ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

EFFICIENT & SECURED DATA COLLECTION MECHANISHM USING HYBRID TOPOLOGY FOR WIRELESS SENSOR NETWORKS

Ms.D.Karthika Devi.,B.E.,
PG Student of ME-Applied Electronics,
Jay Shriram Group of Institutions,
Tirupur, TamilNadu, India.
karthikadevid1711@gmail.com

Mrs.S.Menaga.,M.E.,
Assistant Professor of ECE Department,
Jay Shriram Group of Institutions,
Tirupur, TamilNadu, India.
sri.ece09@gmail.com.

Abstract—**Data collection is one of the challenging task in wireless sensor network. Network lifetime, scalability and load balancing are very important requirements during data gathering in sensor network applications. In order to provide an energy efficient data collection in WSN the VELCT was proposed. The Velocity Energy-efficient and Link-aware Cluster-Tree scheme construct the simple data collection tree (DCT) based on the cluster head election. This tree structure reduces the energy consumption of the cluster head and avoids frequent cluster formation. Here is the data collection node (DCN) which simply aggregates the data from the cluster head and delivers it to the sink via DCT. This cluster and tree based approach minimizes the energy exploitation, reduces end-to-end delay and traffic in the network. The VELCT algorithm provides better QoS in terms of energy consumption, throughput, end-to-end delay, and network lifetime for mobility-based WSNs. The data communication over the network is becoming a critical issue due to security problems.In order to provide the security, RSA algorithm is implemented along with VELCT. It consist of encryption and decryption key, both are given to sender and receiver respectively, this technique will provide a secure data communication over the network.Compared to other algorithmsit reduces the network complexity.**

Keywords—**Data Collection, Cluster Head, DCN, DCT, VELCT, Sensor nodes, Security, RSA algorithm.**

I. INTRODUCTION

Data collection is the most important problem in wireless sensor networks. Main goal of data collection is to collect the large amount of data, and to reduce the data loss due to less memory capacity of sensor nodes. Effective data collection techniques can improve the performance of sensor networks. Choosing a right topology helps to enhance the performance, coverage, lifetime of the network and QoS of the network. An efficient topology ensures that neighbors are at a minimal distance and reduces the probability of a packet being lost between sensor nodes. One very important parameter that plays a major role in the performance of WSNs is energy consumption. Energy consumption is directly related to the transmission distance between the sensor nodes. And the security algorithms involves to transfer the collected data to the sink node in a protected medium by involving the keys.

A. Motivation of the Project

The main aim of the project is to gather the data efficiently and securely from each sensor node to the sink through the DCN nodes of each cluster. DCN nodes are nothing but a sensor nodes that does the job of collecting the data from the CH and sends it to the nearby DCN node which forms a tree like structure. a Velocity Energy-efficient and Link-aware Cluster-Tree (VELCT) scheme is proposed here for data collection in WSNs, which would effectively alleviate the problems of coverage area, motion, interruption, traffic, tree intensity, and end-to-end connection. The VELCT builds the Data Collection Tree (DCT) depending on the cluster head location. The DCN in DCT collects the data from the CH and forwards it to the sink, and also senses the data within its range. The proposed VELCT design minimizes the energy misuse, end-to-end delay and traffic in CH by constructing the DCT in WSNs. Where the asymmetric key algorithm is used to give the secure transmission and reception by the encryption and decryption methods.

B. Data Collection in WSN

Data collection methods in wireless sensor network are classified into three groups. They are Data collection using mobile sensor nodes, data collection using static sink approach and data collection using mobility based approach. The third one is again classified into two groups, they are data collection using single mobile sink and data collection using multiple mobile agents. Multiple mobile agents are again classified into two categories, which are constrained path and uncontrollable path. Memorycapability of Sensor node and energy efficiency are the major challenges in data collection of wireless sensor

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

networks. The major issues of WSN are discussed in the following.

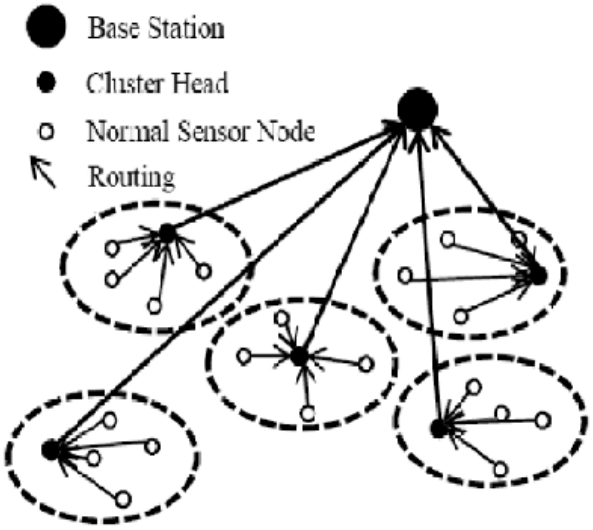


Figure 1 Wireless Sensor Network Architecture

C. Issues in WSNduring Data Collection

Data is sensed from the coverage area within the network, before transmitting it to the sink. Sensors may also generate unwanted data and anenormous amount of data is collected for transmitting by the base station. Which leads to the Data Aggregation. Some of the issues in design of data aggregation include: improving of clustering techniques, unreliability of sensors, improving in-networking aggregation techniques. Main focus is towards energy saving. Other issues are improving security in data transmission, handling tradeoffs, reducing delay, improving quality of service.

D. Security in WSN

Sharing of information over a network is becoming a critical issue because of the security problems. Hence techniques are needed to protect the shared data in an unsecured wireless medium. The present work focus on cryptography to secure the data while transmitting in the network. At First the data which is to be transfer from sender to receiver in the network must be encrypted by using the encrypted algorithm in cryptography .Secondly by using decryption technique the receiver can view the original data. Transmitting data or document can be secured by these ways.

II. LITERATURE REVIEW

Gurpreet Singh Chhabra, Dipesh Sharma says Wireless Sensor Networks (WSNs) can collect the sensed information by hundreds or thousands of sensing nodes and transmit those to the sink. It uses the simplest way that Sensor nodes broadcast the sensed data to sink directly. It is very simple, but it will have a severe problem. When a location of thelongest will spend more energy than the closer one.

Ali Norouzi, Faezeh Sadat Babamir proposed a data collection tree concept is used to find an energy efficient result. Even the best aggregation tree does not distribute the load of data packets to the transmitting nodes moderately while it is consuming the lowest likely energy of the network. Hence it consumes more energy after certain packets transferring completed.

Yong-xian Jin, Feng-zhen Chen described that TBDCS is a tree-based wireless sensor network data collection scheme, it avoids the implosion problem, and minimizes the data transmission times, and also reduces energy consumption. But it lacks in effective trade-off between the delay and the data collection. An improved EEDCP-TB is proposed, which deals with the data distribution for whole network.

Sombir Singh, Sunil K Maakar presents the difference between DES private key based Algorithm and RSA public key basedalgorithm. The main feature that specifies and distinguishone algorithm from another are the capacity to the speed ofencryption and decryption of the input plain text..The encryption execution time anddecryption execution time consumed by DES algorithm and RSA algorithm isequal.

III. PROPOSED METHOD

The methodology proposed for data collection is a hybrid topology, which is the combination of both cluster and tree topologies. Effectiveness of wireless sensor network depends on data collection mechanism. Numerous data collection schemes available such as multipath, chain, tree, cluster and flat topologies. The available data collection schemes failed to provide a guaranteed reliable network in terms of traffic, mobility, and end-to-end connection. Hence the hybrid topology arises to solve the above mentioned problems.

A. Cluster Tree Topology

Cluster Tree Topology is the combinations of cluster and tree topology, then the topology design starts with a special node called DD (Designated Device). The beacon signal contains NetID (IDentity of the Network), CID (Cluster IDentification) and NID (Node IDentification) nodes which are added to the DD. Beacon signal is used to identify the transmission and reception of the connection of sensor nodes.

To overcome the above mentioned protocols limitations of the topologies such as energy consumption, connection time, RSS, throughput, coverage, end-to-end delay and network lifetime, a logical topology for data collection was proposed, which is Velocity Energy-efficient and Link aware Cluster-Tree (VELCT). It is an improved version of CIDT, which

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

alleviates the existing issues in CIDT such as coverage, mobility, traffic, tree intensity and delay of the tree structure.

B. RSA Algorithm

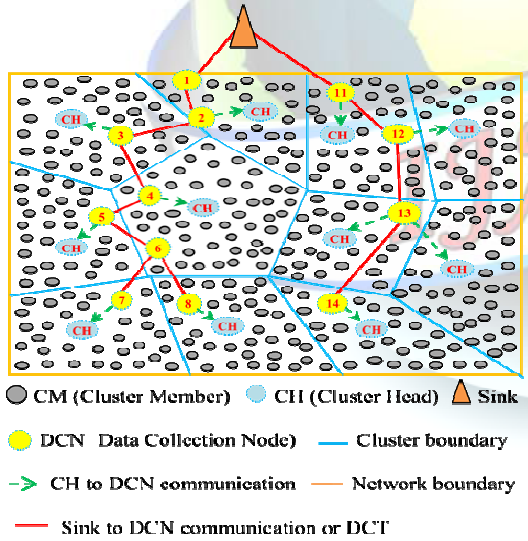
RSA is widely used Public-Key algorithm. RSA algorithm described in 1977. Proposed work consist of RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. RSA algorithm consist of these three steps, Key Generation, Encryption,and Decryption. RSA is an asymmetric key cryptography. It uses different keys for encryption and decryption.

IV. VELCT DESIGN

The VELCT scheme consists of set-up phase and a steady state phase. In the set-up phase, cluster formation and data collection tree construction is introduced. Then, the steady-state phase is started to transfer the data from the cluster members to the destination or sink.

A. Set-Up Phase

Set-up phase does two jobs, one is intra cluster communication and then DCT communication operations. In intra cluster communication a kind of signal is used to find the each sensor location and position in a network. Cluster Head is selected depends on its threshold value.



B. Steady State Phase

Once the set-up phase accomplished, steady-state phase is introduced. In steady-state phase,collected data from cluster members by corresponding Cluster Head is taken into account. Then each CH sends the collected data to the DCN, and it transfers it to the next nearby DCN, which forms like a tree structure which is denoted as DCT. In same way finally it reaches the destination or reaches the sink.

V. RSA ALGORITHM

RSA (named after its authors – Rivest, Shamir and Adleman) is the most popular public key algorithm. RSA uses a pair of keys one for encryption and other for decryption. One of the key is called the private key, it is kept secret and other one is known as public key, which is disclosed. The message or data is encrypted with public key and it can only be decrypted by using the private key. So, the encrypted message cannot be decrypted by anyone who knows the public key and thus secure communication is established. Figure 3 represents the RSA encryption and decryption.

Complexity of the RSA decreased when compared to the DES and AES algorithms. And still the RSA algorithm used in real world applications like banking transactions.It generates the multiple key as one time passwords. Hence we can achieve efficient way of encryption.

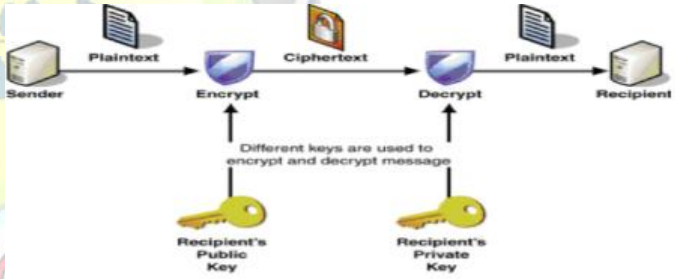


Figure 3 RSA Communication

VI. RESULT AND DISCUSSION

In this work, performance of the sensor network with various parameters via simulations were presented. A WSN system including of 227 nodes was used in the simulation set-up. All the nodes were randomly positioned in a square region of 500 × 500 m2. The size of data packet is 256 bytes, the transmission limit is set as 100m, and the sensing limit is150m.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

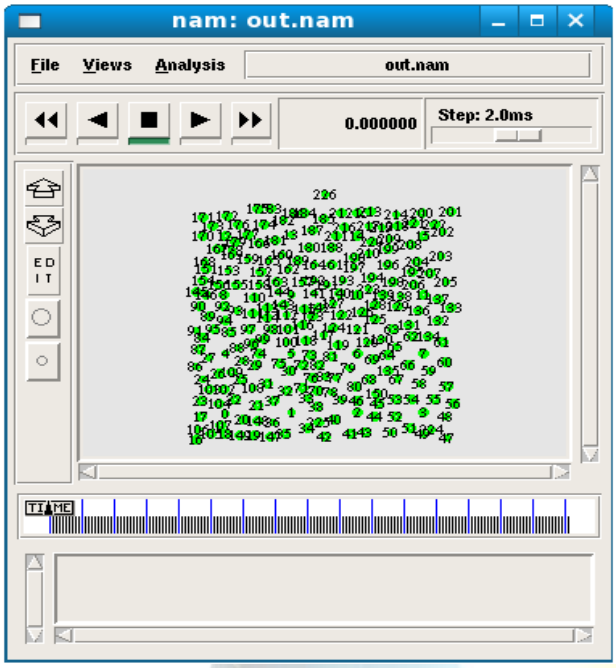


Figure 4 NAM Output before Clustering

Figure 4 shows the simulation output of the NAM window with sensor nodes of 227. All the nodes are deployed in a random manner within the network.

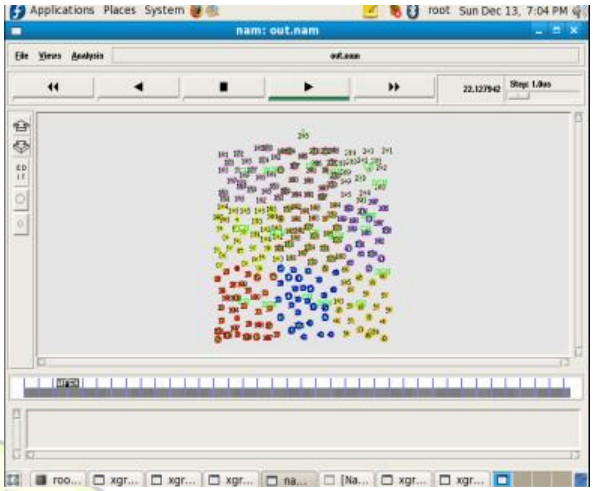


Figure 5 NAM Output after Clustering

Figure 5 shows the NAM output with clustering. Different colors show the different cluster regions. DCN and CH nodes are identified by its name shown in top of the node.226th node is considered as sink node for the given network.

Figure 6 shows the sensor node communication with corresponding cluster head of each cluster in random manner. Each of the circle is a communication of sensor nodes. Traffic of the sensor network is controlled by clustering. Communication takes place by set-up and steady state phases. First CH receives data from each nodes. This process is shown in above figure.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

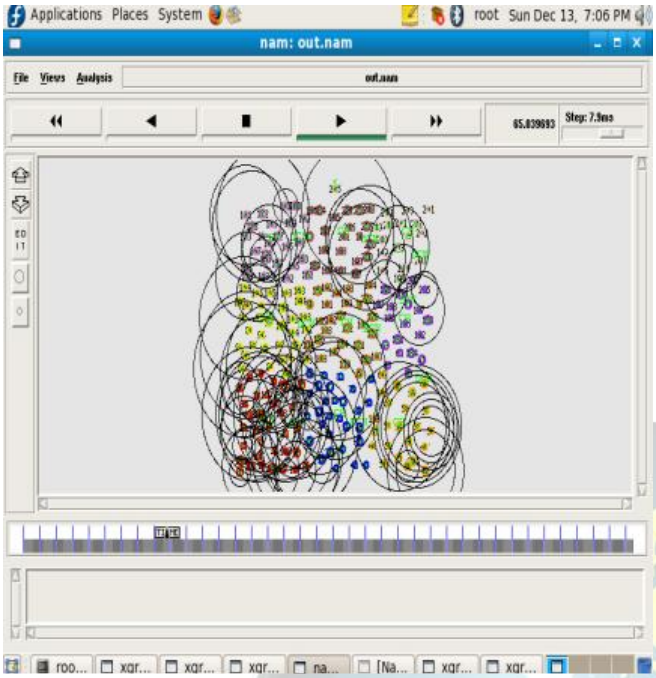


Figure 6 NAM Output with Communication

Figure 7 VELCT is able to achieve better performance in terms of PDR. VELCT is able to provide considerably stable links than other existing algorithms. This is because the VELCT offers stable links with the clustering, cluster head selection operation. Therefore stable links with RSS and maximum connection time is obtained.

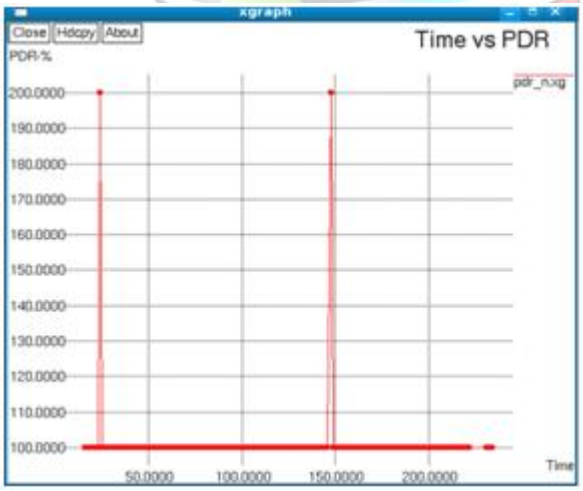


Figure 7 Time versus Packet Delivery Ratio

The time variations shown in the figure implies the packet delayed in the network (the packet delay is shown on figure 10), which is received with the next packet, hence the PDR reaches high at a point of time.

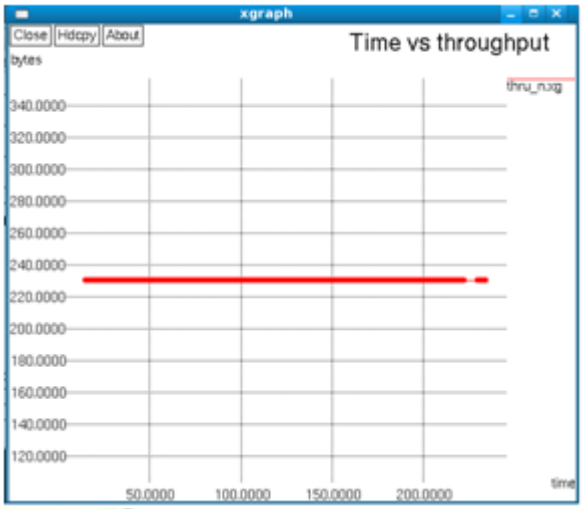


Figure 8Time versus Throughput

Figure 8clearly indicate that the VELCT algorithm is able to achieve better throughput than the existing schemes. This is because of two features. First, traffic load is reduced by clustering in interand intra cluster communication. Second, unwanted packet flooding is avoided, hence the DCT can offer an optimal path from node to sink. For every round of communication number of sensor nodes in each cluster is maintained. Stable throughput is obtained and the difference in the figure shows the time taken to start communication with sink.

In Figure 9 the VELCT selects the cluster head with better threshold value, connection time, RSSI and minimum control packets overhead. Here, each cluster head in a network is selected with the maximum energy, coverage distance and less mobility with corresponding cluster members. This is because the VELCT selects the CH with better threshold value and above mentioned features which helps to reduce the control packet overhead and RSSI is also maintained.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

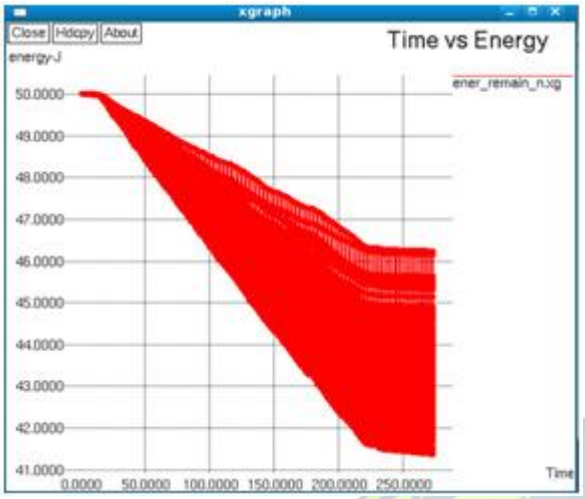


Figure 9 Time versus Total Energy

At the beginning of the aggregation the energy of the network is at high level. When the process starts then the energy level also leads to deplete. The linear decrease shows the energy taken to reach the sink.

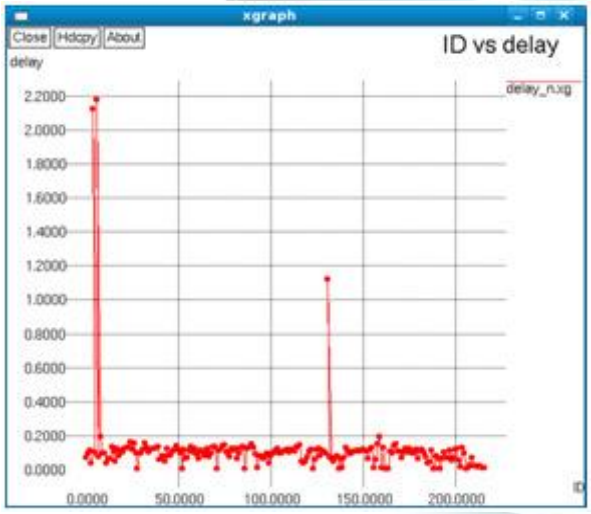


Figure 10 ID versus Delay

Figure 10shows the performance of delay with respect to packet ID. Here, we have selected 227 sensor nodes to examine the performance of delay over the network with packet ID. This is because the VELCT offers the shortest path. It reduces the packet drop ratio and retransmissions of packet over the network.

From the simulation results, it can be noted that the VELCT protocol provides a stable link and adopted itself to high mobility. It is observed that the proposed VELCT protocol can save the sensor node residual energy, and extends the reliability and lifetime of the network. Also, it is adaptable to high mobility environment and provides a better quality communication over the network.

Figure 11 encrypted and decrypted values

Figure 11 consist of encrypted and decrypted values according to the RSA algorithm. It can be viewed from the terminal window. The data's are encrypted by the sender and decrypted by the receiver according to the public and private keys.

VII. CONCLUSION

In this work the data aggregation is achieved by the hybrid topology called Cluster-Tree topology. Each cluster member chooses the cluster head with better connection time and forwards the data packets to the corresponding cluster head in an allocated time slot. Each Data Collection Node (DCN) collects the data packets from its CH .Then each DCN is connected to sink via nearby DCN node. From the simulation results, it is revealed that VELCT provides more stable links, better throughput, energy utilization and PDR with reduced network traffic. The data may lost during the transmission or reception. To avoid that we have worked with RSA cryptography algorithm. It gives the reliable result in encryption and decryption. Complexity increases when we go for higher bits. For end to end communication RSA algorithm is most suitable.Future work is based on attacks.

REFRENCES

[1] Velmani. R and Kaarthick. B (2015), 'An Efficient Cluster-Tree Based Data Collection Scheme for Large Mobile Wireless Sensor Networks', IEEE Sensors Journal, Volume 15, NO. 4.

[2] JenishVarshini.K. andPriya.L.R. (2015), 'Performance Analysis Of Heterogeneous Wireless Sensor Networs

With Cluster Tree Based Routing For Mobile Nodes', International Journal of Advanced Research Trends in Engineering and Technology, Volume II, Special Issue XXV

[3] AnkitTripathi and Sanjeev Gupta (2014),'Survey on Data Aggregation Techniques for Wireless Sensor Networks', International Journal of Advanced Research in Computer and Communication Engineering Volume 3, Issue 7

[4] Velmani.R. and Kaarthick.B. (2014), 'An Energy Efficient Data Gathering in Dense Mobile Wireless Sensor Networks', ISRN Sensor Networks Volume 2014, Article ID 518268

[5] Neethu M. Nair and Felix ArokyaJose.A. (2013),'Survey on Data Collection Methods in Wireless Sensor Networks', International Journal of Engineering Research & Technology (IJERT) Volume 2 Issue 12

[6] Sitender Kumar and Rohitkumarvishwkarma (2013),'A Survey on Routing Protocol for Wireless Sensor Network',(IJARCET)Volume 2, Issue 2

[7] B. Padmavathi, S. Ranjitha Kumari (2013), 'A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique',International Journal of Science and Research (IJSR)Volume 2,Issue4

[8] Sombir Singh, Sunil K Maakar(2013), 'A Performance Analysis of DES and RSA Cryptography',International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)Volume 2, Issue 3

[9] M. Preetha, M. Nithya (2013), 'A Study and Performance Analysis of RSA Algorithm',International Journal of Computer Science and Mobile Computing (IJCSMC), Volume 2, Issue. 6