International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 6 Issue 7, July-2017, Impact Factor: 4.059

Review Paper on Zone Adaptive Virtual Coordinate Selection Approach for WSN Optimization

Parmila Kumari[1], Ms. Pooja Dhankhar[2]

[1]M. Tech. Scholar CBS Group of Institution, Jhajjar, Haryana, India
[2]Asst. Professor, CBS Group of Institution, Jhajjar, Haryana, India

ABSTRACT

There are different mediums of performing the communication over the network. Wireless networks give the concept of distributed architecture so that the sharing of information as well as resources can be done effectively. While performing the communication in such network there is the requirement of more effective information sharing techniques. The main application area for sensor network is in the military field or the battle field to provide the survivability. To survive in such critical conditions with war fighters, there is the requirement of some communication medium that is not fixed and does not required any extra infrastructure. This kind of conditions also needs to transmit different kind of data such as text, images, videos etc. A sensor network provides all these facilities and allows to perform the voice communication as well as to communicate effectively under such complicated situations. These kinds of network also provide the area tracking and action tracking so that the monitoring of the war equipment's and the soldiers can be done effectively. This review paper contains the information about the sensor networks and the characteristics of the sensor network, different kind of ad-hoc networks, different sensor network architectures in different real time scenarios. It also includes the discussion about different network properties.

Keywords: Wireless Sensor Networks, Nodes, Cluster, Ad-Hoc Networks, MANET, Zone Adaptive Approach.

I. INTRODUCTION

In last few years, different kind of ad-hoc networks come into the existence. With the advancement of internet and the growth of personal computers, the use of sensor networks are been increased very fast. These kinds of information transmission include the static and dynamic network types and to define the bidirectional links between the system without defining any wired connection as well as without setting up a static infrastructure. These kinds of network do not require any administrative intervention. These networks are called ad-hoc network. A sensor network [1] is defined as a wide public area network in which number of sensor node are connected. Mobility is the key property of such kind of network. A sensor node is made up of four basic components as shown in Figure 1: a sensing unit, a processing unit, a transceiver unit and a power unit. They may also have application dependent additional components such as a location finding system, a power generator and a mobilizer.

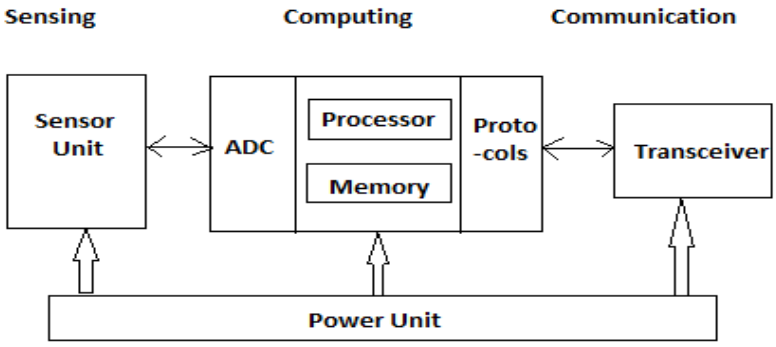

Figure 1: Components of Sensor Node

Sensing units are usually composed of two subunits: sensors and analog to digital converters (ADCs). The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC, and then fed into the processing unit. The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. One of the most important components of a sensor node is the power unit. Power units may be supported by a power scavenging unit such as solar cells. There are also other subunits, which are application dependent. Most of the sensor network routing techniques and sensing tasks require the knowledge of location with high accuracy. Thus, it is common that a sensor node has a location finding system. A mobilize may sometimes be needed to move sensor nodes when it is required to carry out the assigned tasks. All of these subunits may need to fit into a matchbox-sized module.

Here figure 2 is showing the example of a standard sensor network [2]. The network is equipped with different kind of communicating devices. There are different definitions of an ad-hoc network respective to the type of devices as well as the communication devices involved in the system itself. These networks are defined as follows: -

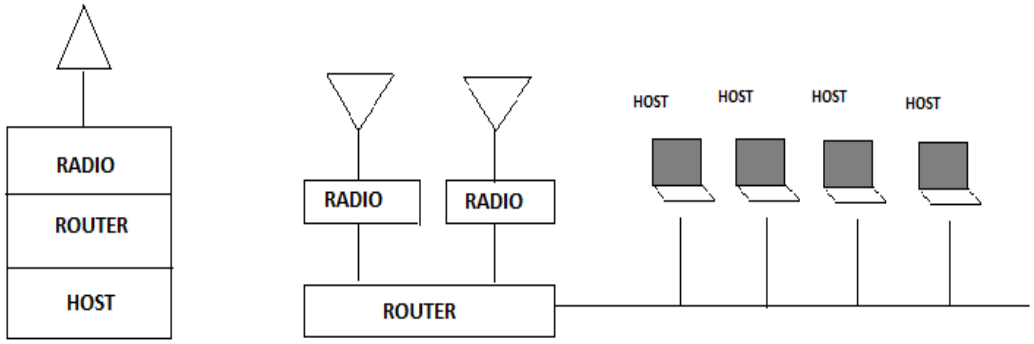

Figure 2: An Example of Sensor Network

A sensor network performs the multi-hop cellular network model that requires the base stations as the main controller points. This network architecture is defined in a P2P network [3]. The decision of next node selection depends on different vectors such as number of packets transmitted in store and forward approach. In such network, a source and destination nodes are specified and the intermediate communicating nodes are selected by the network itself dynamically according to the routing information over the network. The multi-hop communication example is shown in figure 3

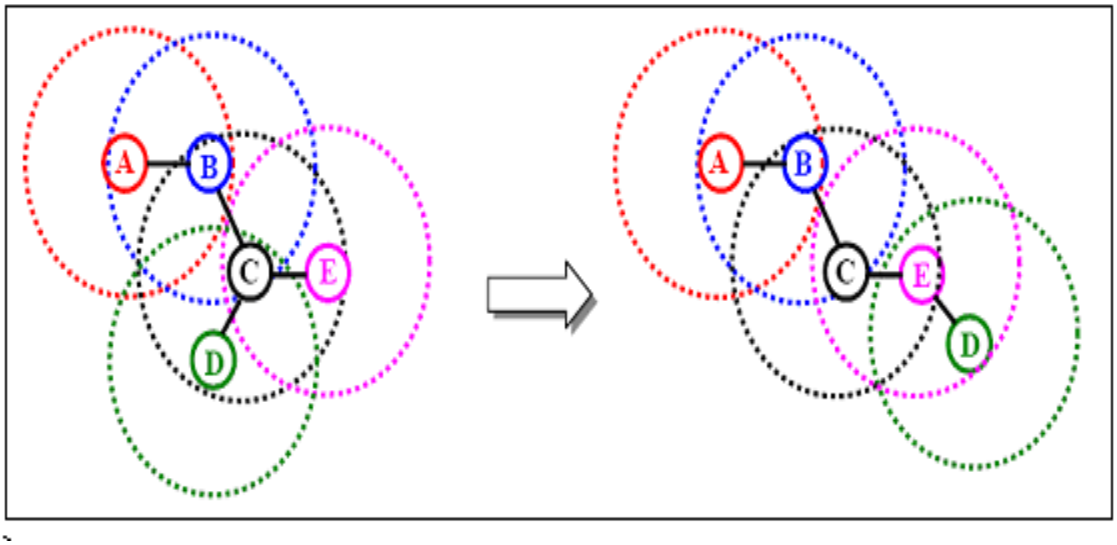

Figure 3: Multi-hop Communication in WSN

The main communicating criteria of WSN are the selection of next node. This can be done in static or dynamic way.

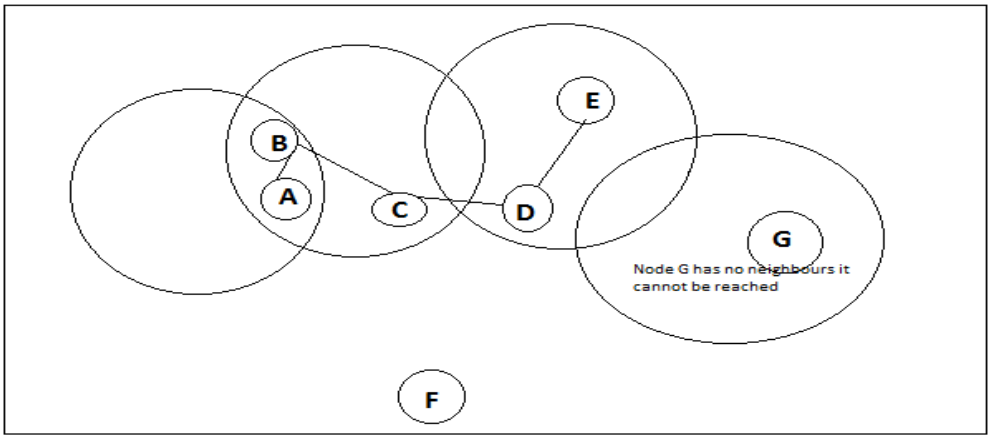

Figure 4: An example of Ad-Hoc Networks

Here in figure 1.4, the route construction in a sensor network is shown. In this network, the circles are showing the coverage of the nodes. Here A is the start node, and it will identify the neighbor nodes in the sequence such as B is selected as the next communicating neighbor node for A, C is selected for Node B. In same way the multi-hop path will be constructed between A and E. Communication cannot be performed to node G, as the node is not in the range of the node.

II. LITERATURE SURVEY

In this section, different routing approaches used by the earlier researchers are shown for any kind of sensor network. Yean-Fu Wen has presented a work to optimize the aggregative routing approach in communication network. Author defined a scheduling mechanism to optimize the routing in clustered network. The analytical decision is here taken under multiple vectors such as capacity analysis, energy analysis and communication. Author has defined the network with some constraints specification. These constraints include the power range and the energy consumption [1].

Yu GU has presented an improved scheduling approach to optimize the routing in communication network. Author defined a static and dynamic clustering approach to define the network architecture. The communication is here based on the sample rate based specification so that the network optimization over the network will be improved. Author identified the aggregative routing with sensing range criteria and generates the optimized route under prioritized constraints [2].

Ahmad and Albhari [3] introduce a new approach for wireless sensor network power management which is based on neural networks. In this new approach an intelligent analysis is used to process the structure of a wireless sensor network (WSN) and produce some information which can be used to improve the performance of WSNs' management application. They applied their intelligent method to their previously proposed management approach which uses the concept of Multi-Agent systems for WSNs' management and observed the improvement of the performance.

Akyildiz [4] describes the concept of sensor networks which has been made viable by the convergence of micro electro mechanical systems technology, wireless communications and digital electronics. First, the sensing tasks and the potential sensor networks applications are explored, and a review of factors influencing the design of sensor networks is provided. Then, the communication architecture for sensor networks is outlined, and the algorithms and protocols developed for each layer in the literature are explored.

Ajay Jangra [5] presented a work on infrastructure driven processing on sensor network optimization. Wireless sensor network (WSN) is an infrastructure less, low cost, dynamic topology, application oriented, multi-hoping network design with small, low power, sensing wireless distributed nods. WSN designing become more complex due to characteristics of deploying nodes, security, authentication and its operation scenario. This paper presents an analytical view on WSN architecture design issues, its objectives and implementation challenges.

Shio Kumar Singh [6] presented a work on different routing protocols present in sensor network. The sensor nodes have a limited transmission range, and their processing and storage capabilities as well as their energy resources are also limited. Routing protocols for wireless sensor networks are responsible for maintaining the routes in the network and have to ensure reliable multi-hop communication under these conditions. In this paper, Author gives a survey of routing protocols for Wireless Sensor Network and compares their strengths and limitations.

Kiran, Kamal and Nitin [7] discussed wireless sensor network is consist a large number of sensor node. And these nodes are resource constraint. That's why lifetime of the network is limited so the various approaches or protocol has been proposed for increasing the lifetime of the wireless sensor network. In this paper they discuss the data aggregation are one of the important techniques for enhancing the life time of the network. And security issues is data integrity with the help of integrity they reduce the compromised sensor source nodes or aggregator nodes from significantly altering the final aggregation value.

Mohamed and William [8] give an energy efficient approach to query processing by implementing new optimization techniques applied to in-network aggregation. They first discuss earlier approaches in sensors data management and highlight their disadvantages and then present their approach and evaluate it through several simulations to prove its efficiency, competence and effectiveness.

Roberto and Pietro [9] present a mechanism for data aggregation in WSN that enforces both confidentiality and integrity of the aggregated data. The proposed mechanism is based on a novel application of peer monitoring and on a delayed aggregation of sensed data. The security of their scheme relies on the concept of additive homo-morphic encryption and on a lightweight key distribution technique. Moreover, their scheme is robust against bogus data injection. Resilience to attacks and to random node failures is also provided.

Young and Yong [10] suggest an inter-connective attestation protocol for a sensor node that is suitable for a wireless sensor network. This protocol is able to earlier detect a node that was damaged by a neighbor node in a sensor network environment without a reliable sensor node. This protocol is for safe authentication for the sensor node. Existing research has focused on interconnectivity authentication for sensor nodes and the BS instead of inter-connective authentication between sensor nodes. Therefore, when a sensor node is captured and viciously modified, and problems result in the network environment, they can be checked.

Jianmin Chen and Jie Wu [11] show some security research in Mobile Ad Hoc Networks (MANETs) and Wireless Sensor Networks (WSNs) is very closely related to cryptography. There are numerous security routing protocols and key management schemes that have been designed based on cryptographic techniques, such as public key infrastructures and identity-based cryptography. Neda. Askari and Hoseini [12] show energy conservation is the most important concern in Wireless Sensor Networks applications which should be considered in all aspects of these networks. Neural Networks as intelligent tools show great compatibility with WSN's characteristics and can be applied in different energy conservation schemes of them.

Huang and Shieh [13] propose a secure encrypted-data aggregation scheme for wireless sensor networks. Their design for data aggregation eliminates redundant sensor readings without using encryption and maintains data secrecy and privacy during transmission. Conventional aggregation functions operate when readings are received in plaintext. If readings are encrypted, aggregation requires decryption creating extra overhead and key management issues. In contrast to conventional schemes, their proposed scheme provides security and privacy, and duplicate instances of original readings will be aggregated into a single packet.

Westh off and Girao [14] show the major threat in WSNs is the presence of an adversary that injects forged data in the network or pretends to be an aggregator. Current mechanisms for authentication are based on complex computations, such as public key cryptography, which are not applicable in WSNs. In most scenarios, an authority issuing shared secrets is not available, as the sensors tend to communicate in a decentralized manner. With the Zero Common Knowledge (ZCK) we provide an authentication protocol that establishes well-defined pair-wise security associations between entities in the absence of a common security infrastructure or pre-shared secrets.

Mohamed Yacoab and Sundaram [15] presented a Compressive Data Aggregation technique which helps to solve the issues of traditional compression techniques. In this technique data is gathered at some intermediate node where size of the data need to be sent is reduced by applying compression technique without losing any knowledge of complete data. XiaoHuaXu [16] presented a work on data aggregation method. Data aggregation is a key functionality for wireless sensor network (WSN) applications. This paper focuses on data aggregation scheduling problem to minimize the latency. They propose an efficient distributed method that produces a collision free schedule for data aggregation in WSNs.

III. CHARACTERISTICS OF SENSOR NETWORKS

The main vector that differentiates a sensor network with any other network type is the used communicating devices called sensor devices. The mobility is the main feature of such networks. Due to the mobility, the special feature points considered

here is the design solution of such kind of network. The issues associated and the characteristics difference between fixed networks and WSN is the sensing nature of the nodes. To control the mobility network and the communication over the network, there is no requirement of any such design issue associated with the network type. The characteristics associated with the work are listed as follows [17]:-

Network Size: The size of a network is defined in terms of network area as well as in the form of network nodes. To coordinate the network under distributed control mechanism, these two vectors are considered. A sensor network can perform a long distance communication up to LOS by using the multi-hop communication. Because of this the network is applicable for rescue areas such as forest etc.

Connectivity: The connectivity is defined in the form of link selection for the next node. To identify the neighbor of a node, the coverage range analysis is done over the nodes. The nodes that come under the coverage area are considered as the connectivity nodes. The bidirectional communication is performed with these networks. The local interference is the factor while considering the connection problem.

Network Topology: Actually, the sensor networks are not dependent on the topology and can provide the output in any topology free networks. The nodes can be placed at random positions in such networks. But in some specific conditions such as in classroom sessions the topology can be setup so that effective throughput will be drawn from the network. The network also subjective to the connectivity type respective to the topology such as centralized connective system or random positioned networks are basic types of such topological architecture.

Bandwidth Constrained Links: Wireless links are defined with lower capacity analysis under the hardwired connections. They are defined under the radio signal so that the long distance communication is possible. The channel bandwidth depends on the signal propagation. This connection can be defined under the bandwidth capacity. While performing the communication the factors included are the link quality analysis and the bit error rate.

Energy Constrained Operation: A sensor network requires some energy to start the communication. To provide this energy, the batteries are attached with sensor devices. The battery backup is the major factor to perform the communication when the sensor device is away from the energy source. As some operation is performed on this sensor device some amount of energy is lost. In the rescue systems, the energy vector is the critical so that more energy backup devices are taken to provide reliable communication.

Security: In a sensor ad-hoc network, the nodes are shared and the information travels among multiple nodes before the final delivery. In such case, it is required for communication to maintain the security so that no intermediate node or any external node captures the communication information. Such kind of network also suffers from different kind of security threats such as DOS attack. As of the public network, sensor network suffer high security risks and having the problem of stolen information and heavy traffic that gives the insecure wireless link over the network.

Autonomous: Another property of the sensor networks is the communication without any centralized administration. The communication over such network is performed by the host and later on controlled by the routers. To perform the distance communication in hybrid networks, the switches and other cross link devices can be used.

Distributed Operation: These kinds of networks does not having any centralized control to perform the network operations. The network is distributed among the terminals. The nodes includes in the network collaborate so that each node can participate over the network and it is able to achieve the secure routing over the network.

Multi-Hop Routing: To enable the infrastructure free communication as well as long distance communication, the multi-hop communication is provided by sensor network. The next hop selection is here done based on the best node election in neighboring nodes. It requires the destination selection while moving through the intermediate nodes so that effective communication will be performed while forwarding through the nodes.

IV. DATA AGGREGATION

In typical wireless sensor networks, sensor nodes are usually resource-constrained and battery-limited. In order to save resources and energy, data must be aggregated to avoid overwhelming amounts of traffic in the network. There has been extensive work on data aggregation schemes in sensor networks, The aim of data aggregation is that eliminates redundant data transmission and enhances the lifetime of energy in wireless sensor network. Data aggregation [18] is the process of one or several sensors then collects the detection result from other sensor. The collected data must be processed by sensor

to reduce transmission burden before they are transmitted to the base station or sink. The wireless sensor network has consisted three types of nodes i.e. Simple regular sensor nodes, aggregator node and querier. Regular sensor nodes sense data packet from the environment and send to the aggregator nodes basically these aggregator nodes collect data from multiple sensor nodes of the network, aggregates the data packet using a some aggregation function like sum, average, count, max min and then sends aggregates result to upper aggregator node or the querier node who generate the query. It can be the base station or sometimes an external user who has permission to interact with the network. Data transmission between sensor nodes, aggregators and the querier consumes lot of energy in wireless sensor network.

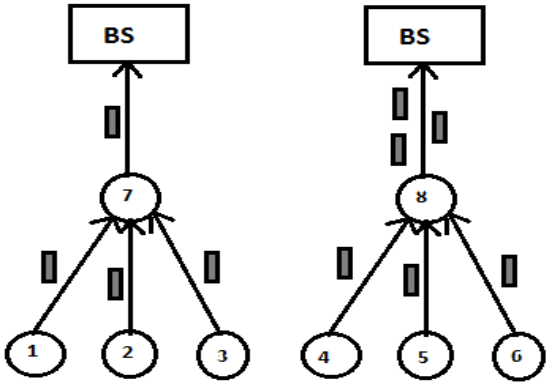

Figure 5: Data Aggregation and Non Aggregation Model

Figure 5 contain two models one is data aggregation model and second is non data aggregation model in which sensor nodes 1, 2, 3,4,5,6 are regular nodes that collecting data packet and reporting them back to the upper nodes where sensor nodes 7,8 are aggregators that perform sensing and aggregating at the same time. In this aggregation model 4 data packet travelled within the network and only one data packet is transmitted to the base station (sink). And other non data aggregation model also 4 data packet travelled within the network and all data packets are sent to the base station(sink), means we can say that with the help of data aggregation process we decrease the number of data packet transmission. And also save energy of the sensor node in the wireless sensor network. With the help of data aggregation we enhance the lifetime of wireless sensor network. Sink have a data packet with energy efficient manner with minimum data latency. So data latency is very important in many applications of wireless sensor network such as environment monitoring, health, monitoring, where the freshness of data is also an important factor. It is critical to develop energy-efficient data-aggregation algorithms so that network lifetime is enhanced. There are several factors which determine the energy efficiency of a sensor network, such as network architecture, the data aggregation mechanism, and the underlying routing protocol. Wireless sensor network has distributed processing of sensor node data. This process also reduces energy consumption or increase life time of the network.

Advantages and Disadvantages of Data Aggregation [19]

Advantage: With the help of data aggregation process we can enhance the robustness and accuracy of information which is obtained by entire network, certain redundancy exists in the data collected from sensor nodes thus data fusion processing is needed to reduce the redundant information. Another advantage is those reduces the traffic load and conserve energy of the sensors.

Disadvantage: The cluster head means data aggregator nodes send fuse these data to the base station. This cluster head or aggregator node may be attacked by malicious attacker. If a cluster head is compromised, then the base station (sink) cannot be ensure the correctness of the aggregate data that has been send to it. Another drawback is existing systems are several copies of the aggregate result may be sent to the base station (sink) by uncompromised nodes .It increase the power consumed at these nodes.

Security Issues in Data Aggregation

There are two type of securities are require for data aggregation in wireless sensor network, confidentiality and integrity. The basic security issue is data confidentiality, it is protecting the sensitive data transmission and passive attacks, like eavesdropping. If we talk about hostile environment so data confidentiality is mainly used because wireless channel is vulnerable to eavesdropping by cryptography method. The security issues is data integrity with the help of integrity we reduce the compromised sensor source nodes or aggregator nodes from significantly altering the final aggregation value.

Sensor node in a sensor network is easily too compromised. Compromised nodes have a capability to modify or discard messages. There are two type of method for securing data hop by hop encryption and end to end encryption, both methods follows some step.

1. Encryption process has to be done by sensing nodes in wireless sensor network.
2. Decryption process has to be done by aggregator nodes.
3. After that aggregator nodes aggregates the result and then encrypt the result again.
4. The sink node gets final aggregated result and decrypts it again.

CONCLUSION & FUTURE SCOPE

In this paper we studied about the sensor networks and the characteristics of the sensor network, different kind of ad-hoc networks, different sensor network architectures in different real time scenarios. We also discussed about different network properties.In typical wireless sensor networks, sensor nodes are usually resource-constrained and battery-limited. In order to save resources and energy, data must be aggregated to avoid overwhelming amounts of traffic in the network.This work can be improved in future under following aspects: a virtual coordinator based zone adaptive model can be defined for improving the communication in sensor network. In this present work, no optimization algorithm is applied and presented to improve the communication but in future some such optimization algorithm can be applied to improve the communication.

REFERENCES

[1]. Yean-Fu Wen, "Energy-Efficient Data Aggregation Routing and Duty-Cycle Scheduling in Cluster-based Sensor Networks", IEEE Conference on Consumer Communication and Networking, pp 95-99, 2007.
[2]. Yu Gu, "Joint Scheduling and Routing for Lifetime Elongation in Surveillance Sensor Networks", IEEE Asia-Pacific Services Computing Conference, pp 81-88, 2007.
[3]. Ahmad Hosseingholizadeh, Dr.AbdolrezaAbhari Department of Computer Science Ryerson University Toronto, Canada: "A neural network approach for Wireless sensor network power management", 2009.
[4]. I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci :" Wireless sensor networks: a survey", Computer Networks 38 (2002) 393–422.
[5]. Ajay Jangra, priyanka, Swati, richa Wireless Sensor Network (WSN): "Architectural Design issues and Challenges", (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 3089-309.
[6]. Shio Kumar Singh1, M P Singh, and D K Singh: "Routing Protocols in Wireless Sensor Networks" –A Survey, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.
[7]. KiranMaraiya, Kamal Kant, Nitin : "Wireless Sensor Network: A Review on Data Aggregation" ,International Journal of Scientific & Engineering Research Volume 2, Issue 4, April -2011 1 ISSN 2229-5518 ,IJSER © 2011.
[8]. Mohamed Watfa, William Daher and Hisham Al Azar : "A Sensor Network Data Aggregation Technique" ,International Journal of Computer Theory and Engineering, Vol. 1, No. 1, April 2009 1793-8201.
[9]. Tamer AbuHmed,"A Dynamic Level-based Secure Data Aggregation in Wireless Sensor Network" Information Security Research Laboratory Graduate School of IT & Telecommunication InHa University.
[10]. Changlei Liu and Guohong Cao, Department of Computer Science & Engineering, The Pennsylvania State University: "Distributed Monitoring and Aggregation in Wireless Sensor Networks", IEEE, March 2010, San Diego, CA.
[11]. SanjeevSetia, Sankardas Roy and SushilJajodia Computer Science Department, George Mason University, Fairfax, VA, USA Center for Secure Information Systems, "Secure Data Aggregation in Wireless Sensor Networks" IEEE Transaction on Information Forensics and Security, VOL. 7, NO. 3, June 2012.
[12]. Neda Enami1, Reza Askari Moghadam1, Kourosh Dadashtabar2 &MojtabaHoseini "Neural Network Based Energy Efficiency In Wireless Sensor Networks: A Survey" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1, August 2010 DOI: 10.5121/ijcses.2010.1104 39.
[13]. Shih-I Huang, "Secure encrypted-data aggregation for wireless sensor networks", IEEE Dec 2007, pp 848-852, Computational Intelligence and Security.
[14]. Dirk Westhoff, "Security Solutions for Wireless Sensor Networks", NEC Technical Journal Vol.1 March 2006.
[15]. M.Y. Mohamed Yacoab,"A Cost Effective Compressive Data Aggregation Technique for Wireless Sensor Networks", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC).
[16]. XiaoHuaXu,"Efficient Data Aggregation in Multi-hop WSNs" National Natural Science Foundation of China, NSF CNS-0832120
[17]. M. Pulido, P. Melin, O. Castillo : "Genetic Optimization of Ensemble Neural Networks for Complex" ,Time Series PredicProceedings of International Joint Conference on Neural Networks, San Jose, California, USA, July 31 – August 5, 2010.
[18]. Frank Yeong-Sung Lin, "A Novel Energy-Efficient MAC Aware Data Aggregation Routing in Wireless Sensor Networks",IEEE International Conference on Communications (ICC),2006, Vol8, ISSN 8164-9547.
[19]. Lei Zhang, "Preserving privacy against external and internal threats in WSN data aggregation", 2 August 2011, DOI 10.1007/s11235-011-9539-8.