Implementation and Result Analysis of Secure Strategy for High Speed Transmission and Efficient Collection of Data in Wireless Sensor Network

Kamal Kr. Gola
M.Tech Student at CS and E Deptt.
Uttarakhand Technical University. Uttarakhand

Bhumika Gupta
Asst. Prof., Dept. of CS and E
G.B. Pant Engg. College
Pauri Garwal, U.K., India

Zubair Iqbal
Asst. Prof., Dept. of CS and IT,
Moradabad Institute of Technology
Moradabad, U.P., India

ABSTRACT
In this work, the 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 an efficient manner. Sensor networks are usually deployed in hostile and unattended environment where an adversary can read and modify the content of the data packet. In such situation the most popular type of attack is the external attack and replay attack. The node needs to be authenticated before data transmission takes place. In external attack the node does not belong to the network try to read and modify the packet. For that we also need to authenticate the node before data transmission. To overcome this problem we are using the concept of public and private key (Modified RSA Digital Signature Scheme). So this work tries to develop an algorithm which will form a network structure in wireless sensor network through which data can be transmitted faster to the base station without affecting life time of network and it also provide the security during communication. The cluster head in a cluster is generally involved in long distance transmission that's why its energy level decreases faster than other cluster members in a cluster. To overcome this problem we used the concept of re-clustering to rotate the responsibility of cluster head among the cluster members in a cluster so that energy can be properly distributed among the nodes.

General Terms
Data Security.

Keywords
WSN, energy efficient, cluster head, data aggregation function, shortest path algorithm, base station, modified RSA digital signature scheme, re-clustering process and QoS parameters.

1. INTRODUCTION
A simplest wireless sensor network (WSN) is a network, possibly having a low - size and minimum complexity or someone can define a sensor network as a composition of a large number of sensor nodes that are densely deployed. A wireless sensor network mainly consists of spatially distributed autonomous sensors those monitor the physical or environmental conditions cooperatively like temperature, sound, vibration, motion, pressure, pollutants, etc. A single WSN can contain a few or several hundreds or even thousand sensors, generally called as nodes, where each node is connected to one or many sensors. Nodes sense the environment and then communicate the information which is collected from the monitored field. The data is forwarded through wireless links, possibly via multiple hops, to a sink that can use it locally, or is connected to other networks (e.g. The Internet) through a gateway. The sink node is a kind of the destination node, where the entire messages originated by sensor nodes are collected. Or in other words, it represents the end point of data collection in wireless sensor network.

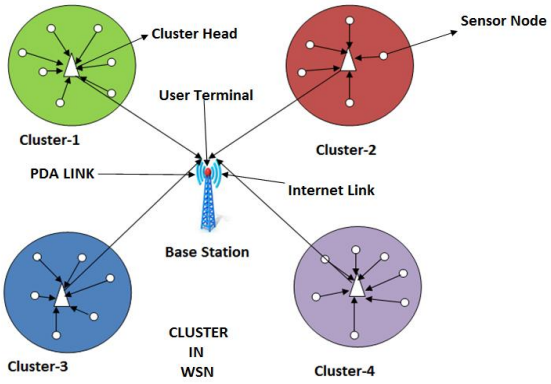

Figure 1.1 Cluster in Wireless sensor network

2. APPLICATION OF WSN
It has many applications in our daily life that are summarized as follow.

1. It can be used for process management with the help of deployment of wireless sensor nodes in an area where a particular phenomenon is to be monitored.
2. Wireless sensor networks have been deployed in several cities to monitor the concentration of dangerous gases for citizens.
3. A network of Sensor Nodes can also help us to find the position and timing if a forest has caught fire. In this, sensor nodes, which are capable of measuring temperature, humidity, gases produced by fire in the trees or vegetation and distance, are used to establish a network which will provide the position of forest at the time of the fire.
4. WSN's can also be used for the purpose of industrial monitoring as well as machinery condition-based maintenance (CBM). It offers significant cost savings and enables new functionality in comparison to a wired system because installation of more sensors is limited by the cost of wiring in wired networks.
5. Wireless sensor networks are also used for the purpose of Data logging in which data is collected for monitoring the environmental information. Then the collected

statistical information is used to show how the systems actually work. The advantage of logging through WSNs over conventional loggers is that the "live" data feed is possible through WSN's.

3. ROUTING CHALLENGES AND DESIGN ISSUES IN WSN

1. Node deployment in WSNs is application dependent that affects the performance of the routing protocol. The deployment of sensor nodes can be of two types: deterministic and randomized.
2. Sensor nodes can lose their accuracy while performing computations and transmitting information in a wireless environment as times passes because nodes are having a limited supply of energy. So energy consumption without losing its accuracy is a major challenge in designing of a WSN.
3. The next factor that generally comes under consideration when we design a WSN is data reporting mode The next factor that generally comes under consideration when we design a WSN is data reporting model. Data reporting can be categorized as follows: time-driven (continuous), event-driven, query-driven, and hybrid [1].
4. Generally network architectures assume that sensor nodes are stationary. However, mobility of base stations and sensor nodes is sometimes necessary, according to applications, so the routing scheme must be applicable for this type of network also.
5. The main problem generally arises when a WSN is deployed is that due to high node density in sensor networks, each node is precluded from being completely isolated from other nodes.
6. Range of coverage of each node is also the limitation of WSN.
7. Data reduction should be done for redundant data, so that network can be made bandwidth efficient.

4. ATTACKS ON ROUTING IN WSN

Bogus routing information By these methods, an attacker can create loops in routing, increase Latency, extend the paths or attract the traffic to the chosen node.

Sinkhole attacks 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 [2].

HELLO flood attack In some protocols, nodes announce themselves to the neighbors by broadcasting the HELLO packets. The node receiving such packet concludes that the broadcasting node is his neighbour and is within the normal radio range. These nodes will send their messages to oblivion trying to reach the neighbor, which is not in their radio range [2].

Sybil attack In the Sybil attack, the attacker simulates multiple nodes and advertises multiple identities to the rest of the network. By this, an attacker can cripple even the robust multipath routing algorithms. [3].

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].

5. LITERATURE REVIEW

Low-energy adaptive clustering hierarchy abbreviated as (LEACH): Heinzelmanet al. Proposed a clustering algorithm called LEACH [5]. In the LEACH technology, the nodes arrange themselves as local clusters, where one node acts as the head of the cluster. All head nodes in the non-cluster transmit their data to the cluster head, while the cluster head node receives data from all the cluster members, performs signal processing functions on the data (e.g., data aggregation), and transmits data to the remote BS.

Power-Efficient Gathering in Sensor Information Systems (PEGASIS): Lindsey and Raghavendra Proposed a PEGASIS protocol [6]. The core idea in PEGASIS is construction of such a chain among the sensor nodes in which each node will receive from the closest possible node and will transmit to a close neighbor. Gathered data moves from one node to the other, get intermixed, and ultimately a node which is designated transmits it to the BS.

(Power Efficient Data Gathering and Aggregation Protocol): Tan and Korpeoglu created a PEDAP protocol [7] further extended the PEGASIS protocol. In the PEDAP protocol, all the sensor nodes make a minimum three of Spain. Apart from bringing down the volume of long distance transmission, the communication distances between the sensor nodes also get lessened. It is a clustering algorithm, but it is more effective in comparison to the LEACH and PEGASIS in terms of energy saving in sensor nodes.

A similar kind of work was done on data collection efficiency by Florenset al. [8]. In their work, lower on data collection time are figured out for various network structures. However, the data fusion's impact, which is considered as one of the major features of sensor networks, was not considered. Wang et al. [9] proposed link scheduling algorithms for wireless sensor networks which can raise network throughput sensor networks which considerably. In their work, however, it is considered that data links to the wireless sensor nodes are defined earlier itself. In contrast, the objective of this paper is to construct the data links amongst the wireless sensor nodes and hence to lessen the delays in the data collection processes.

Chatterjee et al proposed a weight based dispersed clustering algorithm (WCA) [10] which can energetically acclimatize itself with the ever altering topology of ad hoc networks. This approach curbs the number of nodes to be furnished by a cluster head so that it does not demean the MAC functioning. The algorithm performs only when there is a demand, i.e., when a node is no longer able to put together to allocate the load as much as possible itself to any of the existing cluster heads.

An improved WCA, IWCA [11] considers additional constraints like energy and transmission rate for selecting cluster heads. The proposed algorithm is re run after fixed time interval to heads chosen can act as the application nodes in a two-tiered wireless sensor network and may change in different time intervals. After a fixed interval of time, the proposed algorithm is re-run again to find new applications nodes such that the system lifetime can be expected to last longer.

In MSMTP [12] protocol all nodes of the network will transmit the sensed information or aggregated data to their neighbor which are connected in MST structure by multi hop communication. Whole network is divided into three tiers. A

node of tier1 having highest energy will transmit network's fused data to base station, and similarly anode of highest energy from lowest possible tier id is selected to transmit data to base station & in this way load is evenly distributed to all nodes of the sensor network. This will improve the overall system lifetime.

The proposed approach named as Minimum Spanning based clustering Tier Technique (MSCT2) [13] is based on multi hop data transmission nodes to those neighbor nodes which are connected to it in minimum spanning tree (MST) structure for all the nodes of the network and then a node of Highest energy among highest rank tier will transmit the whole network aggregated data to base Station, we keep on repeating this procedure.

6. ENERGY CONSUMPTION MODEL

In proposed technique, we assume a model where the radio dissipates E_{elec}= 50nJ/bit to run the transmitter or receiver circuitry and ε_{amp}= 100pJ/bit/m^2 for the transmit amplifier to achieve an acceptable E_b/N_o [14]. The power needed to transmit k bits of data over a distance d is:

$$E_{tx} = E_{elec}(k) + \varepsilon_{amp} k d^2 \quad (6.1)$$

And the power needed to receive k bits of data is:

$$E_{rx} = E_{ele}(K) \quad (6.2)$$

Where d is the distance between the sources and sinks. Assume that there are 'n' numbers of intermediate nodes to reach at the destination and also each adjacency nodes are differentiated with distance 'r' between them. So the total distance between sources to sink is 'nr'. If we consider the energy expenditure at each node during transmitting a single k-bit message from source node 'N' to base station. A node located with a distance from the base station using the direct communication approach is in equations 6.1 and 6.2, then from equation (6.1)

$$\begin{aligned} E_{direct} &= E_{tx}(k, d = n*r) \\ &= E_{elc}*k + \varepsilon_{amp}*k*(nr)^2 \quad (6.3) \\ &= k\,(E_{elc} + \varepsilon_{amp} n^2 r^2) \end{aligned}$$

Packet passes through the 'n' intermediate nodes to reach at the destinations means it required 'n' times transmit and 'n-1' time receive. From Equation (6.2)

$$E_{rx} = (n-1)E_{elec}K \quad (6.4)$$

So total energy conservation to reach at the destination is

$$\begin{aligned} E &= n\,(E_{elc}*k + \varepsilon_{amp}*k*r^2) + (n-1)\,Erx \\ &= k((2n-1)E_{elec} + \varepsilon_{amp} n r^2) \quad (6.5) \end{aligned}$$

In the direct communication with base station the energy conservation is

$$\begin{aligned} E &= Etx + Erx \\ &= E_{elec}k + \varepsilon_{amp} k d^2 + E_{elec}k \\ &= E_{elec}k + \varepsilon_{amp} k r^2 + E_{elec}k = k\,(2E_{elec} + \varepsilon_{amp} r^2) \end{aligned} \quad (6.6)$$

From the above equations the total energy at n hop distance from the source to sink is defined in equation (6.5) and for single hop communication in equation (6.6).

7. PROPOSED ALGORITHM

7.1 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 nodes in the network. The threshold will be defined by the base station.

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

$$\sqrt{(x2-x1)^2 - (y2-y1)^2} <= T\_Range$$

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

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

4- For 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. $EEAV = 1/NV \sum_{k=0}^{n} RE$

Here, RE is the residual energy of all the neighboring nodes.

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

$$\mathbf{LOS} = \left[(\boldsymbol{\alpha}*\mathbf{ND}) + (\boldsymbol{\beta}*\mathbf{EEAV}) + (\boldsymbol{\gamma}*(\mathbf{1}/\mathbf{SV}))\right]$$

Where α + β + γ =1 α, β and γ are the weighting factors for the corresponding system parameters.

7- 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.

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

7.2 Data Transmission within Cluster

1- 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 the 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 reach at cluster head.

2- If the nearest node is the cluster head, then it directly sends the data to the cluster head.

3- Repeat step 1 for the entire cluster.

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

7.3 Data Transmission from Cluster Head to Base Station

1- 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 as 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.

2- In order to avoid collision, a TDMA 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 around robin fashion. Thus, inter cluster and intra cluster transmission will go hand in hand.

7.4 Re-clustering Process

1- If the cluster head energy level becomes less, then re-clustering procedure will be called. In this, old CH broadcast, re-clustering message within the cluster with its remaining energy level message.

2- The member nodes compare the value of location function and residual energy within the cluster.

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

4- New cluster head broadcast message of its selection and repeat step 10 to 16.

5- The data aggregation function will be implemented at each level by each node and cluster head.

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

7.5 Modified RSA Digital Signature Scheme

7.5.1 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 $\emptyset(n) = (p-1)*(q-1)$

iv) Select integer e , $\gcd(\emptyset(n), e) = 1;\ 1 < e < \emptyset(n)$

v) Calculate d $e * d = 1 \bmod \emptyset(n)$

vi) Public key $(e\ ,\ n)$

vii) Private key $(d\ ,\ n)$

7.5.2 Signing Process (By Member Node and Cluster Head)

i) Sensor node (sender node) creates signature using own private key $\mathbf{S = M^d \bmod n}$ where M is sensed data and S is a digital signature.

7.5.3 Encryption Process (By Member Node and Cluster Head)

i) Before sending the data and signature to receiver node, the sender node encrypts the data using

$$\mathbf{K = M^e \bmod n}$$

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

7.5.4 Decryption and Verifying Process

i) Nearest node (Receiver Node) receives the data and the signature and perform the decryption and verifying process $\mathbf{M = K^d \bmod n}$ it's provide the data confidentiality.

ii) Calculate $\mathbf{S1 = S^e \bmod n}$ if **S1=M** then it's provide the sender authentication.

8. IMPLEMENTATION

i) First deploy the sensor node in the network

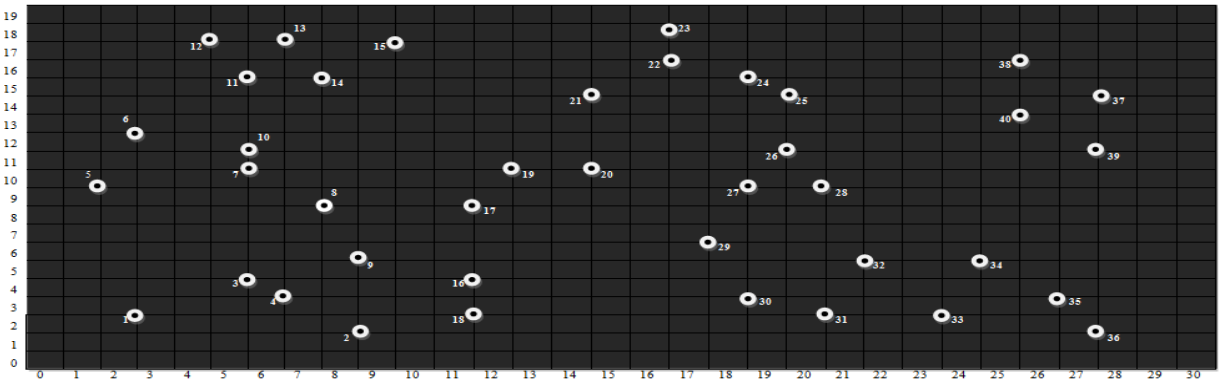

Figure 8.1 Deployment of Sensor node

ii) Find the value of location function.

Table 8.1 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)
8	(8,9)	8	16	89.90468356	1	5.104449156
27	(19,10)	8	15	82.15985024	1	4.804868558
26	(20,12)	8	15	82.85082091	1	4.804827955
19	(13,11)	8	15	88.92716576	1	4.804498063
10	(7,12)	8	14	74.67306972	1	4.505356683
28	(21,10)	8	14	77.45254814	1	4.505164452
20	(15,11)	8	14	78.11991613	1	4.505120333
17	(12,9)	8	14	78.24153769	1	4.505112374
7	(6,11)	8	13	68.72517305	1	4.205820284
29	(18,7)	8	13	70.62097423	1	4.20566404
9	(9,6)	8	12	57.87762654	1	3.906911133
21	(15,15)	8	12	63.68376943	1	3.906281035
34	(25,6)	8	12	67.77273833	1	3.905902078
25	(20,15)	8	11	53.28714362	1	3.607506501
24	(19,16)	8	11	54.65847228	1	3.60731817
3	(6,5)	8	11	55.90666906	1	3.607154781
16	(12,5)	8	11	56.34738171	1	3.607098821
4	(7,4)	8	11	56.44361728	1	3.607086718
32	(22,6)	8	10	45.54041414	1	3.308783407
14	(8,16)	8	10	47.15140433	1	3.30848331
30	(19,4)	8	10	54.89416269	1	3.307286749
11	(6,16)	8	9	38.80123066	1	3.010308951
22	(17,17)	8	9	43.38783384	1	3.009219174
31	(21,3)	8	9	45.83228587	1	3.008727472
40	(25,14)	8	9	47.60680304	1	3.00840216
18	(12,3)	8	9	48.32176609	1	3.008277843
15	(10,18)	8	9	49.52655982	1	3.008076475
33	(24,3)	8	8	36.97910739	1	2.710816919
6	(3,13)	8	8	39.15594043	1	2.710215564
2	(9,2)	8	8	39.24558961	1	2.710192228
5	(2,10)	8	8	47.2488549	1	2.708465814
13	(7,18)	8	7	28.946328	1	2.413818678
12	(5,18)	8	7	31.62240719	1	2.412649258
23	(17,18)	8	7	32.66493291	1	2.412245548
38	(26,17)	8	6	32.5817424	1	2.112276814
39	(28,12)	8	6	33.9790299	1	2.111771966
1	(3,3)	8	6	35.40094085	1	2.111299135
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

iii) According to the LOS value, select the cluster head and form the cluster.

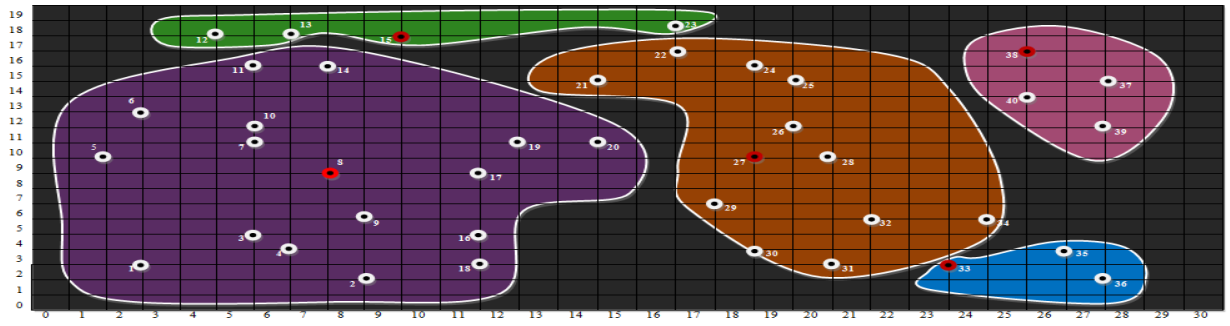

Figure 8.2 Cluster Formation

iv) Key generation process by cluster head

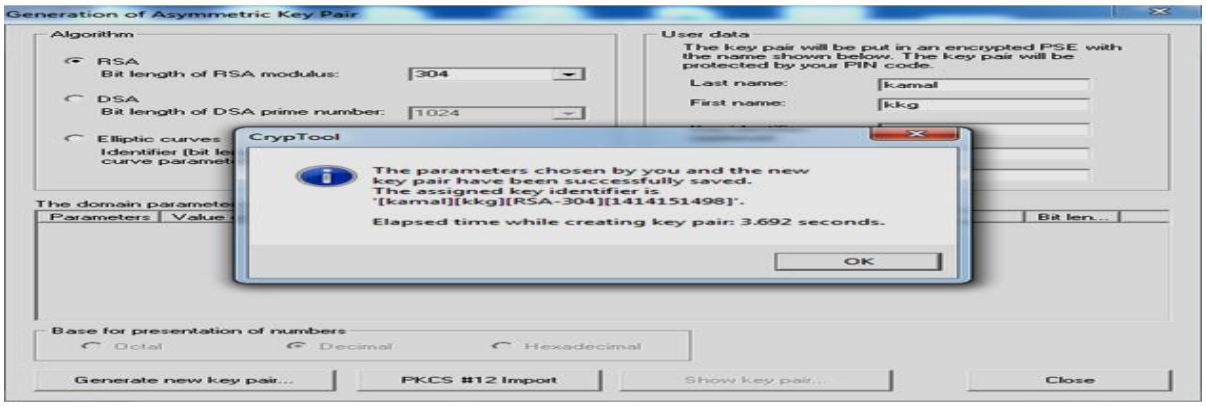

Figure 8.3 Key Generation

v) Now each sender node encrypts the message using public key.

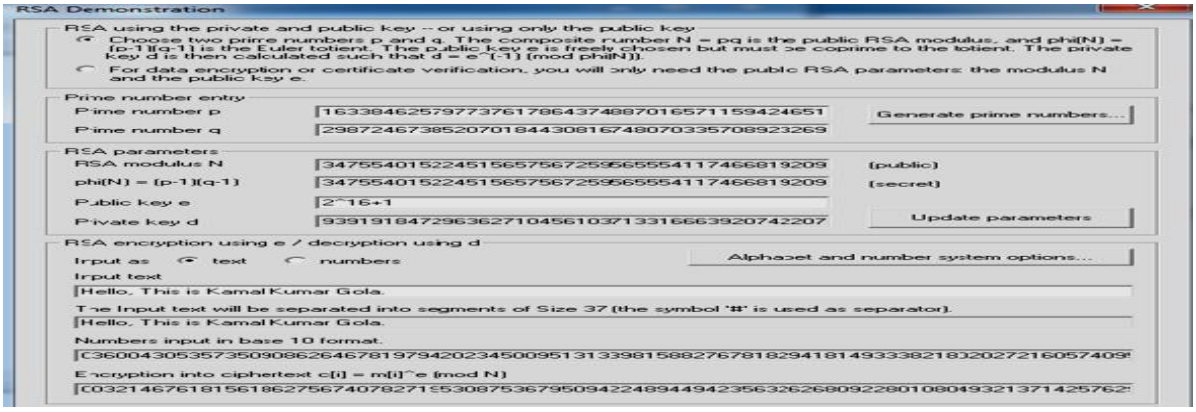

Figure 8.4 Encryption Process

vi) Each sender node generates the signature using private key.

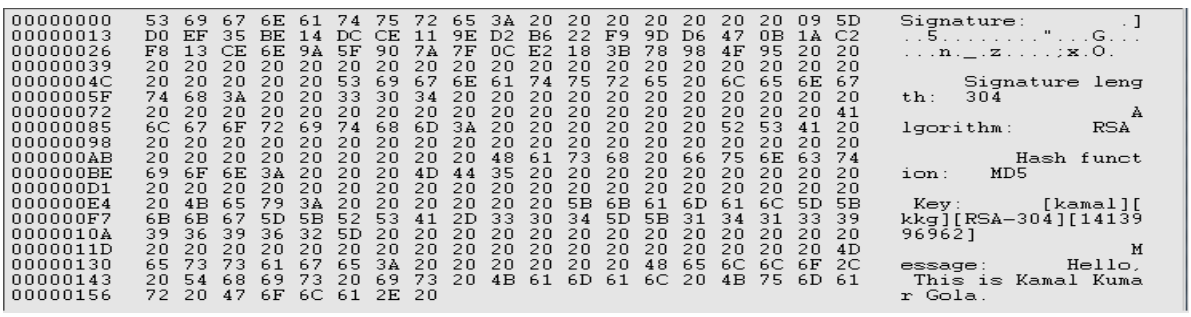

Figure 8.5 Signature Generation

vii) Now for signature verification, receiver node verifies the signature using public key.

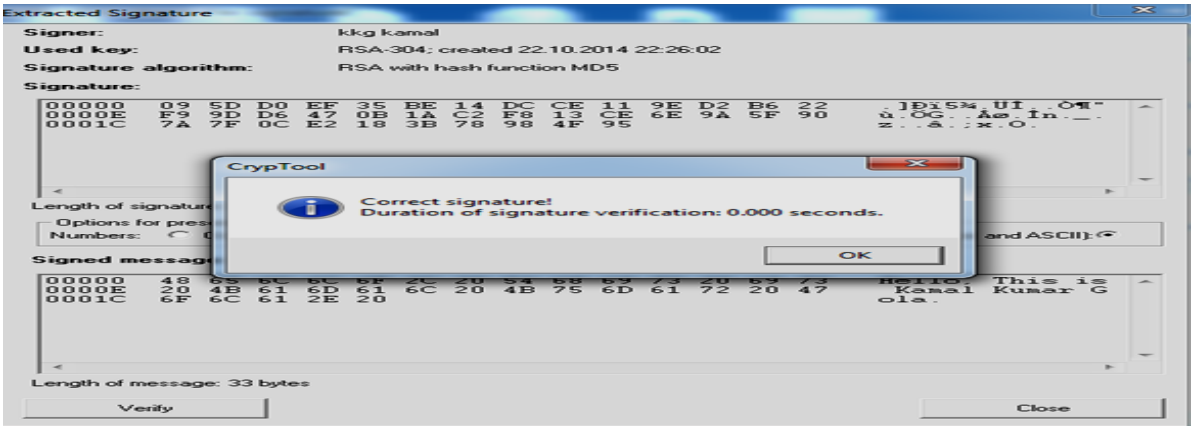

Figure 8.6 Signature Verification

viii) Now receiver node decrypts the message using private key.

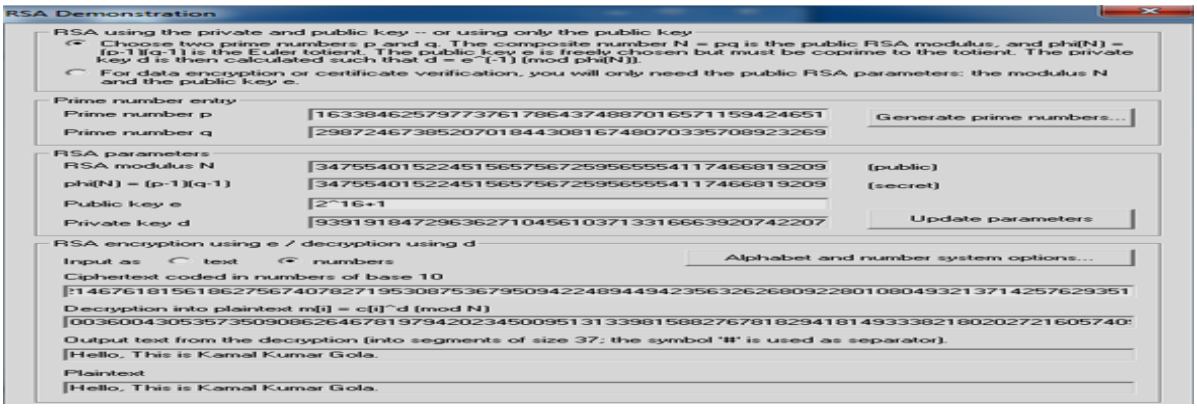

Figure 8.7 Decryption Process

9. RESULT

In order to evaluate the performance of the technique, we have simulated it on a 40 node network. The implementation has been done in C Language. The BS is located at (0, 100) in a field of diameter 100m and for security implementation we used Cryp Tool 1.4.30.

Figure 9.1 shows that the number of clusters which will be formed using the proposed approach. This approach has been compared with MSCT2 approach. In this graph, X-axis indicates number of clusters, Y-axis indicates the transmission range and it is clearly shown that the proposed approach has the best result as compare to MSCT2.

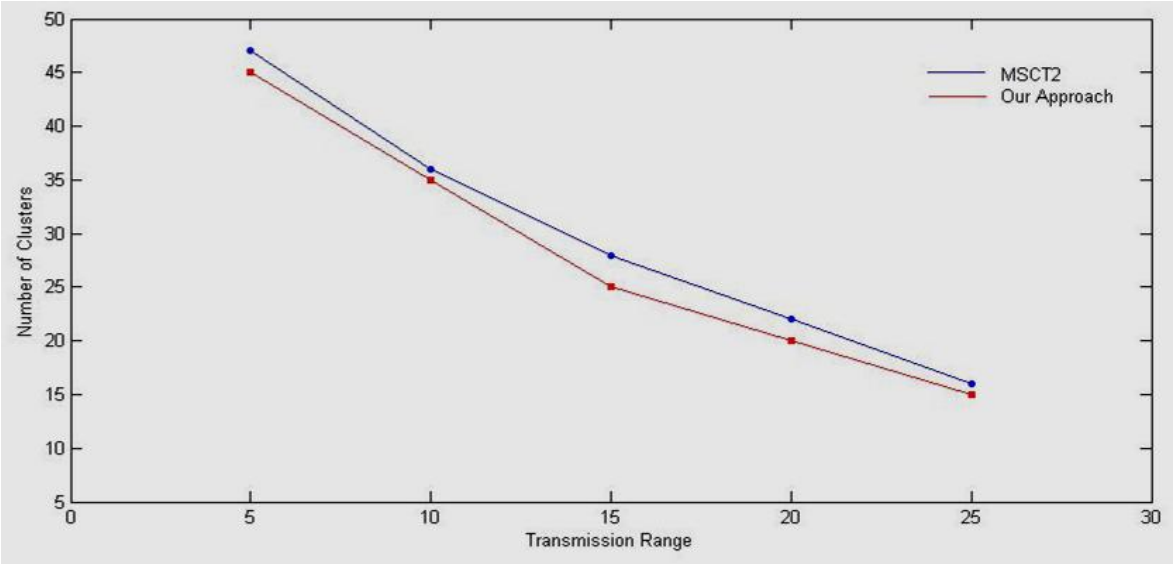

Figure 9.1 Transmission range vs. Cluster

Figure 9.2 shows that comparison of the proposed approach with a MSCT2 in terms for data collection time. In this graph, X-axis indicates the number of nodes, Y-axis indicates the number of data collection and it is clear that the proposed approach shows the best result as compared to MSCT2.

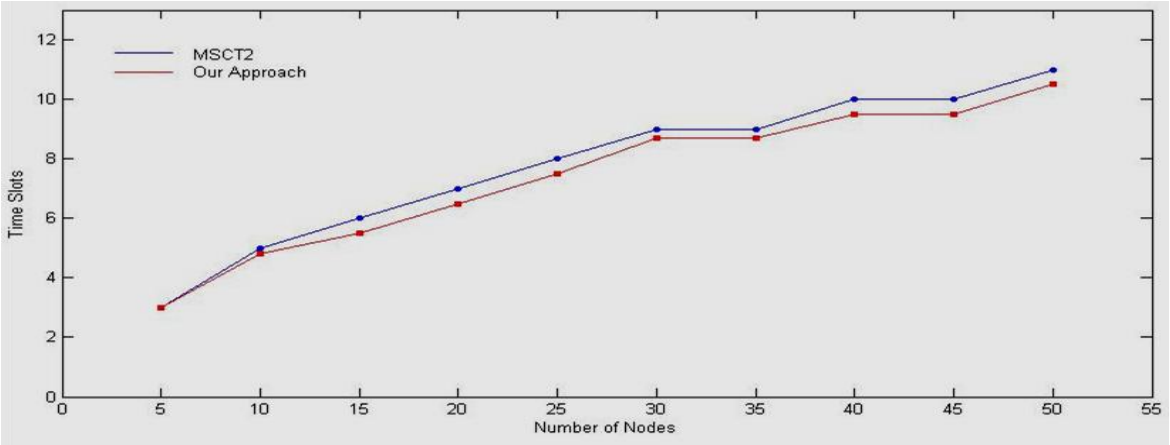

Figure 9.2 Average Data Collection Time

Figure 9.3 shows that comparison of the proposed approach with MSCT2 approach in terms of alive nodes. In this result, we found that using a proposed approach number of alive nodes increased as compared to MSCT2.

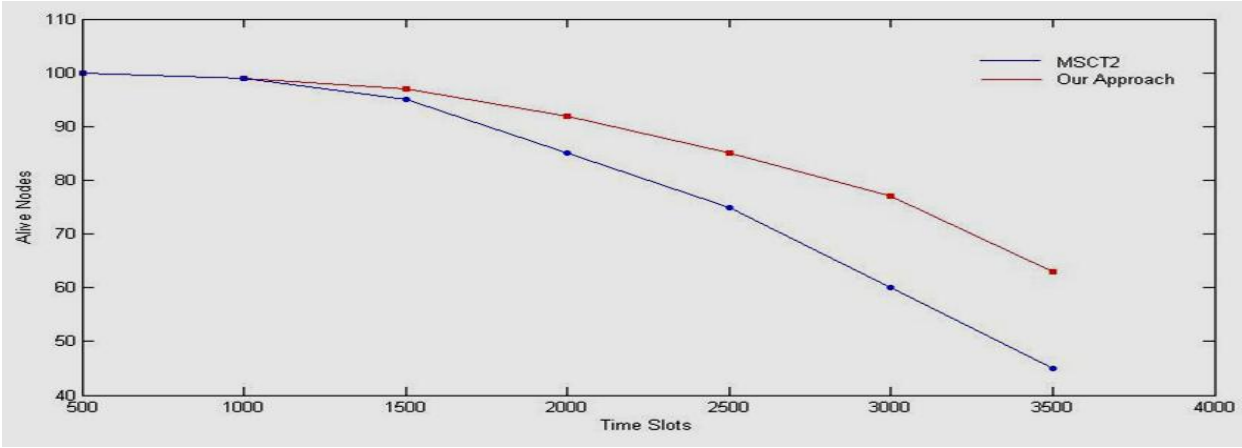

Figure 9.3 Network Lifetime

Figure 9.4 shows that comparison of the proposed approach with others on the basis of energy consumption in the network. So that sensor nodes can transmit their data to base station within their limited battery powered.

In this graph X-axis indicates round and Y-axis indicates energy consumption in the network. From the graph, it is clear that the proposed approach shows the best result as compared to another.

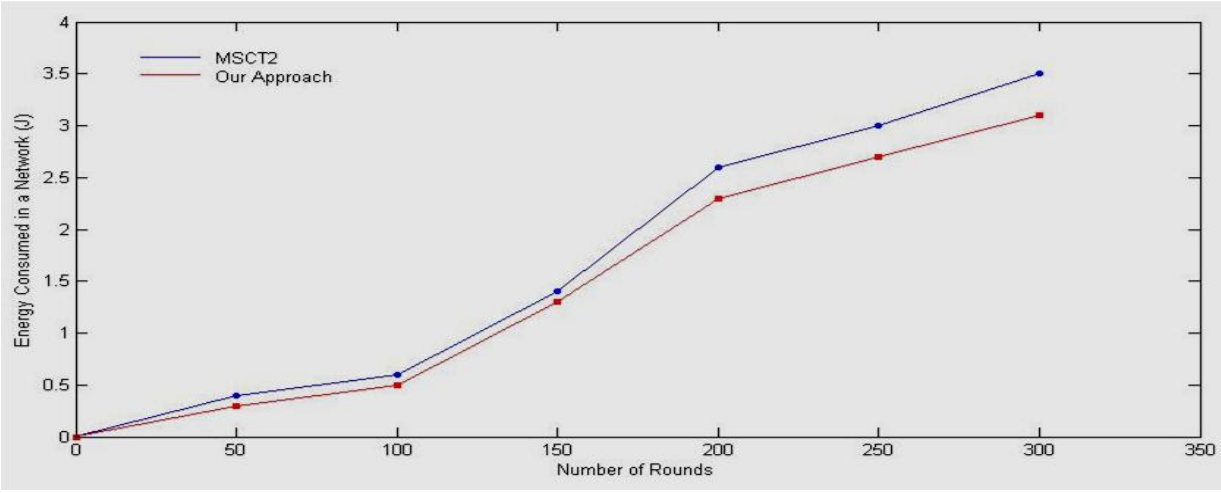

Figure 9.4 Overall energy consumption

10. CONCLUSION

Wireless sensor network is becoming an increasingly important technology that will be widely used in a variety of applications such as public safety, environmental surveillance, disaster surveillance, medical, home and office security, transportation, and military. Sensor networks are usually deployed in hostile and unattended environment where an adversary can read and modify the content of the data packet. This work proposed a secure strategy for high speed data transmission and efficient collection of data in WSN. Proposed algorithm provides security and energy efficiency method for data collection and also provides a technique to select the best cluster head in the cluster. The proposed mechanism is used for secure data transmission, which can able to avoid external attack and authenticate the node during the data transmission and collection process. The proposed security method provides positive features of security such as authentication of the sender and confidentiality of data. The proposed method provides the security features with reducing the packet drop and keep data freshness. This analysis of comparison results established that proposed technique is secured and provide better performance.

11. REFERENCES

[1] Yao, Y. and Gehrke, J., September 2002. The cougar approach to in-network query processing in sensor networks. In SIGMOD Record.

[2] Karlof, Chris. and Wagner, David., September 2003. 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.

[3] Newsome, James. Shi, Elaine. Song, Dawn. and Perrig, Adrian. The Sybil attack in sensor networks: analysis& defenses. In IPSN'04: Proceedings of the third international symposium on Information processing in sensor networks 2004, pages 259–268, New York, NY, USA, ACM Press.

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

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

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

[7] H¨useyin Ozg¨ur Tan. and Ibrahim K Orpeoglu., 2003. Power efficient data gathering and aggregation in wireless sensor networks. *ACM Sigmod Record*, 32 (4): 66–71.

[8] Sun, Xianwei. C-H Huang, Scott. and Li, Minming., 2012. Data collection time in sensor networks", *In Wireless Algorithms, Systems, and Applications*, pages 120–131. Springer.

[9] Wang, Weizhao. Wang, Yang Li, Yu. Wen-Zhan Song, Xiang and Frieder, Ophir. Efficient interference-aware TDMA link scheduling for static wireless networks. In Proceedings of the 12th annual international conference on Mobile computing and networking,2006, pages 262–273. ACM.

[10] Chatterjee, M. Das, and Turgut., 2001. WCA: a weighted clustering algorithm for mobile ad hoc networks. *Cluster Computing*, Vol. 5, No. 2, pp.193–204.

[11] Cheng-Hsi and Wu Tzung-Pei Hong, "An Improved Weighted Clustering Algorithm for Determination of Application Nodes in Heterogeneous Sensor Networks", *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 2, No. 2, pp.173-184, (2011).

[12] Bathla, Gaurav.Khan, Gulista.,2011. Energy efficient routing protocol for Homogeneous WSN, *International Journal of Cloud Computing services and Architecture(IJCCSA)*, Volume 1,Number 2.

[13] Khan, Gulista. Ali, Wajid.Arya, Swati. Sharma,Vaibhav., Feb 2014. Green Routing Strategy For Dynamically Arranged Omogeneous Wsn- Msct2, I*nternational Journal Of Computers & Technology*, Vol 12, No. 6.

[14] Heinzelman, W.R. Chandrakasan, A. and Balakrishnan, H., Energy Efficient Communication Protocol forWireless Microsensor Networks. in Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS'00), Jan, 2000, Maui, HI, pp.3005-3014