+(Y2-Y1)]	Square of [(X2-X1)+(Y2-Y1)]
Node-1	Node-2	3	3	9	2	6	-1	36	1	37	6.08276253
Node-1	Node-3	3	3	6	5	3	2	9	4	13	3.605551275
Node-1	Node-4	3	3	7	4	4	1	16	1	17	4.123105626
Node-1	Node-5	3	3	2	10	-1	7	1	49	50	7.071067812
Node-1	Node-6	3	3	3	13	0	10	0	100	100	10
Node-1	Node-7	3	3	6	11	3	8	9	64	73	8.544003745
Node-1	Node-8	3	3	8	9	5	6	25	36	61	7.810249676
Node-1	Node-9	3	3	9	6	6	3	36	9	45	6.708203932
Node-1	Node-10	3	3	7	12	4	9	16	81	97	9.848857802
Node-1	Node-11	3	3	6	16	3	13	9	169	178	13.34166406
Node-1	Node-12	3	3	5	18	2	15	4	225	229	15.13274595
Node-1	Node-13	3	3	7	18	4	15	16	225	241	15.5241747
Node-1	Node-14	3	3	8	16	5	13	25	169	194	13.92838828
Node-1	Node-15	3	3	10	18	7	15	49	225	274	16.55294536
Node-1	Node-16	3	3	12	5	9	2	81	4	85	9.219544457
Node-1	Node-17	3	3	12	9	9	6	81	36	117	10.81665383
Node-1	Node-18	3	3	12	3	9	0	81	0	81	9
Node-1	Node-19	3	3	13	11	10	8	100	64	164	12.80624847
Node-1	Node-20	3	3	15	11	12	8	144	64	208	14.4222051
Node-1	Node-21	3	3	15	15	12	12	144	144	288	16.97056275
Node-1	Node-22	3	3	17	17	14	14	196	196	392	19.79898987
Node-1	Node-23	3	3	17	18	14	15	196	225	421	20.51828453
Node-1	Node-24	3	3	19	16	16	13	256	169	425	20.61552813
Node-1	Node-25	3	3	20	15	17	12	289	144	433	20.80865205
Node-1	Node-26	3	3	20	12	17	9	289	81	370	19.23538406
Node-1	Node-27	3	3	19	10	16	7	256	49	305	17.4642492
Node-1	Node-28	3	3	21	10	18	7	324	49	373	19.31320792
Node-1	Node-29	3	3	18	7	15	4	225	16	241	15.5241747
Node-1	Node-30	3	3	19	4	16	1	256	1	257	16.03121954
Node-1	Node-31	3	3	21	3	18	0	324	0	324	18
Node-1	Node-32	3	3	22	6	19	3	361	9	370	19.23538406
Node-1	Node-33	3	3	24	3	21	0	441	0	441	21
Node-1	Node-34	3	3	25	6	22	3	484	9	493	22.20360331
Node-1	Node-35	3	3	27	4	24	1	576	1	577	24.0208243
Node-1	Node-36	3	3	28	2	25	-1	625	1	626	25.01999201
Node-1	Node-37	3	3	28	15	25	12	625	144	769	27.73084925
Node-1	Node-38	3	3	26	17	23	14	529	196	725	26.92582404
Node-1	Node-39	3	3	28	12	25	9	625	81	706	26.57066051
Node-1	Node-40	3	3	25	14	22	11	484	121	605	24.59674775

ii) Find the Neighbors of Each Node

NEIGHBOURS OF NODE-1

Distance Between		X1	Y1	X2	Y2	(X2-X1)	(Y2-Y1)	$(X2-X1)^2$	$(Y2-Y1)^2$	[(X2-X1)+(Y2-Y1)]	Square of [(X2-X1)+(Y2-Y1)]
Node-1	Node-3	3	3	6	5	3	2	9	4	13	3.605551275
Node-1	Node-4	3	3	7	4	4	1	16	1	17	4.123105626
Node-1	Node-2	3	3	9	2	6	-1	36	1	37	6.08276253
Node-1	Node-9	3	3	9	6	6	3	36	9	45	6.708203932
Node-1	Node-5	3	3	2	10	-1	7	1	49	50	7.071067812
Node-1	Node-8	3	3	8	9	5	6	25	36	61	7.810249676

NEIGHBOURS OF NODE-2

Distance Between		X1	Y1	X2	Y2	(X2-X1)	(Y2-Y1)	$(X2-X1)^2$	$(Y2-Y1)^2$	[(X2-X1)+(Y2-Y1)]	Square of [(X2-X1)+(Y2-Y1)]
Node-2	Node-4	9	2	7	4	-2	2	4	4	8	2.828427125
Node-2	Node-18	9	2	12	3	3	1	9	1	10	3.16227766
Node-2	Node-9	9	2	9	6	0	4	0	16	16	4
Node-2	Node-3	9	2	6	5	-3	3	9	9	18	4.242640687
Node-2	Node-16	9	2	12	5	3	3	9	9	18	4.242640687
Node-2	Node-1	9	2	3	3	-6	1	36	1	37	6.08276253
Node-2	Node-8	9	2	8	9	-1	7	1	49	50	7.071067812
Node-2	Node-17	9	2	12	9	3	7	9	49	58	7.615773106

iii) Find the Total Distance of Neighbors of Each Node

TOTAL DISTANCE OF NEIGHBOURS OF NODE-1

Distance Between		X1	Y1	X2	Y2	(X2-X1)	(Y2-Y1)	$(X2-X1)^2$	$(Y2-Y1)^2$	[(X2-X1)+(Y2-Y1)]	Square of [(X2-X1)+(Y2-Y1)]
Node-1	Node-3	3	3	6	5	3	2	9	4	13	3.605551275
Node-1	Node-4	3	3	7	4	4	1	16	1	17	4.123105626
Node-1	Node-2	3	3	9	2	6	-1	36	1	37	6.08276253
Node-1	Node-9	3	3	9	6	6	3	36	9	45	6.708203932
Node-1	Node-5	3	3	2	10	-1	7	1	49	50	7.071067812
Node-1	Node-8	3	3	8	9	5	6	25	36	61	7.810249676
TOTAL DISTANCE OF ALL NEIGHBOURS OF NODE-1											35.40094085

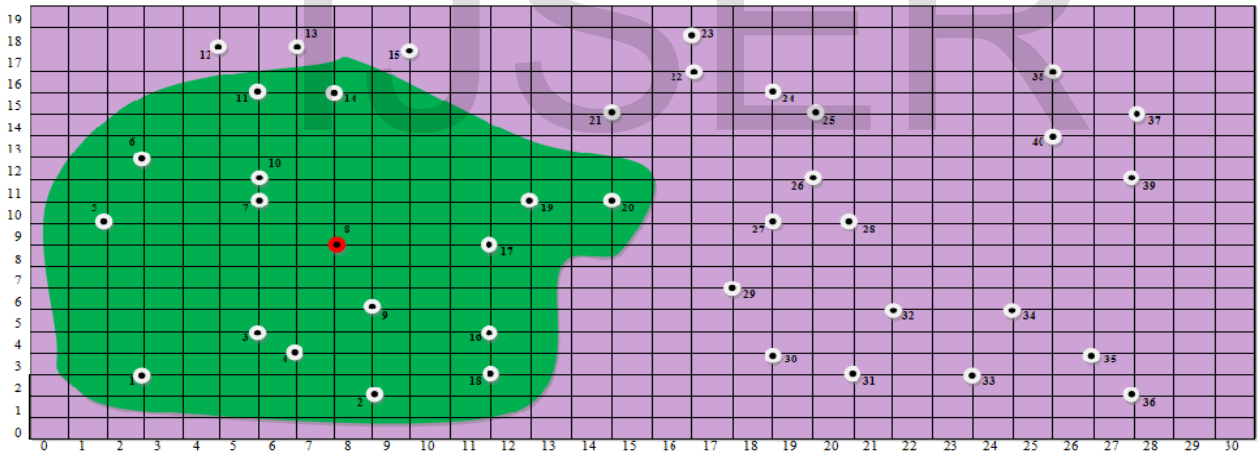
TOTAL DISTANCE OF NEIGHBOURS OF NODE-2

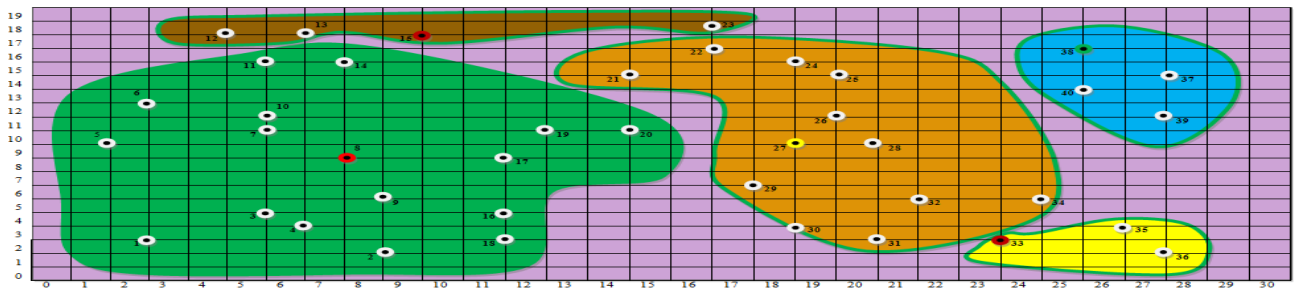
Distance Between		X1	Y1	X2	Y2	(X2-X1)	(Y2-Y1)	$(X2-X1)^2$	$(Y2-Y1)^2$	[(X2-X1)+(Y2-Y1)]	Square of [(X2-X1)+(Y2-Y1)]
Node-2	Node-4	9	2	7	4	-2	2	4	4	8	2.828427125
Node-2	Node-18	9	2	12	3	3	1	9	1	10	3.16227766
Node-2	Node-9	9	2	9	6	0	4	0	16	16	4
Node-2	Node-3	9	2	6	5	-3	3	9	9	18	4.242640687
Node-2	Node-16	9	2	12	5	3	3	9	9	18	4.242640687
Node-2	Node-1	9	2	3	3	-6	1	36	1	37	6.08276253
Node-2	Node-8	9	2	8	9	-1	7	1	49	50	7.071067812
Node-2	Node-17	9	2	12	9	3	7	9	49	58	7.615773106
TOTAL DISTANCE OF ALL NEIGHBOURS OF NODE-2											39.24558961

iv) Find the value of location function

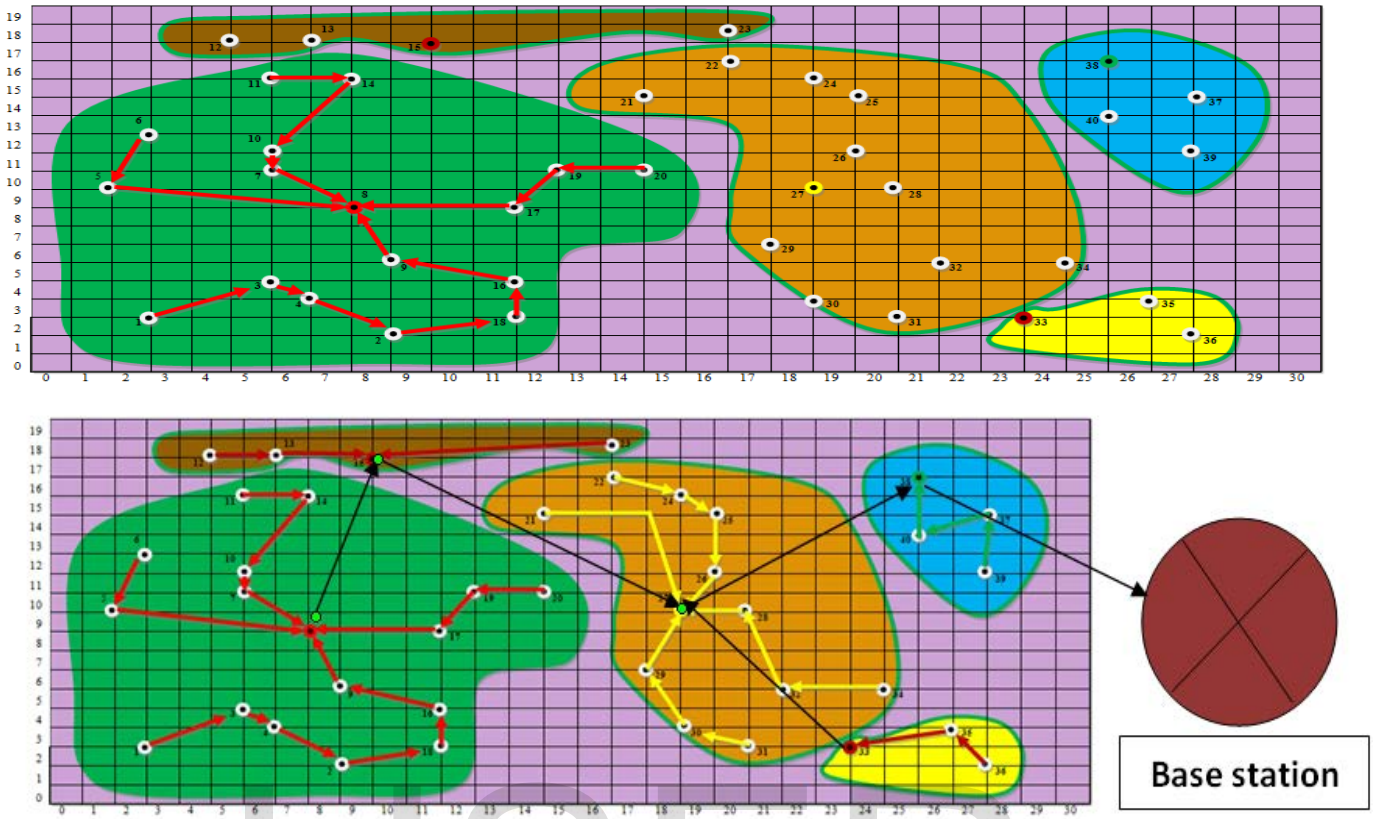
N_Identity	N_Location	T_Range	Degree of Node(ND)	Total Distance of All Neighbours(SV)	Average Energy(EEAV)	Location Function(LOS)
1	(3,3)	8	6	35.40094085	1	2.111299135
2	(9,2)	8	8	39.24558961	1	2.710192228
3	(6,5)	8	11	55.90666906	1	3.607154781
4	(7,4)	8	11	56.44361728	1	3.607086718
5	(2,10)	8	8	47.2488549	1	2.708465814
6	(3,13)	8	8	39.15594043	1	2.710215564
7	(6,11)	8	13	68.72517305	1	4.205820284
8	(8,9)	8	16	89.90468356	1	5.104449156
9	(9,6)	8	12	57.87762654	1	3.906911133
10	(7,12)	8	14	74.67306972	1	4.505356683
11	(6,16)	8	9	38.80123066	1	3.010308951
12	(5,18)	8	7	31.62240719	1	2.412649258
13	(7,18)	8	7	28.946328	1	2.413818678
14	(8,16)	8	10	47.15140433	1	3.30848331
15	(10,18)	8	9	49.52655982	1	3.008076475
16	(12,5)	8	11	56.34738171	1	3.607098821
17	(12,9)	8	14	78.24153769	1	4.505112374
18	(12,3)	8	9	48.32176609	1	3.008277843
19	(13,11)	8	15	88.92716576	1	4.804498063
20	(15,11)	8	14	78.11991613	1	4.505120333
21	(15,15)	8	12	63.68376943	1	3.906281035
22	(17,17)	8	9	43.38783384	1	3.009219174
23	(17,18)	8	7	32.66493291	1	2.412245548
24	(19,16)	8	11	54.65847228	1	3.60731817
25	(20,15)	8	11	53.28714362	1	3.607506501
26	(20,12)	8	15	82.85082091	1	4.804827955
27	(19,10)	8	15	82.15985024	1	4.804868558
28	(21,10)	8	14	77.45254814	1	4.505164452
29	(18,7)	8	13	70.62097423	1	4.20566404
30	(19,4)	8	10	54.89416269	1	3.307286749
31	(21,3)	8	9	45.83228587	1	3.008727472
32	(22,6)	8	10	45.54041414	1	3.308783407
33	(24,3)	8	8	36.97910739	1	2.710816919
34	(25,6)	8	12	67.77273833	1	3.905902078
35	(27,4)	8	5	19.6947001	1	1.820310033
36	(28,2)	8	5	25.64134397	1	1.815599806
37	(28,15)	8	3	8.990704785	1	1.244490394
38	(26,17)	8	6	32.5817424	1	2.112276814
39	(28,12)	8	6	33.9790299	1	2.111771966
40	(25,14)	8	9	47.60680304	1	3.00840216

v) Formation of Cluster





vi) Transmission of Data From Member Node to Cluster Head



8 Result and Conclusion

In this paper a secure strategy for high speed data transmission and efficient data collection based on dijkstra algorithm for shortest path and selection of cluster head as well as cluster formation is proposed. Proposed technique also provide the security at the time of transmission .In order to evaluate the performance of technique, we will simulate it on 40 node network. The simulations will do in c++. The BS is located at (0,-100) in a field of diameter 100m. We will run the simulation to determine the round in which every node is died. Parameters using will be same as that of [12]. Once a node dies it is considered dead for the rest of simulation, and our results expected to show much better system stable lifetime (period when all nodes of network are alive) because it balances energy dissipation among sensor nodes by using all nodes as cluster head with equal priority (highest energy node and highest location value will serve as cluster head) thus maximizing stable life time & achieves better results. We will implement in C++ to show the performance of our scheme.

References

[1] "21 ideas for the 21st century", Business Week, Aug. 30 1999, pp. 78-167.

[2] S.K. Singh, M.P. Singh, and D.K. Singh, "A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", International Journal of Advanced Networking and Application (IJANA), Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.

[3] S.K. Singh, M.P. Singh, and D.K. Singh, "Energy-efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN), Aug.2010, vol. 2, no. 3, pp. 49-61.

[4] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[5] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks" in IEEE Tmnsactions on Wireless Communications (October 2002), vol. 1(4), pp. 660-670.

[6] S. Lindsey and C.S. Raghavendra, "PEGASIS: Power-efficient Gathering in Sensor Information System", Proceedings IEEE Aerospace Conference, vol. 3, Big Sky, MT, Mar. 2002, pp. 1125-1130.

[7] Ossama Younis and Sonia Fahmy" Heed: A hybrid, Energy-efficient, Distributed Clustering Approach for Ad-hoc Networks", IEEE Transactions on Mobile Computing, vol. 3, no. 4, Oct.-Dec. 2004, pp. 366-369.

[8] HO. Tan, "Power efficient data gathering and aggregation in wireless sensor networks," SIGMOD Record, 2003, 32(4): 66 -71.

[9] Chi-Tsun Cheng, Chi K Tse, and Francis CM Lau. A delay-aware data collection network structure for wireless sensor networks. Sensors Journal, IEEE, 11(3):699–710, 2011.

[10] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, vol. 1, issue 2-3, pages 293–315, September 2003.

[11] James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig. The sybil attack in sensor networks: analysis & defenses.In IPSN'04:

Proceedings of the third international symposium on Information processing in sensor networks, pages 259–268, New York, NY, USA, 2004. ACM Press.

[12] Anthony D. Wood and John A. Stankovic. Denial of service in sensor networks. IEEE Computer, vol. 35, issue 10, pages 54–62, 2002.

[13] T. S. Rappaport. Wireless Communications. Prentice-Hall, 1996.

[14] R. Steele. Mobile Radio Communications. Pentech Press, London, 1992.

[15] Vaibhav Sharma, Gulista Khan, Kamal Kr. Gola and Rahul Rathore "SECURITY STRATEGY FOR DYNAMIC HOMOGENEOUS WSN"IJARCSSE 3 (4),March - 2014,pp. 1-8