Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.146 – 156

RESEARCH ARTICLE

Energy Efficient Trust Mechanism using Genetic Algorithm in WSN

Nidhi Aley
Department of CSE, GHREAT, Nagpur
nidhi.a02@gmail.com

Shruti Kolte
Department of CSE, GHREAT, Nagpur
shrutikolte32@gmail.com

ABSTRACT

A wireless sensor network consist of large number of small tiny nodes which are only activate for limited amount of time, these nodes are distributed in nature and are vulnerable. These sensors are responsible for performing not only computation and communicate data but it senses some essential parameter and sends information to base station or sink.

Now a day’s wireless technology becoming more popular, hence the two major parameters, energy and security are very important issues and difficult to handle. These issues are interrelated since because of energy issue and limited power resources there are some restrictions on implementation of security.

The security issues are data integrity, Data confidentiality, service availability and energy consumption. In such case, the designing protocol for security issues must ensures minimization in energy consumption.

This paper describes some solution to the WSN’s energy issues and secure routing, as well as a combination of shortest path and routing algorithm is used to save time and network lifetime. Genetic algorithm is used as filter to the packet, which applies the rules on packet and checks its validity.

1. INTRODUCTION

Sensor modes perform data processing, computing, sensing and communication with limited resources like power, memory size and bandwidth. Therefore care has to be taken while designing the network under these limitations. Most of the energy is consumed in communication of data. It is impossible to recharge the deployed node, and the lifetime of network is interdependent on battery lifetime, thus energy is vital for many applications.

In WSNs energy utilization, routing, data processing, data aggregation, security etc. are related to each other. For any application if network is not secure from attack, then entire effort of transmission of data is lost.

There are two types of attacks/intruder: external and internal. External intruder do not have authorize access to system and they attack by using various penetration technique. Whereas internal intruder have access permission that can perform authorized activity. These internal intruders are insider threat to the system.

External intruder may attack to change the nodes to behave maliciously resulting in an abnormal behavior. The internal intruder attack to change the data processed within the nodes. In this paper we are more concern about internal attacks.

Trust mechanism with the notion of trust in human society has been developed to defend against insider attacks.

In general trust mechanism works in 3 stages:

1) Node behavior monitoring: Watchdog is a monitoring mechanism popularly used in this stage. It records each node’s behaviors such as packet forwarding. This collected data will be used for trustworthiness evaluation in the next stage. The confidence of the trustworthiness evaluation depends on how much data a sensor collects and how reliable such data is.
2) Trust measurement: Trust model defines how to measure the trustworthiness of a sensor node. There are several representative approaches to build the trust model, which include Bayesian approach, Entropy approach, Game-theoretic approach, and Fuzzy approach.
3) Inside attack detection: Based on the trust value, a sensor node determines, whether its neighbor is trustworthy for collaboration (such as packet forwarding). If a neighbor’s trust value is less than a certain threshold, it will be considered as malicious node.

Thus, an inside attacker can disguise its malicious behavior behind network traffic or noise. Thus, it cannot ignore the fact that insiders have internal knowledge about our network and security mechanisms against attacks. By exploiting such knowledge, inside attackers can launch their attacks intelligently to avoid being detected.

2. PROBLEM DEFINITION AND OBJECTIVES

- The energy consumption and network lifetime of WSNs are interdependent. It required less energy for processing of data whereas more for transfer of data from sensor to other.
- When all the nodes start detecting an intruder and transfer information to base station a large amount of energy consumed, and network lifetime reduced.
- The challenge is to establish an effective vulnerability/attack detection and response system for accurately detecting attacks and minimizing the impact of security breach to virtual network system users.

The main Objectives of using proposed system are:

- Reduce the energy consumption and increase the network lifetime of the WSNs.
- Design a reliable, energy-efficient trust mechanism for WSNs by considering the identified vulnerabilities and defending approaches.
- Utilize redundancy and energy efficiently, because workloads such as message exchanges that are required to manage disjoint paths may significantly degrade the network functions.
- Activate only one sensor node called watchdog to detect an intruder and communicate the information with sink.

3. IMPLEMENTATED WORK

The detection of any change in the data processed is difficult. Generally the analysis of data sent by each node is done by internal intrusion detection.

The proposed algorithm is used for internal data analysis, where it applies the rules on data packet and checks its validity. Next it checks for node validation and select the routing path to send data packet. The routing table includes entry of valid node, their distance, and cost. The watchdog node, who doesn’t involve in communication, will maintain the behavior and availability of each node in network. The remaining nodes are use for processing of data for further routing. The affected node is ignored and next shortest/ best routing path is initialized. Now an affected node is sent to sink where a recovery algorithm is applied on it at the same time. Hence the process of detection and then recovery of malicious node is not involved in main data processing. This will surely consume less energy as it does not allow the data packet to reach the malicious node, and select next best rout. Thus energy consumption is minimizes during this process.

The proposed system uses fundamental routing protocol named Link State Routing Protocol with the exclusion of Dijkstra's algorithm. This protocol is particularly attractive in the case of Wireless Sensor Networks which have limited hardware and software features. The redundancy on applying **Dijkstra's algorithm** here reduces the routing overhead. Its absence in calculation of the shortest path is compensated using our 'Select the Most Trusted Route' (SMTR) algorithm which chooses the most reliable (or trusted) route.

Algorithm 1:

For calculating the trust of node -

Initial condition:

Each node wants to communicate with other nodes in the network.

Input:

Get the source and destination of the network.

Output:

Trust value calculation and communication.

Begin:

Apply Link State Routing Protocol.

Taking routing as main objective, proposed routing mechanism dedicated for wireless sensor networks. In our proposed method, the new algorithm SRPT (Secure Routing Path using Trust values) has better performance as compared to existing systems. Here, in this approach, during transmission of packets, if any node in the routing path get fails to transmit the packets. That time it automatically select another routing path through which the packet sent to the requested destination.

The combination of link state routing protocol, dijkstra, and genetic algorithm are designed and placed in following way:

Algorithm 2:

a) Routing algorithm

    1. Select source and destination node
    2. If selected node is not valid then
    3. Source=0, destination =0
    4. If location is selected and both nodes are valid then
    5. Calculate distance from source to destination
    6. Draw path from source to destination
    7. Add that path to path dictionary

b) Shortest path algorithm

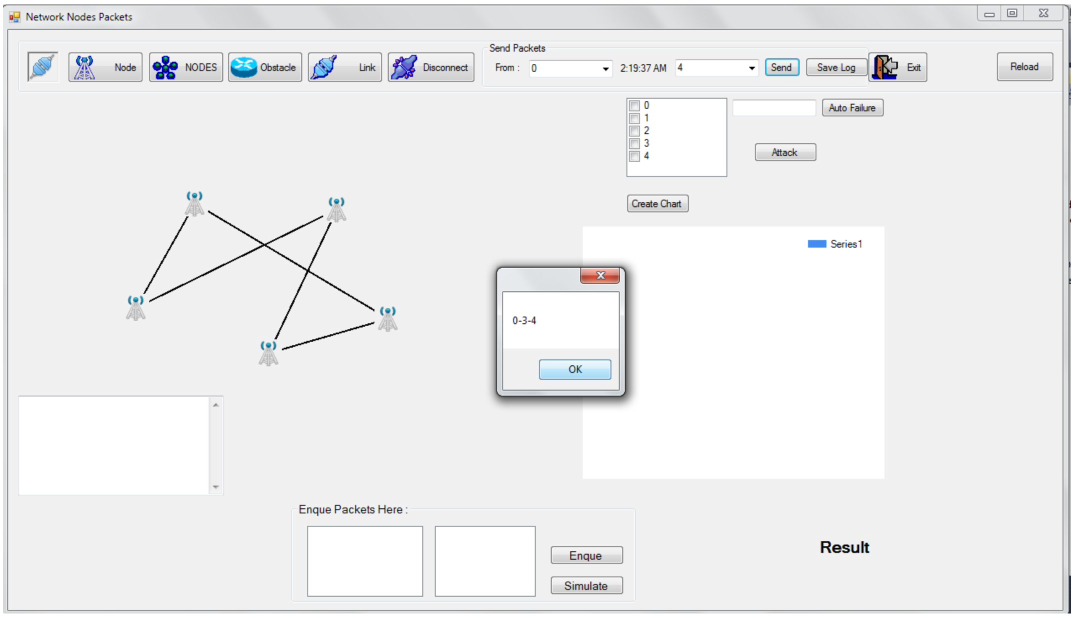
    8. Calculate all distance matrixes
    9. For all path
    10. Select first two paths
    11. Compare shortest distance
    12. Set the shortest path to top
    13. If obstacle found
    14. Set another shortest path to top

c) Packet filtering via genetic algorithm with 3des encryption

    15. If packet found then
    16. Encrypt/decrypt
    17. Apply filtering
    18. Check packet behavior and size
    19. Compare with last successful transmission from path dictionary
    20. If changed then send to sink
    21. If same then pass to next hop
    22. Add entry in path dictionary

4. IMPLEMENTATION DETAILS

The working environment for proposed algorithm for energy efficient trust mechanism is implemented using c#.net and visual basic 2010. As shown in fig.1, a sensor network with 5 nodes is created, and they are linked with each other. The sender and receiver node is decided from respective text box. As user press send button the shortest path among the nodes selected and packet routs through that hops.



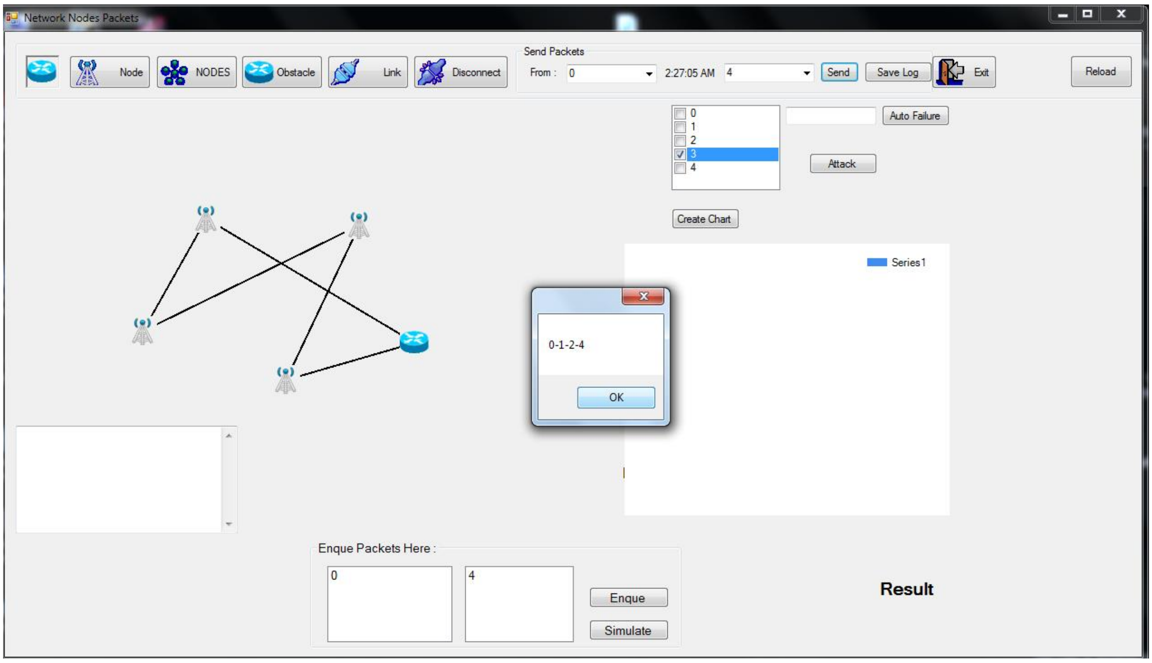
From : 0 2:19:37 AM 4

□ 0
□ 1
□ 2
□ 3
□ 4

0-3-4

Fig.1 Network creation and packet sending

As shown in fig.2 if node failure appears, the proposed algorithm chooses another shortest path to reach destination. In this process packet never reach to affected node instead it select the path before sending and then rout through safe hops.



From : 0 2:27:05 AM 4

□ 0
□ 1
□ 2
☑ 3
□ 4

0-1-2-4

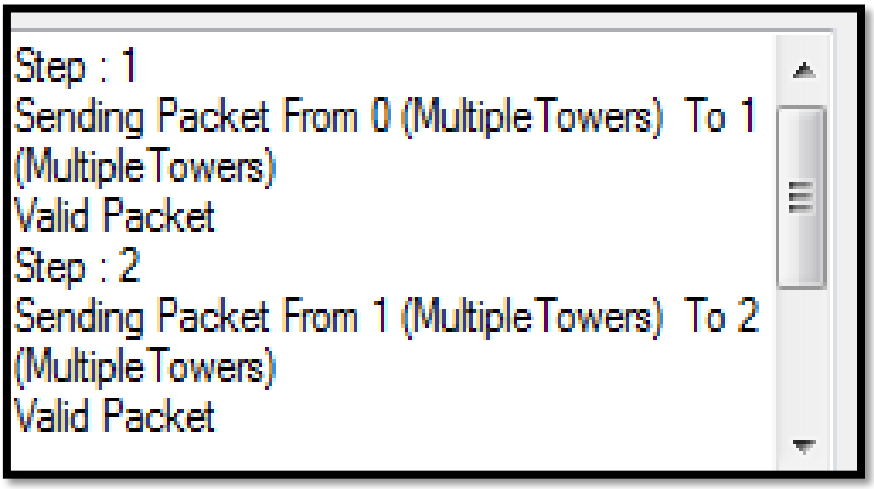
0

4

Fig.2 Node failure and selection of another safe route

5. RESULT CALCULATED

Fig.3 shows generated shortest path and the list of hops from where the packets pass successfully. Each time other nodes connected to the current node is checked and the safe node will only receive the data. The packet validity checking is done every time whenever it reaches to a hop.



```
Step : 1
Sending Packet From 0 (MultipleTowers)  To 1
(MultipleTowers)
Valid Packet
Step : 2
Sending Packet From 1 (MultipleTowers)  To 2
(MultipleTowers)
Valid Packet
```

Fig.3 Packet rout and validity checking

6. COMPARATIVE ANALYSIS

I. Comparison of original and malicious packet

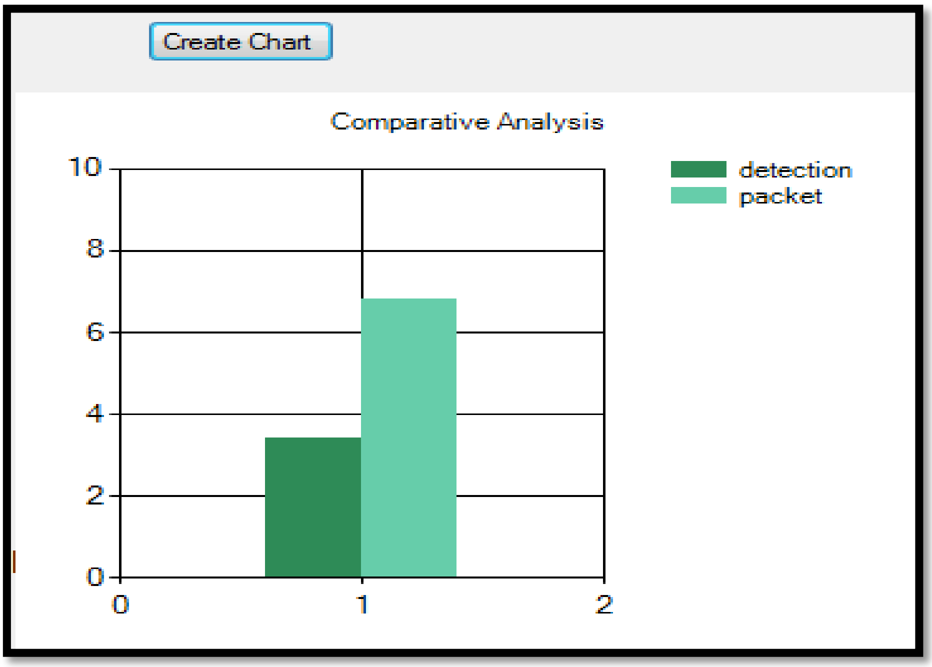
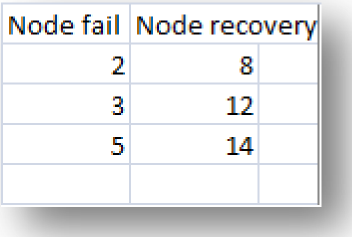


Fig.4 Analysis of original and malicious packet found

II. Comparison of node failure and recovery

Fig.6 a) and b) shows that each time whenever sensor network created, the frequency count of node fail is less than node recovery by using genetic algorithm. The following time chart shows the number of occurrences of node failure. In real transaction node failure results in big delay that can destroy the whole transaction, hence users' trust towards the sent packet will reached to the destination is not sure.

The select another best path concept make sure the same transaction with different rout with all security that pass the packet safely to destination. The next rout assumes different nodes that are either recovered or continuously active nodes.



Node fail	Node recovery
2	8
3	12
5	14

Fig.6 a) node failure and recovery analysis

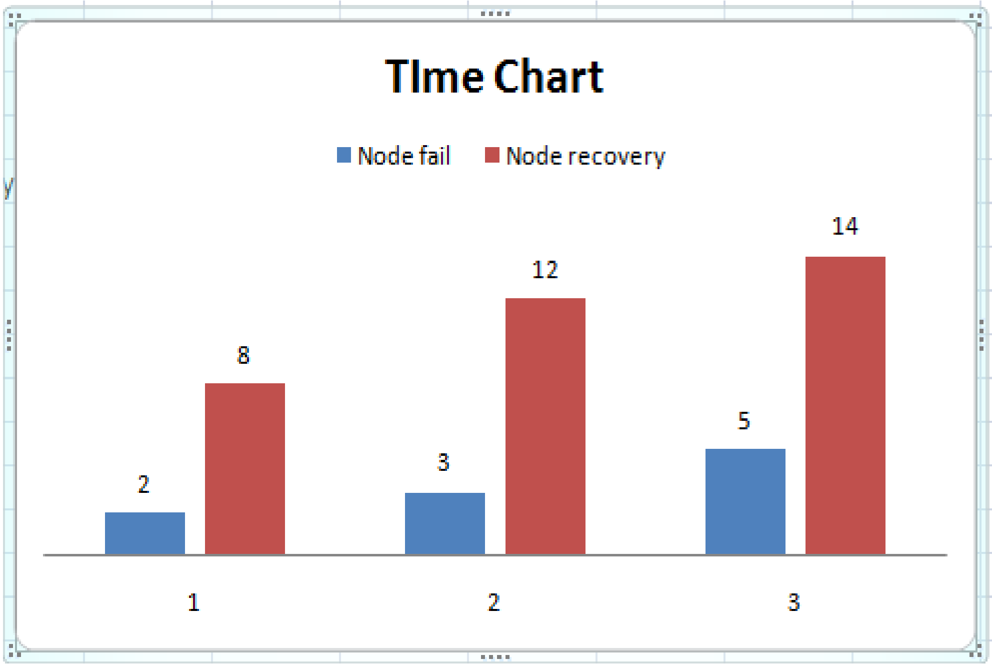
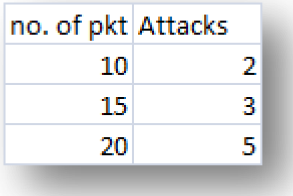


Fig.6 b) Time chart for node failure and recovery

III. Chances of node attack

While working with sensor network the analysis work shows that there are certain chances of number of occurrences of node attack with particular number of nodes. Following table describe it better.



no. of pkt	Attacks
10	2
15	3
20	5

Fig.6 c) Chances of node attack

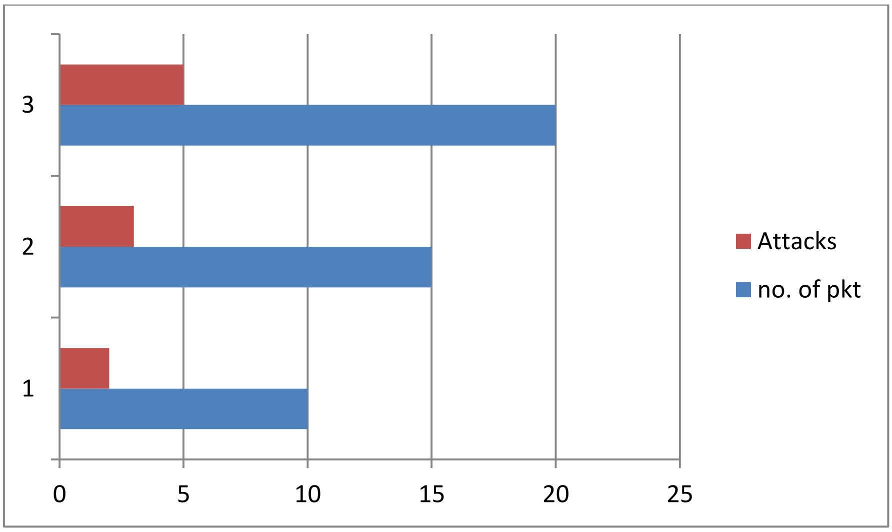


Fig.6 d) Time chart for chances of attack

7. CONCLUSION

In this implemented work, we applied combination of Dijkstra and link state routing algorithm for finding best and safe path among the network. A sending packet check the node index and decide the routing path, since the packet never reaches to affected node which removes the processing time required to detect and then recover the original packet. This mechanism saves time as well as increase the network lifetime.

The separate defense system by using genetic algorithm is used that detect and recover the node, since affected node is out of network, no network jam occurs. The node energy is utilized efficiently as the recovery is managed in such a way that the overloaded condition occurs due to which they get time to recover from low energy state.

Finally experiments show that proposed algorithm utilizes energy efficiently and increase network lifetime.

REFERENCES

[1] Y. Cho and G. Qu, Y Wu. “Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks”, IEEE CS Security and Privacy Workshops 2012.

[2] Pramod D Mane, Prof. D.H.Kulkarni,” Watchdog Three-Tier Technique to Secure Wireless Sensor Network”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) , 2013, 751-754.

[3] Shaila K et al. “Probabilistic Model For Single And multi-sensing Intrusion Detection in Wireless Sensor Networks”, IOSR Journal of Computer Engineering, Volume 16, Issue 1, Ver. IX Feb. 2014.

[4] K.Q. Yan, s. c. Wang, S.S. Wang and C.W. Liu, “Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network”, IEEE, 2010.

[5] Mr. Ansar S, Prof. Pankaj K, Prof. Hitesh Gupta, “Hybrid Intrusion Detection for Anomaly & Misuse Attack using Clustering in Wireless Sensor Network”, IJARCET, Volume 2, Issue 11, November 2013.

[6] Sneha Dhage, Purnima Soni, “Intrusion Detection and Fault Tolerance In Heterogeneous Wireless Sensor Network: A Survey”, International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014.

[7] Hamed Khanbabapour , Hamid Mirvaziri, “An Intelligent Intrusion Detection System Based On Expectation Maximization Algorithm in Wireless Sensor Networks”, ICT, Volume 4, January 2014.

[8] Joseph Rish Simenthy, K. Vijayan, “Advanced Intrusion Detection System for Wireless Sensor Networks”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Special Issue 3, April 2014.

[9] Ravi Kumar, Sunil Kumar, Prabhat Singh, “Enhanced Approach for Reliable & Secure Wireless Sensor Network”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

[10] Satvir Singh, Meenaxi, “A Survey on Energy Efficient Routing in Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013

[11] K. F. Man, K. **S.** Tang, and **S.** Kwong, "Genetic Algorithms: Concepts and Applications", IEEE Transactions on Industrial Electronics, Vol. 43, No. *5*, October 1996.

[12] Georges R. Harik, Fernando G. Lobo, and David E. Goldberg, "The Compact Genetic Algorithm", IEEE Transactions on Evolutionary computations, Vol. 3, No. 4, November 1999.

[13] B.Baranidharan, B.Shanthi, "A Survey on Energy Efficient Protocols for Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887), Volume 11– No.10, December 2010.

[14] Ali Ghaffari, "An Energy Efficient Routing Protocol for Wireless Sensor Networks using A-star Algorithm", Journal of Applied Research and Technology, Vol.12, August 2014.

[15] Zahra Rezaei, Shima Mobininejad, "Energy Saving in Wireless Sensor Networks", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.1, February 2012.

[16] Rathna. R and Sivasubramanian. A, "Improving Energy Efficiency In Wireless Sensor Networks Through Scheduling And Routing", International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No.1, January 2012.