International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

SECURE DATA TRANSMISSION IN HYBRID COMPRESSIVE SENSING BASED WSN

Richa Singh[1], Deepika Gupta[2]

[1]*Computer Science and Engineering, Dr. K.N.*
Modi Institute of Engineering and Technology(India)
[2]*Computer Science and Engineering,*
Meerut Institute of Engineering and Technology (India)

ABSTRACT

Wireless Sensor Network (WSN) consists of large number of sensor nodes that are characterised by limited processing power and computation capability. These sensor nodes have the capabilities of information sensing, data processing while communicating with other nodes in the network. So, it is desirable to design simple and energy-efficient data gathering (or aggregation) method to reduce data transmission consumption of each sensor and to balance the traffic load throughout network. In this paper, we use a hybrid compressive sensing (CS) method which is applied to the clusters of sensor nodes. The information on locations and distribution of sensor nodes is used to design the data collection method in cluster structure. Sensor nodes are organized into clusters. Within a cluster, data are collected at the cluster heads by shortest path routing then at the cluster head, data are compressed to the projections using the CS technique. The projections are forwarded to the sink following a backbone tree. And then security is also added to this system for secure transmission so that only valid data is to be transmitted to the sink node. Finally, we will simulate the improved version of CS technique using Network Simulator (NS-2) in terms of the number of transmissions and end to end delay.

Keywords: WSN, Clustering protocol, Cluster head, compressive sensing, secure transmission

I. INTRODUCTION

A Wireless Sensor Network (WSN) contains hundreds or thousands of sensor nodes and a base station (BS) or sink node. These sensor nodes have limited energy power. Usually, the base station is not resource-constrained and might on a far distance from the area that is monitored. These sensor nodes are integrated with sensing, processing and wireless communication capabilities [12]. The main task of a sensor node is to sense and collect data from a certain domain, process them and transmit it to the sink where the application lies as shown in fig.1.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

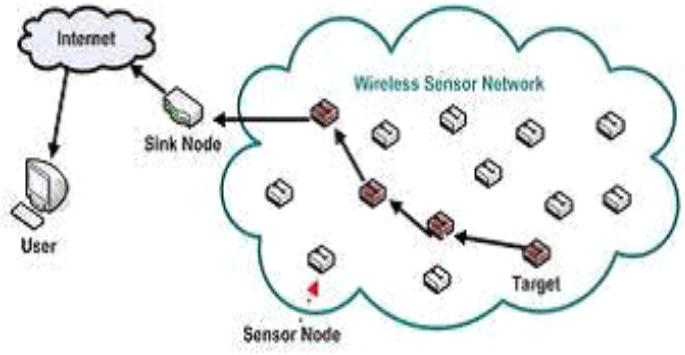

Fig.1 Wireless sensor network

Each sensor node has several parts: a sensing unit, a processing unit, a communication unit, a power unit. With the help of radio communication range, a sensor node transmits the data to base station or sink node through multi-hop path. WSN can be categorized into two types: unstructured WSN and structured WSN. In unstructured WSN, sensor nodes are densely deployed in ad-hoc manner in the sensing region. While in structured WSN, sensor nodes are deployed in a pre-planned manner. So, the maintenance of structured WSN is much easy as compare to unstructured WSN [1].

A WSN may be used in the variety of everyday life activities or services such as military target tracking and surveillance, natural disaster relief, hazardous environment exploration, seismic sensing, etc. In military target tracking and surveillance, a WSN can assist in intrusion detection and identification. Specific examples include spatially-correlated and coordinated troop and tank movements. With natural disasters, sensor nodes can sense and detect the environment to forecast disasters before they occur. In biomedical applications, surgical implants of sensors can help to monitor a patient's health. For seismic sensing, ad hoc deployment of sensors along the volcanic area can detect the development of earthquakes and eruptions. Along with the various applications there are some limitations of WSN such as- power restriction**,** limited computation power of sensor nodes**,** storage restriction**, r**andom topology**,** hostile environment, limited support for networking, etc.

Some features that make the sensor network different from other wireless and traditional networks are [2]: hardware bottleneck including size's restrictions, power supplier, process power and capacity, memory; high density of node's distributions in operation region; failure talent of the nodes; dynamic and periodic topological changes; using the broadcast communication instead of peer to peer method; data oriented network (The nodes don't have any identification code).

Compressive sensing is one of the emerging technologies that open the frontiers for data collection in sensor network. CS techniques are used for various purposes such as data acquisition or data gathering, data transmission [6].It has a surprising property that one can recover sparse signals from far fewer samples than is predicted by the Nyquist–Shannon sampling theorem. In the conventional paradigm, natural signals are first acquired at Nyquist- Shannon sampling rate, and then compressed for efficient storage or transmission [7]. CS shift this paradigm by combining the sampling and compression into one step by measuring samples that contain

the maximum information about the signal, this eliminates the need to acquire and store large number of samples only and drop the minimal values.

Rest of the paper is organized in the following manner- Section II presents routing protocols for WSN. Section III presents the technical architecture of system, section IV presents the problem description and solution. Section V include the system methodology and section VI include the simulation and evaluation of system and finally, section VII concludes this paper.

II. ROUTING PROTOCOLS

One of the critical technologies in WSN is routing.A routing protocol is a way of determining a path between a source node (i.e., a sensor node) and a destination (i.e., sink node) for sensed data transmission [3]. Routing in WSN is very challenging and time consuming due to the inherent characteristics of this network which differ this network from other networks such as mobile ad hoc networks or cellular networks [4].

Routing protocols in WSN are classified into two major categories as shown in table 1: Protocol Operation and Network Structure.

Based on protocol operation, routing protocols are classified into following categories: Negotiation based routing, Multipath based routing, Query based routing, QOS based routing and Coherent based routing.

Based on Network structure, routing protocols are classified into three categories: flat-based routing, location-based routing and hierarchical or clustering-based routing [14].

Table 1: Classification of Routing Protocols

Routing Protocols in WSNs	
Protocol Operation	Network Structure
• Negotiation based routing • Multipath based routing • Query based routing • QOS based routing • Coherent based routing	• Flat based routing • Hierarchical or clustering based routing • Location based routing

Clustering is one of the efficient protocols used to extend the lifetime of network. In clustering routing protocol, sensor network is divided into number of clusters. Each of these cluster have three types of nodes: ordinary nodes, cluster head (CH) and a base station or sink node. Ordinary nodes are responsible for sensing information and transmit that sensed information to their respective cluster head. Cluster head of each cluster are responsible for data aggregation and reduction and then transmit that aggregated data to base station.

Clustering routing is becoming an active branch of routing technology in WSN due to its number of advantages [5] such as: i) it reduces the size of the routing table by localizing the route setup within the cluster; ii) no topology overhead; iii) it helps in conserving communication bandwidth; iv) lifetime of network is increased.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

III. TECHNICAL ARCHITECTURE AND IMPLEMENTATION

The architecture of this system as shown in fig.2 shows that the sensor field is divided into certain number of clusters and each cluster has its own cluster head. Cluster member transmits the data without using CS to CHs. Data aggregation is performed at the CHs and CS technique is applied to aggregated data and then CHs add the signature to the aggregate data. At the sink signature is verified and then the valid data is transmitted to sink.

The main objective of this paper is to reduce the number of transmission in wireless senor network so that the network lifetime is enhanced; minimum energy consumption at each sensor node; reduce end to end delay and secure transmission.

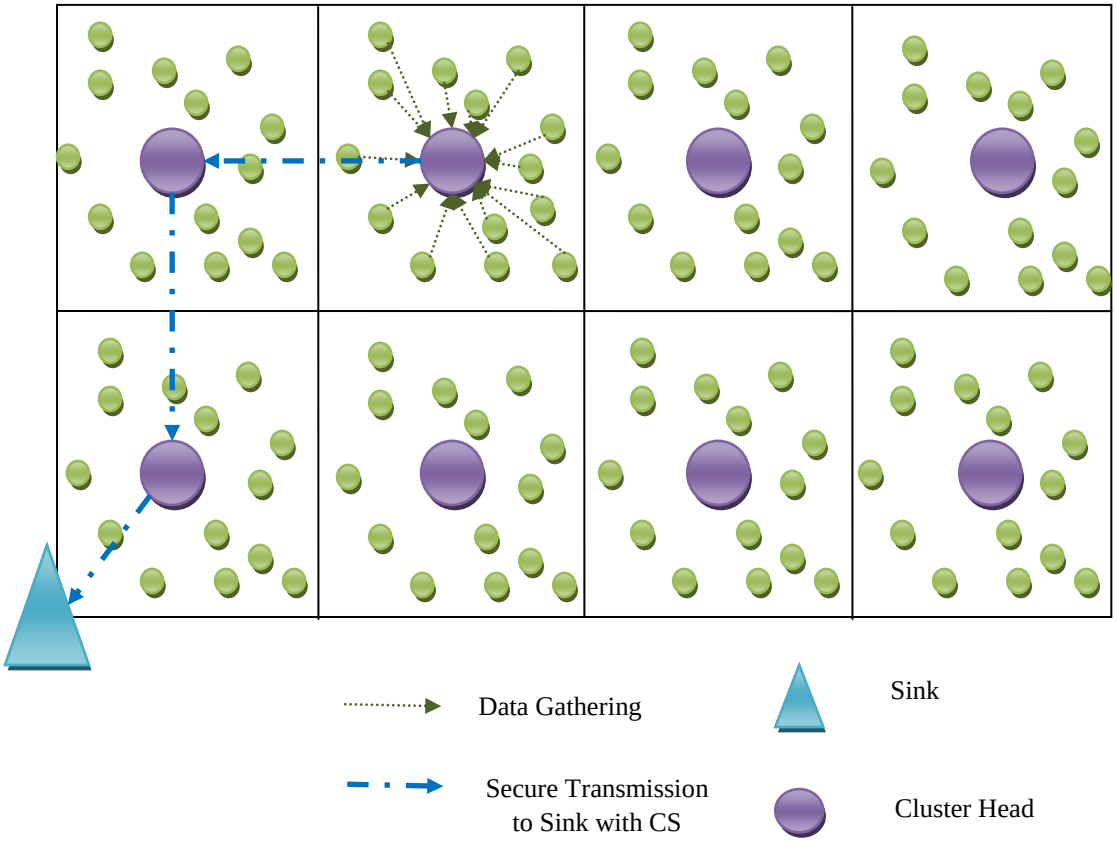

Fig.2 System Architecture

IV. PROBLEM DESCRIPTION AND SOLUTION

In the previous work, the sensor field is divided into certain number of clusters and each cluster has its own cluster head. Within a cluster, each cluster member transmits data to the cluster head (CH) without using CS and data aggregation is performed at the CH [9]. Then CHs transmit the aggregated data to sink. In this works security is not considered and this technique reduces the number of transmissions but still there is a need to reduce the transmission number

In this paper, we first propose a clustering method that uses the hybrid CS for sensor networks. The sensor nodes are organized into clusters. Within a cluster, nodes transmit data to the cluster head (CH) without using CS. A data gathering tree spanning all CHs is constructed to transmit data to the sink by using the CS method.
Then we propose an elliptic curve digital signature algorithm to provide security. In this, the cluster head add the signature with the collected information from its members. At the sink the signature is verified using the same algorithm.

V. SYSTEM METHODOLOGY

5.1 Cluster head election

Given the geographic location of the central point of a cluster-area, the sensor node that is the closest to the central point will become the CH.Since the sensor nodes do not know who is the closest to the central point of a cluster area, and we do not know if there is a sensor node falling into the close range of the central point, we let all nodes within the range of Hr from the centre be the CH candidates of the cluster, where r is the transmission range of sensors. The value of H is determined such that there is at least one node within H hops from the central point of a cluster. To elect the CH, each candidate broadcasts a CH election message that contains its identifier, its location and the identifier of its cluster.
The CH election message is propagated not more than 2H hops. After a timeout, the candidate that has the smallest distance to the centre of the cluster among the other candidates becomes the CH of the cluster. In the extreme case that no sensor node falls within H hops from the central point so that there is no CH for this cluster-area, the nodes in this cluster area accept the invitation from neighbouring CHs and become members of other clusters. Thus, no node will be left out of the network.

5.2 Sensor Node Clustering

After a CH is elected, the CH broadcasts an advertisement message to other sensor nodes in the sensor field, to invite the sensor nodes to join its cluster. An advertisement message carries the information: the identifier and location of the CH, and the number of hop that the message has travelled. The hop count is initialized to be 0. When a sensor node receives an advertisement message, if the hop count of message is smaller than that recorded from the same CH, it updates the information in its record including the node of previous hop and the number of hop to the CH, and further broadcasts the message to its neighbour nodes; otherwise, the message is discarded.
After the advertisement of CH is complete, each non-CH node decides which cluster it joins. The decision is based on the number of hops to each CH. The routing from a sensor node to its CH follows the reverse path in forwarding the advertisement message.

5.3 Data aggregation with compressive sensing

In this module, within a cluster, each sensor node transmits its data to its designated CH via the shortest path. The routes that sensor nodes use to send their data to the CH form a shortest path tree in each cluster. The total number of intra cluster transmissions is the sum of the distance of all sensor nodes to their CHs. The distance between two nodes is defined as the number of hops of the shortest path between them. Data collected from sensor nodes is compressed by the CS method at the CHs. The data projections generated at each CH are forwarded to the sink in M rounds along the backbone tree.

At each CH in the backbone tree, it aggregates its own data projection with the projections received from other CHs by using the CS method and forwards the aggregated projection upward toward the sink along the tree. There are usually multi hops between two CHs.

5.4 Secure Transmission Module

Security is one the important concern in WSN. We implement Elliptic curve Digital signature algorithm to provide security. The cluster head add the signature with the collected information from its members. At the sink, the signature is verified using the same algorithm. If it is valid, the sink accepts the data or otherwise the sink rejects the data and keeps away the malicious node from the network. Other cluster head also never communicate through the malicious list.

5.4.1 Algorithm Detail

The Elliptic Curve Digital Signature Algorithm (ECDSA) [8] [13] is a variant of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography. As with elliptic curve cryptography in general the bit size of the public key believed to be needed for ECDSA is about twice the size of the security level in bits. By comparison in the security level of 80 bits meaning an attacker requires the equivalent of about 2^{80} signature generations to find the private key the size of a DSA public key is at least 1024 bits whereas the size of an ECDSA public key would be 160 bits. On the other hand, the signature size is the same for both DSA and ECDSA: 4*t* bits, where *t* is the security level measured in bits that are about 320 bits for a security level of 80 bits. Suppose Alice wants to send a signed message to Bob. Initially the curve parameters (CURVE, G, n) must be agreed upon. In addition to the field and equation of the curve we need G a base point of prime order on the curve; *n* is the multiplicative order of the point G. Alice creates a key pair, consisting of a private key integer d_A randomly selected in the interval [1, *n*-1] and a public key curve point $Q_A = d_A*G$. We use * to denote elliptic curve point multiplication by a scalar.

For Alice to sign a message *m* follows these steps:

- Calculate *e*=HASH (*m*), where HASH is a cryptographic hash function, such as SHA-1.
- Let *Z* be the L_n leftmost bits of *e*, where L_n is the bit length of the group order *n*.
- Select a random integer *k* from [1, *n*-1].
- Calculate the curve point(x_1, y1) = *k***G*.

- Calculate $r=x_1 \pmod n$. If $r=0$, go back to step 3.
- Calculate $s=k^{-1}(Z+rd_A) \pmod n$. If $s=0$, go back to step 3.
- The signature is the pair(r, s).

5.5 Performance evaluation

All sensor nodes are randomly scattered with a uniform distribution. Randomly select one of the deployed nodes as the source node. The location of the sink is randomly determined.

We evaluate our proposed method with respect to the following metrics: PDR, E2E latency.

- **No. of transmission:**is the number of report messages the sink receives from all the cluster head nodes.
- **End to end latency:** It refers to the time taken for a packet to be transmitted across a network from source to sink node.

These parameter values are recorded in the trace file during the simulation by using record procedure. The recorded details are stored in the trace file. The trace file is executed by using the Xgraph to get graph as the output

VI. SIMULATION AND EVALUATION

NS2 simulator is used to evaluate our proposed method with respect to the following metrics: Number of transmission, which is the number of report messages the sink receives from all the cluster head nodes and end to end latency, it refers to the time taken for a packet to be transmitted across a network from source to sink node. These parameter values are recorded in the trace file during the simulation by using record procedure. The recorded details are stored in the trace file. The trace file is executed by using the Xgraph to get graph as the output. The network simulations are implemented using NS2 simulation tool. In this senario, clustering without hybrid CS, clustering with hybrid CS and clustering with secure hybrid CS are evaluated based on the above two performance metrics which are: Number of Transmission and End to End Delay. Table2. shows the parameters used to simulate the environment.

Table 2. Simulation Parameter

Parameters	Values
Simulator	NS2.28
Simulation time	20.
Simulation area	900 X 600
MAC Protocol	802.11
Number of Nodes	55
Radio Propogation Model	TwoRay Ground
Routing Protocol	DSR

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

6.1. End-to-End Delay

The term end-to-end delay refers to the time taken by a packet to be transmitted across a network from source node to destination node that includes all possible delays caused during route discovery latency, retransmission delays at the MAC, propagation and transfer times. Result in fig.3. Shows that end to end delay is further reduced when security is added to the clustering with hybrid CS because only valid data is transmitted to sink node, as compared to the clustering with hybrid CS and clustering without hybrid CS.

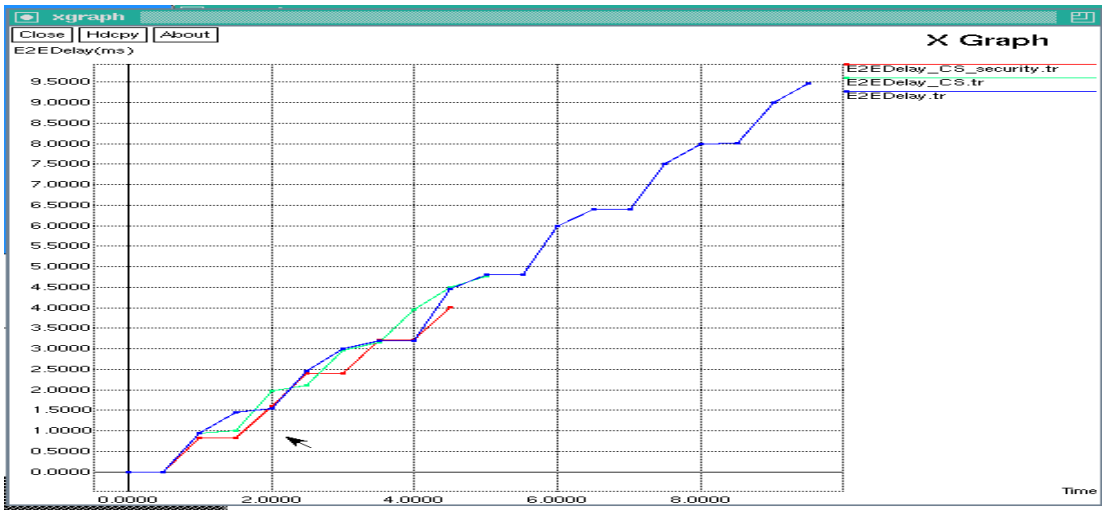

Fig.3 End to end delay vs Time

6.2 . Number of Transmission

The term number of transmission refers to the number of report messages the sink node receives from all the cluster head nodes. The number of transmissions are further reduced when security is added to the clustering with hybrid CS because only valid data is transmitted to sink node, as compared to the clustering with hybrid CS and clustering without hybrid CS. Result is shown in fig. 4

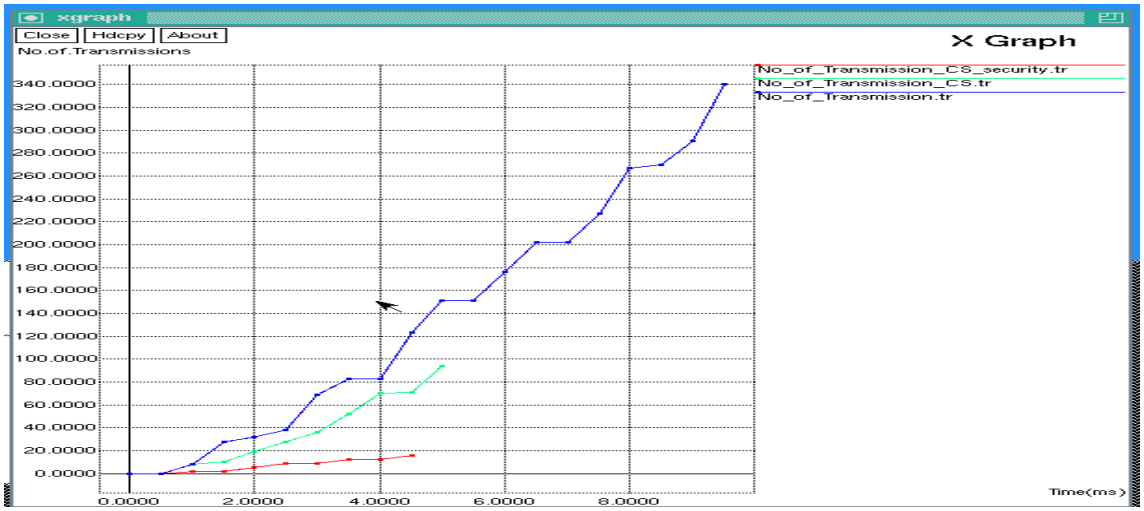

Fig. 4 Number of Transmission vs Time

VII. CONCLUSION

In this paper, we used hybrid CS to design a clustering-based data collection method, to reduce the data transmissions in wireless sensor networks. The information on locations and distribution of sensor nodes is used to design the data collection method in cluster structure. Sensor nodes are organized into clusters. Within a cluster, data are collected to the cluster heads by shortest path routing; at the cluster head, data are compressed to the projections using the CS technique. The projections are forwarded to the sink following a backbone tree. Then security is also added to this system for secure transmission, which further reduces the number of transmissions and end to end delay as only valid data is transmitted to the sink node. This proposed work mainly focuses on reducing the number of data transmissions by using the hybrid compressive sensing to the clusters of sensor nodes. The Proposed method is evaluated by considering two metrics: number of transmission and end to end latency

REFERENCES

[1] N. Sharma1 and A. Nayyar2, "A Comprehensive Review of Cluster Based Energy Efficient Routing Protocols for Wireless Sensor Networks" *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, Volume 3, Issue 1, January 2014.

[2] A.G. Delavar, S. Shamsi, N. Mirkazemi, J. Artin, "SLGC: A New Cluster Routing Algorithm In Wireless Sensor Network For Decrease Energy Consumption," *International Journal of Computer Science, Engineering and Applications (IJCSEA)* Vol.2, No.3, June 2012.

[3] H. Lee, M Jang, and J.W Chang, "A New Energy-Efficient Cluster-Based Routing Protocol Using a Representative Path in Wireless Sensor Networks", *International Journal of Distributed Sensor Networks*, Volume 2014.

[4] R.K. Yadav, R. Singh and D. Gupta, "Clustering Routing Protocol in Wireless Sensor Networks: A Review" in the Proceedings of the *International Conference on Futuristic Trends in Computational Analysis and Knowledge Management*, Feb. 2015.

[5] V. Katiyar, N. Chand and S. Soni, "Clustering Algorithms for Heterogeneous Wireless Sensor Network: A Survey", *InternationalJournal of Applied Engineering Research*, Dindigul Vol.1, No 2, 2010.

[6]R. Singh, R. K. Yadav, D. Gupta, "Compressive Sensing In WSNS: A Review", *International Journal of Engineering Research & Management Technology*, March- 2015 Volume 2, Issue-2.

[7] C. Luo F. Wu, J. Sun, C.W. Chen, "Efficient Measurement Generation and Pervasive Sparsity for Compressive Data Gathering", *IEEE Transactions On Wireless Communications*, VOL. 9, NO. 12, DECEMBER 2010.

[8] H. Zhong, R. Zhao, J. Cui, X. Jiang and J. Gao,"An Improved ECDSA Scheme for Wireless Sensor Network", *International Journal of Future Generation Communication and Networking*, Vol. 9, No. 2 (2016).

[9] R. Xie and X. Jia,"Transmission-Efficient Clustering Method for Wireless Sensor Networks Using Compressive Sensing",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 3, MARCH 2014.

[10] B. Ameena, Prof. M. Biradar,"The Hybrid Compressive Sensing Data Collection Method in Cluster Structure for Efficient Data Transmission in WSN",*International Journal of Science and Research (IJSR),*Volume 4 Issue 6, June 2015.

[11] J. Dhillon , K. Prasad , R. Kumar, A. Gill,"Secure Data in Wireless Sensor NetworkBy Using DES", *International Journal of Wireless & Mobile Networks (IJWMN)* Vol. 3, No. 3, June 2011.

[12] S. K. Gupta, P. Sinha,"Overview of Wireless Sensor Network: A Survey", *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 3, Issue 1, January 2014.

[13] B. R. Tapas Bapu and L. C. Siddanna Gowd, "Security over the Wireless Sensor Network and Node Authentication using ECCDSA" *Indian Journal of Science and Technology*, Vol 9(39), DOI: 10.17485/ijst/2016/v9i39/99397, October 2016.

[14] N. Sharma and A. Nayyar, "A Comprehensive Review of Cluster BasedEnergy Efficient Routing Protocols forWireless Sensor Networks", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, Volume 3, Issue 1, January 2014.