American Journal of Computation, Communication and Control
2014; 1(1): 18-23
Published online April 20, 2014 (http://www.aascit.org/journal/ajccc)

Keywords
Wireless Sensor Network,
Security,
Energy Efficient,
Clustering,
Data Aggregation

Received: February 19, 2014
Revised: April 08, 2014
Accepted: April 09, 2014

A secured energy efficient clustering and data aggregation protocol for wireless sensor network

Sudharsan Omprakash[1], Giridharan Nanthagopal[2], Santosh Kumar Omprakash[3]

[1]IT, Anna University, R.V.S College of Engineering and Technology, Dindigul, India
[2]ECE, Anna University, Velammal College of Engineering and Technology, Madurai, India
[3]Software Engineer, Accenture, Bangalore, India

Email address
osudharsan@gmail.com (S. Omprakash), giri9393@gmail.com (G. Nanthagopal), oneorss@gmail.com (S. K. Omprakash)

Citation
Sudharsan Omprakash, Giridharan Nanthagopal, Santosh Kumar Omprakash. A Secured Energy Efficient Clustering and Data Aggregation Protocol for Wireless Sensor Network. *American Journal of Computation, Communication and Control.* Vol. 1, No. 1, 2014, pp. 18-23

Abstract
Energy consumption is a main factor which increases the life time of the network, where the energy can be saved in each individual node as well as by cluster based routing in the network. If the network is energy consumed and the security is less, the network cannot be consider as a trustable network, and passing a secret message is highly impossible in the network. Even though the energy and the security are two different and independent factors in the WSN, a secured energy efficient network should consider both the factors. In this paper we proposed, a Secured Energy Efficient Clustering and Data Aggregation – [SEECDA] protocol for the heterogeneous WSN, in which the security, energy efficient clustering, data aggregation are combined to achieve a best performance in terms of QOS by security and energy. The proposed approach includes a security mechanism, and an innovative cluster head election mechanism and the route will be selected with less energy needed. The simulation output shows that the SEECDA balances the security, energy efficiency and prolongs the network life time is high when compared to LEACH, EEHCA and EDGA, EECDA respectively.

1. Introduction

In recent years, Wireless sensor network (WSNs) plays a vital role in various application domains such as object detecting, medical caring, forest monitoring and so on. Energy ability and scalability are two greater challenges in Wireless Sensor Networks. For example, the number of nodes in a randomly unfold network needs to be enough high to ensure connectivity. As a result, when using its maximum transmission power, a node may have very large of neighbors. Therefore, it becomes critical if it tries to store the information about its neighbor. Having more neighbors than the required leads is unnecessary for energy consumption in the network. This problem can be overcome by using topology control which restricts the set of neighbors of given node. The transmission power can be reduced along

power consumption by carefully choosing the set of neighbors. Lack of energy efficiency which delays the lifespan of the network is one of the serious issues in the Wireless Sensor Network (WSN). In this, a Secured Energy Efficient Clustering and Data Aggregation – [SEECDA] protocol for the heterogeneous WSN, in which the security, energy efficient clustering, data aggregation are combined to achieve a best performance in terms of QoS by security and energy efficiency is proposed. The main characteristics of a WSN include Power consumption, Ability to come up with node failures, Mobility of nodes, Failure in communication, diversity of nodes, Ability to bare tough ecological conditions and so on. Sensor nodes can be considered as tiny computers, extremely basic in terms of their interfaces and their components. They usually have a processing unit, sensors, a communication device and a power source generally in the form of a accumulator (battery).

One of the big provocations (challenge) in WSN is to manufacture low cost and small sensor nodes. Number of the nodes is under the research and progress level, specially their software. Applications concerned with Local area network or Wide area network communicates with WSN through a gateway. The Gateway behaves as a span (bridge) between the WSN and the other network. This makes data to be stored and processed by device with more means (resources), for example in a server which is located far or remotely.

2. Related Works

The author in paper [1] discusses about the wide variety of attacks in WSN and their classification mechanisms and different securities available to handle them including the challenges faced. [2] Proposed to select intermediary nodes for each packet rather than sending the packets directly to the destination node. This disperses all the packets that are to be transmitted using a modified form of Backpressure algorithm [3] and then directs them to the destination node using SENCAST [4]. By following this method, most of the packets that are sent through a network have the probability of escaping black holes. Simulations show that our approach is much more effective in terms of security when compared to their deterministic counterparts. In [5], the paper says that it needs to be developed an effective routing mechanism that can with high probability, circumvent the black hole formed by this attack. The Purely Random Propagation (PRP) algorithm developed generates randomized dispersive routes so that the routes taken by the shares of different packets changes over time. Besides randomness, the generated routes are also highly dispersive and energy efficient, making them quite capable of bypassing black hole. Also, the energy constraint is highly optimized in the entire routing mechanism leading to minimal energy consumption. Extensive simulations are conducted to investigate the security and energy performance of our mechanism. In [6], proposed to achieve both flexibility and energy efficiency, allowing the end-user to maximize system lifetime.

The security factors are provided using multipath routing protocol in WSN [9]. There is variety of security issues and concerns are focused in [8]. LNCS – [Location aware network coding] protocol is proposed in [10]. According to the range assignment, the energy can be consumed in the network [11]. A new lightweight Group based Trust Management Scheme is proposed in WSN for employing the clustering [12]. A meta-protocol [Meta-TMP] is proposed in [13], which is used to represent the class of topology maintenance protocol. A valid IDS algorithm for WSN is proposed which don't require prior knowledge of the behavior of the network [14]. The impact of optimization of the feature set for Wireless IDS which improve the performance of the security in [15]. A monitoring sensor node is having capability to detect an intruder, is analyzed with the help of the neighbor nodes and those nodes statistical model is discussed in [16].

An approach which detects the attackers available inside the network is proposed in [17], which has the efficiency to defending two types of attacks. [18] Introduced a representation to describe three probability distributions which improve the detection rate. DOS attack on the physical layer is analyzed and an extension of the security in the same layer using ant system is proposed in [19]. Congestion control for wired network is generally done using end-to-end and in network layer mechanism it is acting in concert is discussed in [20].

But in this paper, a novel secure routing protocol is proposed for wireless sensor networks in which sensor nodes as well as the base station are mobile. The protocol achieves security property through symmetric key cryptography and threshold key cryptography. An analysis of the security strengths of the protocol is presented. Simulation results show the throughput of the proposed protocol and a comparison with LEACH regarding its throughput.

3. Methods

The functionality of the SEECDA consists of five phases: ID based clustering, Cluster Head Election, ID verification, Data Aggregation and Maintenance. The Id based cluster formation phase divide the network area into M number of sub area according to the size of the network and total number of nodes going to deploy in the network. While deploying the nodes in the network, there is a dynamic ID is provided with the area number or name of the area concatenated and the number of nodes in each area is more or less equal in count. After the cluster formation the cluster head election phase is accomplished. Before going to elect the cluster head each node should be verified for ID verification. In according to the highest energy the CH is elected and the CH broadcast a message to BS.

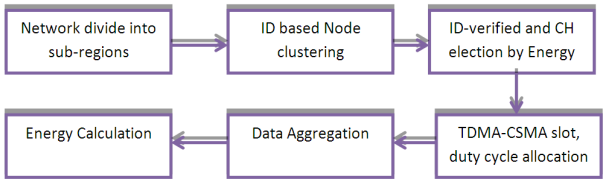

Figure 1. *System Model.*

The system model for SEECDA is analyzed, and it is shown in figure-1, where a network region is divided in to sub regions, and the number of nodes is placed by assigning a dynamic ID for security verification. The region sizes are approximately equal in area and numbers of nodes deployed in each region are deployed in equal manner.

According to the ID number of each node and is equally placed in all the sub-regions and sends a hello message to the BS. The node ID starts from 0 to N-1, where the node 0 is placed in the cluster-1, node 1 is placed in the cluster-2, where the i^{th} node is placed in cluster-i+1 respectively. All the nodes are initiated with energy as 100. For every transaction a node needs some energy value. The spending energy is subtracted from the initial energy in every transaction, and the energy of the nodes is getting changed [decreased]. Due to the highest energy, the CH is elected and slot allocation is applied for each node to avoid collision and save the energy.

An optional slot can be given for each node in a duty cycle manner for large size of data and huge number of data to be sends to the cluster nodes and CH, can be obtained by TDMA-CSMA methodology. Finally the CHs can gather and aggregate the data to the BS and CH will be elected according to the energy value.

$$E_{TX}(data_i) = E_{TX}\, x\, data_i + (d(i,j)^2)\, x\, ERX\, x\, data \quad [1]$$

$$E_{RX}(b) = E_{RX}\, x\, data \quad [2]$$

The Mathematical representation of the system model is written as:

The network area is separated into M sub-regions. Then each region is considered as a clusters and BS recruits this phase. In the network region M_i, the distance of a node which is far away from the BS in the region M and the distance between each sensor node sni and base station is calculated using equ-[3].

$$dist = \max(\forall_{i=1}^{N} d(s_{ni}, BS) \quad (3)$$

The CH is elected according to the node's energy Ei and the Energy to transmit or receive Ec with other nodes in the cluster and the BS. Nodes in a cluster calculate their probability to become a cluster head CH.

$$CH(nodei) = 1 - \left[\frac{((\frac{t_{round}}{ttf}) x (Ec + u)) + \sum_{j=1}^{n(c)} E_{TX}(bnode, mni)}{Er} \right] \quad (4)$$

The CH is elected using the equ-(4), where μ is the energy needed for data aggregation. T_{round} is the number of round and at each round the number of slots assigned by TDMA frame period. The t_{round}/t_{tf} is the total number of times that the CH needs to do the aggregation and the total energy to communicate with the cluster members [mn] to transmit the TDMA time slots. N© is the total number of nodes in the cluster. The energy to transmit b data to the next hop cluster head (CH_i) is, derived from [1] and [5].

$$E_{TX}(data_{node_i}, CH_i) = E_{TX}\, x\, data) + (dist(sn, CH_i)2)\, x\, ETX\, x\, data \quad [5]$$

Data aggregation by the CH is the process of aggregating all the data from all the cluster nodes in the cluster, and sends it to BS, for eliminating the redundant transmission in the communication of the cluster nodes with the BS. By accept the TDMA slot, all cluster members pitch the oversee information to its CH. Each CH postpone for one TDMA frame to collect the teaching from its member nodes. After each TDMA design, CH contains the information and forwards the lot of data to the base station

4. Algorithm

1. Network G = { G_1, G_2, G_3, ……. G_n}
2. K = length(G)
3. E_i =100; E_{TX} = 2.0; E_{RX} = 1.5; E_{SLEEP} = 0.10; E_{IDLE} = 0.5; E_{LISTEN} = 0.75;
4. for i = 1 to NN / K
5. $node_i$[key] = strcat (randi(NN), G_i)
6. G_i(i) = node[i]
7. End
8. For i = 1 to NN
9. For j = 1 to length(G_i)
10. If (($node_i$(key)).valid == "true") then node(i).msg → BS
11. Else discard the $node_i$
12. $node_i$.slot =1;
13. E_i[$node_i$] = E_i[$node_i$] – E_{TX}[$node_i$];
14. End j
15. End i
16. For i = 1 to K step length(G_i)
17. CH = max(max(E_i[$node_i$]));
18. end
19. For i = 1 to NN
20. For j = 1 to length(G_i)
21. If (nodei.slot == 1)
22. If (($node_i$(key)).valid == "true") then node(i).data → CH && CH_i.data ← CH_i.data + node(i).data
23. Else discard the $node_i$. data
24. $node_i$.slot = 0;
25. E_i[$node_i$] = E_i[$node_i$] – E_{TX}[$node_i$];

26. $E_i[CH_i] = E_i[CH_i] - E_{RX}[CH_i]$;
27. End j
28. End i
29. For i = 1 to length(G_i)
30. CH_i.aggdata → BS
31. end
32. repeat step 6
33. If ($E_i(node_i) \leq 17$) then $node_i$.state = dead;
34. For I = 1 to NN
35. If ($node_i$.state = = dead) then $E_i(node_i) = 100$; // battery Recharge
36. End

5. Results and Discussion

In this section we discuss the pretense muse and deed valuation of the intend technique using Wireless sensor network simulator-2.34. In our simulation fork, 100 sensory nodes are randomly extended in a field with extent 100m x 100m. All nodes transfer same size packets. Remaining parameters are listed in TABLE I.

Table 1. *Network simulator – parameter setting.*

Parameter	Value
Initial Energy	100 Joules
Receive Power	22.2 mW
Transmit Power	31.2 mW
Sleep Power	0.0006 mW
Data packet size	40 bytes
Noise Bandwidth	30 KHz

We use the random deployment model for the sensor network topology setup. BS is placed in the location (120, 50) which is away from the sensor field. We have compared our results with LEACH and LEACH – C [5] protocols. Energy is one of the major issues in wireless sensor network. In LEACH protocol, clusters are not evenly distributed so the cluster members spent more energy to transmit a packet to its cluster head. In LEACH – C clusters are evenly distributed but at each round all nodes send its information to the central BS and it is more expensive. But in our proposed method, clusters are formed based on the K – means clustering algorithm. Thus all the clusters are evenly distributed and all the cluster members are closer to its cluster head. So the energy consumption for SEECDA is less than the energy consumption for LEACH protocols.

The Figure-2 shows a Network G with N number of Nodes. After creation of the network we can perform the cluster formation and cluster head selection process. In the particular Network (G), Nodes in the network are selected randomly according to the size of each node and nodes are organized in that particular network. After deploying nodes in that network an ID number is provided for each node for identification and for some future use.

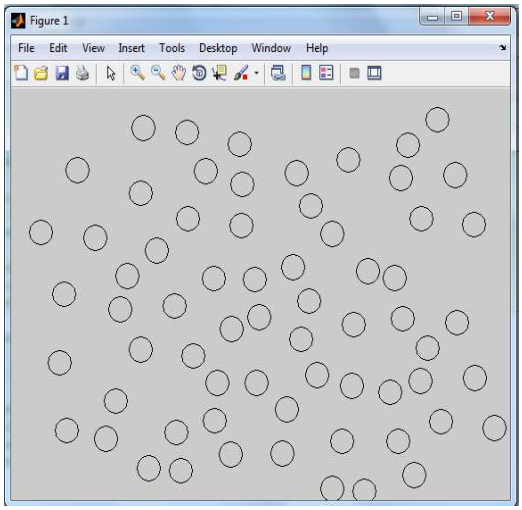

Figure 2. *Network with N no of nodes.*

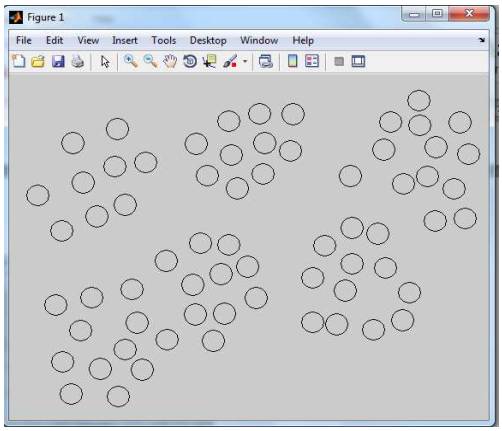

Figure 3. *Nodes are grouped as clusters.*

The Figure-3 shows the grouping of nodes in a particular Network. The nodes are organized and grouped into clusters based on unique ID number of nodes. A particular r network contains some number of clusters and each cluster contains some number of nodes. For example in Figure-3, cluster 1 contains the nodes and their ID number will be from 1 to 10 and also the cluster 2 contains the nodes and their ID number will be from 11 to 20 and so on. Based on ID number, nodes of each Cluster formed in a network Figure-2: Network G with N number of Nodes deployed randomly

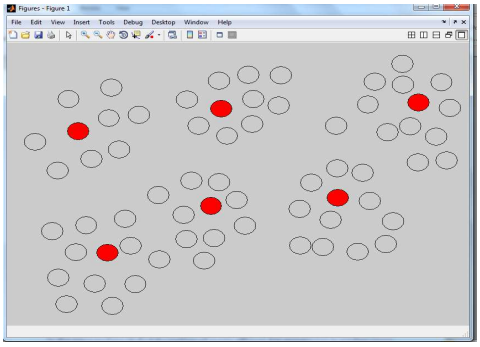

Figure 4. *Clusters with CH elected.*

The Figure-4 denotes the Cluster Head selection. Each cluster contains number of nodes based on unique ID. After deploying those nodes in a particular cluster, we have to choose the cluster head. Before choosing the cluster head, we should check whether the node is belongs to a particular cluster or not. After the successful completion of checking, we choose individual head for each cluster. The main purpose of the Cluster Head is to communicate with other nodes which are deployed in that particular cluster.

6. Comparison of Network Life Time with other Reported Results

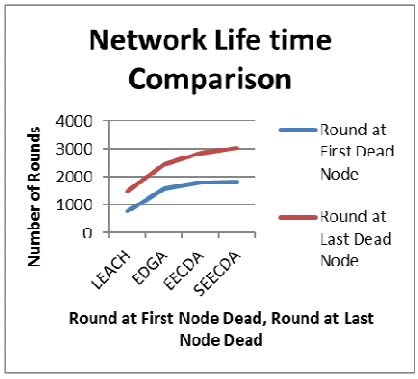

Figure 5. *Network lifetime as a function of first and last dead nodes in area 800 x 800.*

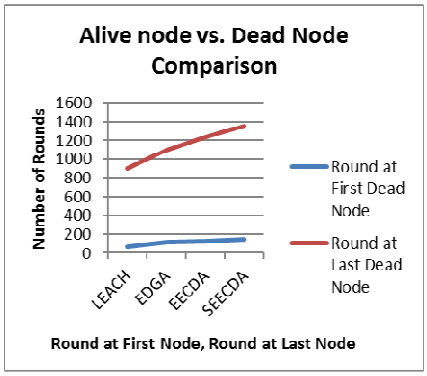

Figure 6. *Network lifetime as a function of first and last node in area 1200*1200.*

The Figure-5 shows the comparison for a small area network lifetime of first and last node. Here we are going to compare three approaches namely LEACH, EDGA, EECDA with our proposed approach SEECDA. In LEACH approach, the first dead node was detected at 789th round and the last dead node detected at 1499th round. In EDGA approach, the first dead node was detected at 1589th and the last dead node was detected at 2453rd round. In EECDA approach, the first dead node was detected at 1786th round and last dead node was detected at 2856th round. In our SEECDA approach, the occurrence of first dead node was detected at 1830th round and the last dead node was detected at 3045th round. So the Network life time in our SEECDA approach is better when compared with existing three approaches LEACH, EDGA, and EECDA.

The Figure-6 shows the Network lifetime comparison of LEACH, EDGA, EECDA and SEECDA large area network. In the LEACH method, in 75th round the first dead node was discovered. But the last dead node was occurred in 900th round itself. In the EDGA method, in 120th round the first dead node occurred but the last dead node was occurred at 1100rd round. In EECDA approach , the first dead node and last dead node occurred at 132nd round and 1234th round respectively. The SEECDA approach achieves better network lifetime when compared with other three existing approaches such as LEACH, EDGA, and EECDA.

7. Comparison of Energy with the other Reported Results

The Figure-7 shows the comparison of energy in each round for LEACH, EDGA, EECDA and SEECDA. Initially, consider the energy value as 100 at 10th round. In each approach, whenever the rounds increased, the corresponding energy level will be decreased. In LEACH approach , at 1000 level the energy level decreased as 23 , when at 3000 round, the energy level becomes as EDGA approach at 1000 round the energy level will be 58 and after that linearly energy level gets decreased AS 0. In EECDA approach at 4000 round, the energy level becomes as 0.But in our SEECDA approach even though it will reach 4000, the energy level remain as 8 and this energy level will be sufficient for some more rounds. In our proposed SEESDA approach, the energy level also be better when compared with other existing approaches.

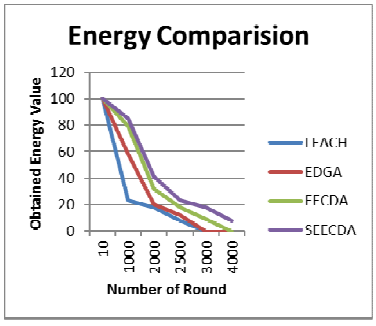

Figure 7. *Energy Comparison in each Round.*

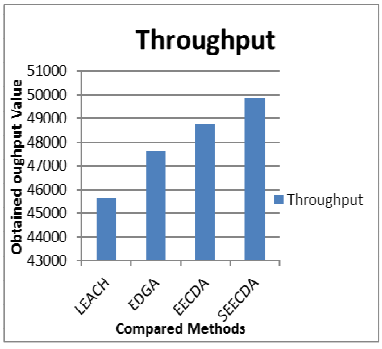

Figure 8. *Throughput comparison.*

Figure-8 shows throughput comparison existing of approaches. In LEACH approach, the obtained throughput was 45600. In EDGA approach, the throughput obtained was 47000. And in EECDA approach the throughput obtained was 48500. In our proposed SEECDA approach, the throughput obtained was 49800. The highest throughput was obtained in our proposed method, when compared with the other existing approaches.

8. Conclusion

In this paper, we have studied the problem of energy efficient data transmission in wireless sensor networks and proposed a cluster based data aggregation method which consists of four phases. As clustering process is performed only when it is necessary, the setup message transmission is reduced. Cluster heads are chosen in an optimal way. Any node becomes the cluster head only when it has the higher capability to communicate its cluster members throughout a round. Results of our simulation study indicate that proposed method conserve more energy and highest throughput when compared with other existing approaches. In future, the throughput, energy of the system will be improved and life time of the node in each round also will be improved.

References

[1] Yogesh Kumar, Rajiv Munjal, Krishan Kumar, "Wireless Sensor Networks and Security Challenges", National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC) 2011

[2] G. Ravi, M. Mohamed Surputheen, R. Srinivasan, "Secure Packet Transmission in Wireless Sensor Networks using Dynamic Routing Techniques", International Journal of Computer Applications (0975 – 8887)

[3] Michael J. Neely, Rahul Urgaonkar, "Optimal Backpressure Routing for Wireless Networks with Multi-Receiver Diversity, AD HOC NETWORKS (ELSEVIER)", July 2009, Vol. 7, No.5, PP. 862-881.

[4] P. Appavoo and K. Khedo, "SENCAST: A Scalable Protocol for Unicasting and Multicasting in a Large Adhoc Emergency Network", IJCSNS International Journal of Computer Science and Network Security, February2008, Vol.8, No.2.

[5] J.Preetheswari, J. Mark Jain, " Optimized Secure Data Delivery based on Randomized Routing in Wireless Sensor Networks", International Conference on Recent Trends in Computational Methods, Communication and Controls (ICON3C 2012)

[6] M.Shankar, Dr.M.Sridar, Dr.M.Rajani, " Performance Evaluation of LEACH Protocol in Wireless Network", International Journal of Scientific & Engineering Research, Volume 3, Issue 1, January-2012 ISSN 2229-5518

[7] Hiren Kumar Deva Sarma, Avijit Kar, and Rajib Mall, "Secure Routing Protocol for Mobile Wireless Sensor Network", 2011 IEEE

[8] Ali Modirkhazeni, Norafida Ithnin, Othman Ibrahim, "Secure Multipath Routing Protocols in Wireless Sensor Networks: A Security Survey Analysis", 2010 Second International Conference on Network Applications, Protocols and Services

[9] Eliana Stavrou, Andreas Pitsillides," A survey on secure multipath routing protocols in WSNs", 2010 Elsevier

[10] ERMAN AYDAY, FARSHID DELGOSHA, FARAMARZ FEKRI, "Data Authenticity and Availability in Multihop Wireless Sensor Networks", ACM Transactions on Sensor Networks, Vol. 8, No. 2, Article 10, Publication date: March 2012.

[11] Fadila Khadar and David Simplot, Centre de Recherche INRIA Lille - Nord Europe, "Incremental Power Topology Control Protocol for Wireless Sensor Networks", 2009 IEEE

[12] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d'Auriol, Heejo Lee, Sungyoung Lee,Young-Jae Song, "Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 20, NO. 11, NOVEMBER 2009

[13] Andrea Gabrielli, Luigi V. Mancini, Sanjeev Setia, and Sushil Jajodia, "Securing Topology Maintenance Protocols for Sensor Networks", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 3, MAY/JUNE 2011

[14] Chun-ming Rong , Skjalg Eggen , Hong-bing Cheng, "A Novel Intrusion Detection Algorithm for Wireless Sensor networks", 2011 IEEE

[15] Khalil El-Khatib, "Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 21, NO. 8, AUGUST 2010

[16] QiWang, ShuWang, ZhonglouMeng, "Applying an Intrusion Detection Algorithm to Wireless Sensor Networks", 2009 IEEE

[17] Yi-Ying Zhang, Wen-Cheng Yang, Kee-Bum Kim, Myong-Soon Park, "Inside Attacker Detection in Hierarchical Wireless Sensor Network", 2008 IEEE

[18] Ming Li, Wei.jia Jia, and Wei Zhao*, "Decision Analysis of Network-Based Intrusion Detection Systems for Denial-of-Service Attacks", 2001 IEEE

[19] K.SANTHI SAGAR REDDY, Dr. S. VARADARAJAN, M.SUNIL KUMAR, "IMPROVING QOS UNDER DDOS ATTACKS IN WIRELESS SENSOR NETWORKS USING ANT SYSTEM", International Journal of Engineering Science and Technology (IJEST) 6 June 2011.

[20] Bret Hull, Kyle Jamieson, Hari Balakrishnan, "Mitigating Congestion in Wireless Sensor Networks", SenSys'04, November 3.5, 2004, Baltimore, Maryland, USA.Copyright 2004 ACM 1-58113-879-2/04/0011