A Novel Security Based Data Transmission Protocol For Cluster Based Wireless Sensor Networks

Ch. Mounika
Mtech student ,Dept. of CSE,.
Gudlavalleru Engineering College, Gudlavalleru, India

Ch. Suresh Babu
Associate Professor, Dept of CSE, Gudlavalleru Engineering College, Gudlavalleru , India

Abstract:

Device to device communications in cellular networks are promising frameworks for enhancing network spectrum, throughput and transmission delay. Cooperative network has been used to enhance efficiency and system coverage of adhoc networks.Cooperative communication allows terminals to collaborate with each other for data transmission. The challenge is to enhance performance with limited availability of resources.In this proposed work, a new secured data transmission mechanism is introduced for efficient communication between the sensor nodes. Experimental results show that proposed model performed well against security and transmission power compared to traditional models.

Keywords –WSN, Security, IBOOS,SET,Protocols.

I. INTRODUCTION

Wireless sensor network consists of a large number of small, low power, low cost sensor nodes with limited memory, computational, and communication resources
and a Base Station. These nodes continuously monitor environmental conditions and collect detailed information about the physical environment in which they are installed, then transmits the collected data to the BS. BS is a gateway from sensor networks to the outside world. The BS has a very large storage and large data processing capabilities. It passes the data it receives from sensor nodes to the server from where end-user can access them. The sensors nodes are generally deployed around the area of the Base Station and form groups as per the need of the Base Station. WSN has an advantage of being operated unattended in the environment where continuous human monitoring is either risky, ine_cient or infeasible. Sensor nodes run on batteries and once nodes are deployed, their batteries cannot be recharged, so they have a short lifespan. WSN [1, 2] consists of a large number of sensor nodes, moreover these sensor nodes run on non rechargeable batteries. So to serve the objective of fault-tolerance, load balancing and network connectivity, grouping of nodes is required. Clustering [3] is a process of dividing sensor nodes into groups on the basis of various parameters, and selecting a group leader from each group. The groups are called clusters and group leaders are called Cluster Heads(CHs) of the clusters. Parameters for forming the clusters include distance between the cluster head and its member, intra- cluster communication cost, residual energy of sensor nodes, location of node with respect to BS etc.

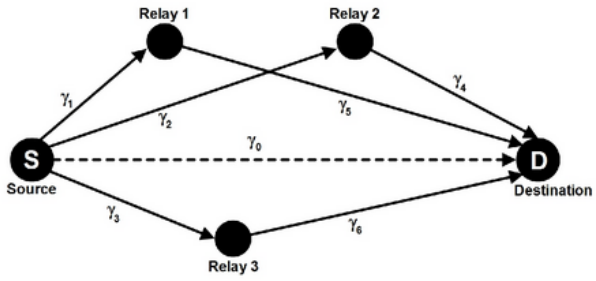


Fig. 1. Cooperative communication network

Figure 1.1 shows a communication network scenario when there is clustering in the network. Clustering divides the sensor nodes in the network into clusters and selects a Cluster Head (CH) for each cluster so that member from
Each cluster communicates through their CH in order to communicate to the BS. In this way clustering increases the network lifetime as after clustering a least number of nodes will access the

channel for communication with the BS, all the information and updates of whole cluster are collected together at CH and forwarded to the next CH in the hierarchy or the BS.

Motivation : When Wireless Sensor Networks are deployed mainly for military and health applications, there is a high need of secure communication among sensor nodes.

There are di_erent techniques to secure network data transmissions, but due to power constraints of WSN, group key based mechanism [11] is the most preferred

one. Hence, to implement scalable energy e_cient secure group communication, the best approach would be hierarchical based like Clustering [3]. In most of the WSN [1,2] designs based on clustering, Base Station is the central point of contact to the outside world and in case of its failure; it may lead to total disconnection in the communication. So in order to provide better fault tolerant immediate action, a new BS at some other physical location will have to take the charge. This may lead to a total change in the hierarchical network topology, which in turn leads to re-clustering the entire network and in turn formation of new security keys. Hence, in such situations, we need a clustering algorithm which will perform the minimum re-clustering with minimum energy consumption and minimum execution time. LEACH is a distributed hierarchical protocol, which provides data aggregation for sensor networks by selecting random CHs in a distributed manner. It forms clusters based on the received signal strength and uses the CH nodes as routers to the Base Station. All data processing such as data fusion and aggregation are local to the cluster. Each node transmits to them CHs which in turn aggregate and compress the data and send to the Base Station. A stochastic algorithm is used (round by round) by each node to determine whether it can become CH in that round or not. All non CH nodes communicate to the CH in TDMA fashion as scheduled by CH. In LEACH, Cluster Head is selected dynamically and rotated periodically which counts for less power consumption of the network. But since it uses single- level clustering scheme, power consumption is comparatively more to those algorithms that use multi-level clustering. Nodes that have been CH cannot be CH

for next i rounds. At the end of each round, node that is not a CH selects the closest CH and joins its cluster by informing the CH. This protocol creates non overlapping clusters. Although there is no energy-balancing problem in LEACH but it doesn't care about the energy consumption in intra-clusters communication. So clusters formed and its structure in LEACH may not be optimal. EEMC [7] is a multi-level clustering protocol, which organizes nodes into a hierarchy of clusters and aims at minimizing the total power consumption of the network as they use multi-level clustering scheme. It is an extension of TLCS (Two Level Clustering Scheme) [7] where each cluster is divided into sub clusters (level-2) having their respective cluster heads. These CHs after gathering data packets transmit the aggregated data packet to the corresponding CH of level-1 and _nally all CHs (level-1) send data to the BS.

Operation of data collection is done in rounds and each round has two phases: 1. Cluster setup phase : This phase means that the nodes execute this algorithm to establish multi-level clustering topology on its own. This phase works in a top-down fashion [20], that is Cluster Heads at level-i will be elected before level-(i + 1). Initially, all active nodes are set to non-CH nodes. Then each of these nodes send their location information and current residual energy to the BS to indicate that the algorithm will select a new set of CHs in level-1. When BS receives these values, it sends a message containing the total remaining energy of the network and the total reciprocal of the distance from all nodes to the BS. Once active nodes receive this command message, they set their probability of becoming level-1 CH on the basis of receiving values. Since along with node's residual energy, transmission distance of node is also considered as a factor in deciding CH, those nodes which are closer to the BS and/or have higher remaining energy have more chances to become level-1 CH. Transmission distance is considered as a factor because ultimately the CH has to transfer the packet to BS, so if distance is large more energy will be consumed and vice-versa. Later the elected level-1 CHs will broadcast an advertisement message its radio range, whoever non-CH node receive this advertisement message, sends a message back to CH containing its residual energy and joins that cluster. In this way both CHs and cluster members have information of each other. Then CHs will send a command message to their members containing number of nodes in the cluster, total remaining energy of cluster members

and total reciprocal distance from normal nodes to the cluster head. In this
way level-2 CHs will be selected and so on for further levels.

In an intra - cluster, one cluster-head will continue to be the CH, so energy consumption for new CH set up and updating cluster is reduced. These clusters are referred as layers, clusters closest to Base Station belong to the top layer. So, the entire network is divided into the V-wedges of clustering angle _ and these wedges form cluster of varying size. The operation is broken into rounds where each CH receives data either from its members or from lower layer CH and send the aggregated data either to the base station or the upper layer cluster with TDMA mechanism. It has high scalability due to these layering mechanisms. This protocol creates non-overlapping cluster with high stability as there is no node mobility possible. Initially Base Station informs to all the nodes of top layer about their CH and informs CH about its members. Then for lower layer immediate upper layer CH plays the role of Base Station in giving node information.

II. LITERATURE SURVEY

SPIN has moderate latency factor as it has to see that all ensures that all the interested nodes in the network to achieve the required data. It has a moderate scalability because whenever a new node enters it sends signals or a request for data sharing and all those nodes which are low in energy does not respond to any action to save energy, moderate energy awareness can be seen in SPIN as the nodes which are interested only take part in data sharing and the one which has low energy reserves stops responding to the messages sent by neighboring nodes. It has very low data overhead on the network as only a few nodes take part in the transmission. It keeps its quality of service factor, low as there are redundant data in the network; all the nodes share the same data. Memory is wasted as all the nodes share same data, and it is not an end to end transmission many nodes interfere while transmitting the data to the sink or base station.
GEAR has moderate energy efficiency as the nodes only follow the least cost paths that are calculated, until a new path is found which is much more least path than the earlier, this shows that even after using the least cost paths it fails in conserving more energy. It has a low latency as the time taken by a node to transmit between the source nodes to the destination region and from their to the destination node in the region. An average overhead is seen during transmission, if nodes find drained nodes in the network they stop data transmission
until a new least cost path is found. The quality of service is low as it has certain network instabilities like link failure, power failure or topology changes can bring down data transmission. Lots of bandwidth is wasted in searching the destination region and then the destination node using different kinds of algorithms.
Latency is moderate because when a source nodes wish to forward the data to the neighbor grid, all the nodes in that grid see that only one among them remain active to continue the forwarding strategy and the rest nodes go to sleep. It has a high scalability, any number of nodes can join the network and they divide themselves into grids and when there is more than one node, one of them goes to sleep to conserve energy. This makes it achieve high energy awareness as all the nodes changes states from active, discovery and sleep. As intermediate nodes are in sleep state, very few nodes take part in transmission gives low overhead of data in the network. It has very low quality of service factor as it has unpredictable traffic pattern, non end to end transmission prevails.

MECN

It has low scalability as if new nodes added to the sparse graph it does not consider them even though they are the nearest nodes to the base station. This also leads to low latency as each node has to calculate the sparse graph for its nearest neighbours every time it has data to transmit. Lot of energy is wasted in this sparse graph construction every time a node starts transmission. Even though its not considerable amount of energy it makes MECN a moderate energy aware protocol. A low quality of service factor is found as it has network instabilities like link failure, power failure, and limited bandwidth.

Protocol	Algorithm	Advantages
KASP	1ECDH 2 SKG 3 GKG	Better storage, Less overhead
S-AKA	It designed in two phases SAKA I, SAKA II	Less bandwidth consumption, guarantee robustness
Hybrid	ECDSA,	Reduces high

Energy efficient group key agreement protocol	PKA	Energy efficient protocol
Authenticate key agreement protocol	ECC	Preserves the quality of real time voice
3-IDAKA	Identity based verifier signature scheme	Only one round of message exchange makes the protocol efficient
Certificate based authenticated key agreement protocol	PKI	Two schemes are given which can resist attacks, useful to limited computational capabilities.
PAKE	ECC	Protocol is resilient to various attacks

SAR

SAR has low latency factor as nodes always follows a routing table which shows a least cost path from the node to the sink, and there is for sure one path existing to the destination, QoS is more when compared with other conventional protocols, It has no resource limitations like
limited bandwidth, transmission power, memory buffers. It has a limited scalability factor as it has to construct routing table for the newly deployed nodes which is costly. It has fault tolerance and easy node recovery for node failures. The power usage is very low and least compared because it constructs tree structure with only those nodes which are energy reserved and capable of QoS metric, the one which do not qualify are ignored from forming the roots in the tree. The purpose of Time Division Multiple Access is to give time slot to the nodes so that different nodes can access the channel without collision. In WSNs, different nodes communicate with a base station or sink node. Using TDMA, a time slot is given to the node so that each node can send data to sink in that time slot and during the inactive slots nodes sleep to save energy. In this case, nodes can use full bandwidth during the time slot. In this scheme, clock synchronization is required to avoid collisions; therefore sinks have to broadcast the clock synchronization packet to all nodes while it has to receive the packet to avoid the collision. While receiving the packet it has to be reactive from sleep mode, as the active modes energy is consumed in this case.

III. PROPOSED WORK

In a wireless sensor network a message contains information about an event that occurred. The message can be small or long, usually long messages increase the latency and can also waste the energy. If the few bits are corrupted in first transmission then a retransmission is done due to which lots of energy is consumed. A long message can be divided into small packets but for transmission of each packet control packet is needed and due to control packet for each small packet transmission delay will be increased. The SMAC protocol divides the long packet into small fragments and sends them in burst. SMAC uses only one packet for RTS and CTS for the whole transmission. In this situation when a packet is sent, the Source waits for the ACK and if it gets the ACK packet it transfers the next fragment. On the other hand, if it does not get any ACK it increases the transmissions time by one fragment and retransmit that fragment. The current transmission can be corrupted at the Source end if the Source does not get an ACK from the destination. If an existing node wakes up during the transmission process, it can start using the medium if it finds it free. This may lead to disturbance in the transmission at the destination side. To avoid this, each packet contains the field for transmission duration. If a new node joins the network during the transmission, after receiving the RTS or CTS packet it will go to sleep state and when it wakes up, it will be able to get information about extended period of time if there is a packet loss.

In cooperative communication data transmitted by single user may receive multiple users with same or different frequency channels.

In order to support multi-cell joint transmission with neighboring cells, a cooperative frequency subset is defined for each cell in CFR scheme. Then the resources are allocated to users in each cell cluster according to the following frequency reuse rule:

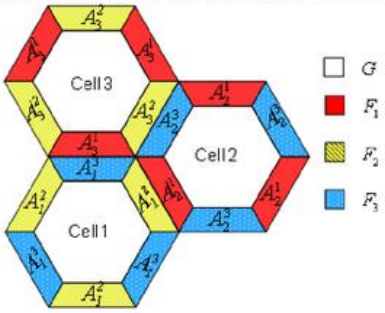
Step 1: In each cell, the whole resources are divided into two sets, G and F, where $G \cap F = \varnothing$. Resources in set G are used for CCUs in each cell, while resources in set F are used for CEUs.

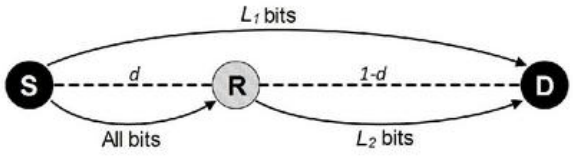
Step 2: Set F is further divided into three subsets, marked by F_1, F_2, F_3, with $F_i \cap F_j = \varnothing (i \neq j)$.

Step 3: For each cell cluster, F_i is assigned for cell i as a cooperative frequency subset, which is used for providing cooperative data transmission for the CEUs in neighboring cells.

Step 4: F_j is assigned for the CEUs in cell-edge zones marked with A_i^j.

Based on the defined frequency reuse rule, the frequency allocation for each cell in the cluster is shown in Fig.3.





Step 5: Clusterhead broadcast their identity in the networks.

Step 6: Base station broadcasts its information to all the sensor nodes in the network.

$$B_s -> s_N$$

Step 7: Clusterheads broadcast their identity to all the sensor nodes in the current cluster as

$$C_h -> Curr_N$$

Step 8: If the current cluster node wants to send data to other neighbor nodes it performs two operations

a) Let D be the data to be sent to neighboring nodes along with secured parameters like nonce,hash.
b) Encrypting the data in the current cluster .

$$C_h -> \{Encr(D), \text{nonce},\} Curr_N, \text{Comp(Trust)}$$

Comp(Trust):T=Number of packets requested by the sensor node/Unit time

If $T < \lambda(\text{default}:100)$

Set node as Secured

Else

Set node as Insecured.

Step5: if CH has a maximum convergence degree in neighbor nodes with energy <energythreshold and flag is secured .

Then

Broadcast Chmessage(ID)

Set CH state active.

Else

Wait a predefined time for receiving secured neighbor nodes .

Select cluster head, according to broadcasting.

End if

Step 9: if received CH or Join Message then

Update secured neighbors list.

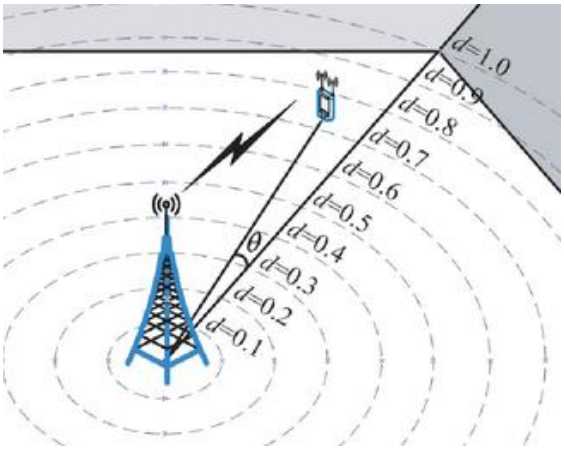
End if

Step 10: Data transmission from non-cluster head node to its cluster head

$$NonCluster_N -> B_s : \{E(k, D), \text{H(D, id)}\}$$

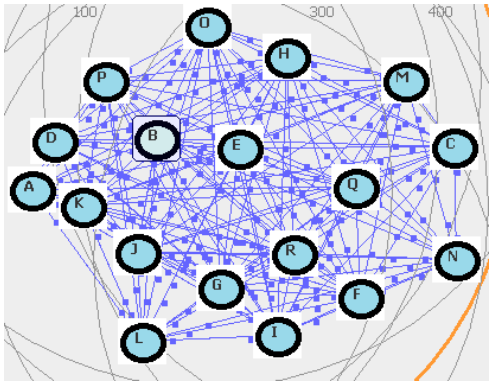
Step 11: When the cluster head completes data aggregation it sends aggregated data to its base station.

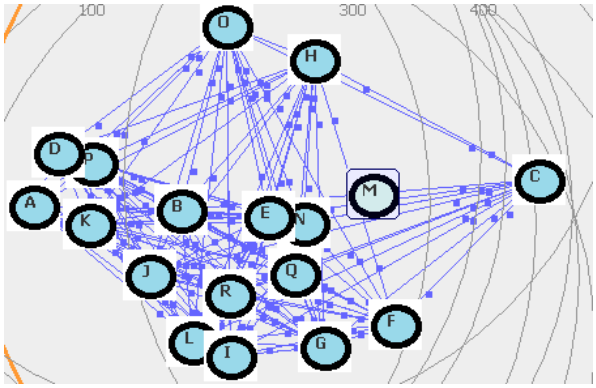
$$C_H -> B_S : \{\text{E(D, id)}, \text{H(D, id)}\}$$



IV.Experimental Results

All experiments are performed with the configurations Intel(R) Core(TM)2 CPU 2.13GHz, 2 GB RAM, and the operating system platform is Microsoft Windows XP Professional (SP2).



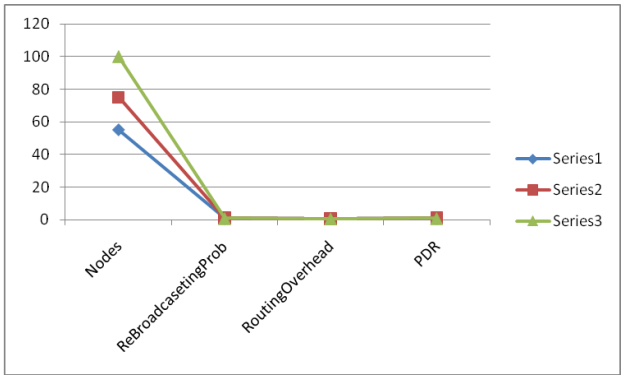


09:21:09 Q2501 : NODE INFO : K received control message from R
MAC collision Rate :0.05132
Normalized Routing Overhead :0.81852
Packet Delivery Ratio 0.97625
Avg Time Delay (%) :47.77189
Rebroadcasting Area 11.14617
ReBroadcasting Probability 0.92215
Number of CBR Connections :48
09:21:09 Q2501 : NODE INFO : L received control message from R
MAC collision Rate :0.15785
Normalized Routing Overhead :0.74227
Packet Delivery Ratio 0.94433
Avg Time Delay (%) :51.17496
Rebroadcasting Area 33.12658
ReBroadcasting Probability 0.92296
Number of CBR Connections :10
09:21:09 Q2501 : NODE INFO : M received control message from R
MAC collision Rate :0.11218
Normalized Routing Overhead :0.78431
Packet Delivery Ratio 0.96044
Avg Time Delay (%) :46.49888
Rebroadcasting Area 20.86764
ReBroadcasting Probability 0.89927
Number of CBR Connections :45
09:21:09 Q2501 : NODE INFO : N received control message from R
MAC collision Rate :0.08225
Normalized Routing Overhead :0.78449
Packet Delivery Ratio 0.98973
Avg Time Delay (%) :50.08031
Rebroadcasting Area 16.94794
ReBroadcasting Probability 0.95822
Number of CBR Connections :13
09:21:09 Q2501 : NODE INFO : O received control message from R
MAC collision Rate :0.14188
Normalized Routing Overhead :0.81649
Packet Delivery Ratio 0.95402
Avg Time Delay (%) :48.21303
Rebroadcasting Area 34.48403
ReBroadcasting Probability 0.94354
Number of CBR Connections :13
09:21:09 Q2501 : NODE INFO : P received control message from R
MAC collision Rate :0.17473
Normalized Routing Overhead :0.77942
Packet Delivery Ratio 0.92324
Avg Time Delay (%) :51.45782
Rebroadcasting Area 19.81915
ReBroadcasting Probability 0.85038
Number of CBR Connections :42
09:21:09 Q2501 : NODE INFO : Q received control message from R
MAC collision Rate :0.15288
Normalized Routing Overhead :0.71410
Packet Delivery Ratio 0.90097
Avg Time Delay (%) :47.02508
Rebroadcasting Area 23.17515
ReBroadcasting Probability 0.87003
Number of CBR Connections :6
MAC collision Rate :0.19429
Normalized Routing Overhead :0.76301
Packet Delivery Ratio 0.97875
Avg Time Delay (%) :50.28623
Rebroadcasting Area 25.51178
ReBroadcasting Probability 0.90952
Number of CBR Connections :31
09:33:41 Q6951 : NODE INFO : N received control message from R
MAC collision Rate :0.17091
Normalized Routing Overhead :0.73708
Packet Delivery Ratio 0.93225
Avg Time Delay (%) :46.97062
Rebroadcasting Area 17.02839
ReBroadcasting Probability 0.85956
Number of CBR Connections :49
09:33:41 Q6951 : NODE INFO : O received control message from R
MAC collision Rate :0.12752
Normalized Routing Overhead :0.79400
Packet Delivery Ratio 0.97803
Avg Time Delay (%) :50.07110
Rebroadcasting Area 12.56391
ReBroadcasting Probability 0.93415
Number of CBR Connections :4
09:33:41 Q6951 : NODE INFO : P received control message from R
09:33:41 Q6951 : NODE INFO : M received control message from R
MAC collision Rate :0.09960

Normalized Routing Overhead :0.79987
Packet Delivery Ratio 0.90504
Avg Time Delay (%) :46.15934
Rebroadcasting Area 17.98740
ReBroadcasting Probability 0.95452
Number of CBR Connections :10
MAC collision Rate :0.12874
Normalized Routing Overhead :0.79323
Packet Delivery Ratio 0.95155
Avg Time Delay (%) :48.03498
Rebroadcasting Area 31.02623
ReBroadcasting Probability 0.95636
Number of CBR Connections :49
09:33:41 Q6951 : NODE INFO : Q received control message from R
MAC collision Rate :0.10391
Normalized Routing Overhead :0.72237
Packet Delivery Ratio 0.98536
Avg Time Delay (%) :49.37436
Rebroadcasting Area 20.82254
ReBroadcasting Probability 0.93979
Number of CBR Connections :35

Perfornance Measures:

Nodes	ReBroadcasetingProb	RoutingOverhead	PDR
55	0.9	0.7	0.95
75	0.92	0.65	0.97
100	0.94	0.69	0.94



V. CONCLUSION

These protocols has proved efficiently that they are more useful in not only routing the most important data but also in conserving energy resources of a sensor (the batter) using different operation approaches. Most of the protocols show better and efficient features for application like surveillance, but there are still many more challenges that need to be solved in the sensor networks like in MAC protocols, there is still need to find out the suitable solution for real time support and energy efficiency because contention based protocols are energy efficient but they don't guarantee the real time support while contention protocols give real time support but lack in energy efficiency. . In this proposed work, a new secured data transmission mechanism is introduced for efficient communication between the communication nodes. Experimental results show that proposed model performed well against security and transmission power compared to traditional models.

7.REFERENCES

[1] Römer, Kay; Friedemann Mattern "The Design Space of Wireless Sensor Networks" IEEE Wireless Communications, Dec. 2004.
[2] V. Raghunathan, C. Schurgers, S. Park, and M. B. Srivastava, "Energy-Aware wireless Microsensor Networks", IEEE Signal Processing Magazine, 19 (2002), pp 40-50.
[3] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks", Proc. 4th ACM International Conference on Mobile Computing and Networking (Mobicom'98), Aug. 2000.
[4] Marcel Busse, Thomas Haenselmann, Wolfgang Effelberg, "TECA: A Topology and Energy Control Algorithm for Wireless Sensor Networks", Proc. Of ACM/IEEE International Symposium on Modeling, Analysis and simulation of Wireless Mobile Systems, Malaga,
Spain, October 2006.
[5] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks", Wireless Network, Volume:8, pp. 169-185, 2002.
[6] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," Proceedings of ACM MobiCom '00, Boston, MA, 2000, pp. 56-67.
[7] M. Chu, H. Haussecker, and F. Zhao, "Scalable Information-Driven Sensor Querying and Routing for ad hoc Heterogeneous Sensor Networks", The International Journal of High Performance Computing Applications, Vol. 16, No. 3, August 2002.
[8] Y. Yao, J. Gehrke, "The cougar approach to in-network query processing in sensor Networks", in: SIGMOD Record, September 2002. [9] Jichuan Zha, Ahmet T. Erdogan, and Tughrul Arslan, "A Novel Application Specific Network Protocol for Wireless Sensor Networks", IEEE Reference number 0-7803-8834- 8/05.
[10] Wendi B. Heinzelman, Anathan P. Chandraskan, and Hari Blakrisshnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks", IEEE Trans. on Wireless Communications, 1 (4): 660-670, OCT 2002.