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

IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.230 – 235

IMPROVING ENERGY EFFICIENCY AND SECURENESS IN WSN USING BIST

[1]P.Gokila, [2]R.Rajesh

[1]B.E Student, Department of Computer Science and Engineering, [2]AP/CSE

[1] gokilamaha@outlook.com, [2] mtechrajeshr@gmail.com

IFET College of Engineering

Abstract*— Sensor networks collect large amounts of data that can convey important information for critical decision making. The node in a wireless sensor network is a tiny device that is used to capture environment information. Sensor devices are used to capture temperature and pressure details from the environment. Sensors are used to cooperatively monitor physical or environmental conditions. When In network data aggregation is performed there is significant reduction in the amount of communication overhead and energy consumption in a large WSN. The data aggregation plays a important role in WSN to reduce energy consumption that occurs due to excessive communication. In this project, the new approach is introduced that is Built-in-Self-Test (BIST), RC-6 algorithm and Aggregation method is considered which will perform secure data aggregation.

***Keywords*— secure transmission, energy consumption life time, clustering, BIST, wireless sensor network.**

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance .In addition to one or more sensors, the each node in a wireless sensor network is typically equipped with a radio transceiver or other wireless communications device, a small Micro controller, and an energy source, usually a battery for the entire function in network. Size and cost constraints on sensor nodes result in corresponding constraints based on the several factors such as energy, memory, computational speed and bandwidth. A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor in the WSN supports a multi-hop routing algorithm. In computer science and telecommunications area, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year. A number of data mining algorithms have been recently developed that greatly facilitate the processing and interpreting of large stores of data. The sensors in Wireless Sensor Networks (WSNs) must have long network lifetime because it has limited power and communication capabilities. There should be a Minimum energy consumption in WSN for increasing the network lifetime is main aim in Wireless Sensor Networks. To achieve this goal, a data aggregation technique is introduced. All Wireless sensor networks have small sensor nodes which are deployed for sensing, data processing and aggregation, and communicating components. The data aggregation plays an important role in WSN to reduce energy consumption that occurs due to excessive communication.

Data aggregation is useful to improves The lifetime of nodes by eliminating the redundant data transmission. The Data transmission follows a multi Hop fashion technique in which each Node sends its data to the neighbor node nearer to sink. Cluster is formed in network with various sensor nodes. There is one cluster head for each clusters . From the several clusters the data is transmitted to the base station through the cluster heads. The security must be maintained in the wireless sensor networks to deliver the data correctly and confidentially.

Requirements needed for security:

The security is needed for WSN because of following reasons:

Data confidentiality –To ensure that the data content of the message should not be leaked to the unauthorized receiver. Some secure data aggregation techniques provide this property using hop-by-hop basis in which any aggregator node needs to decrypt the received data that is before applying the aggregate function on it and then encrypt the aggregated data before transmitting it directly to the base station(BS) or to the higher level aggregator. the received encrypted data.

Authentication – Enables the sensor node to ensure the identity of the peer node which it is communicating with the network. A compromised node can launch attack in which it may be end data under several fake identities in order to corrupt the aggregated data.

Availability – To guarantee the survivability of the network services against Denial-of-Service attacks. The attack aims at an aggregator can make some part of the network losses its availability because the aggregator is must.

II. RELATED WORK

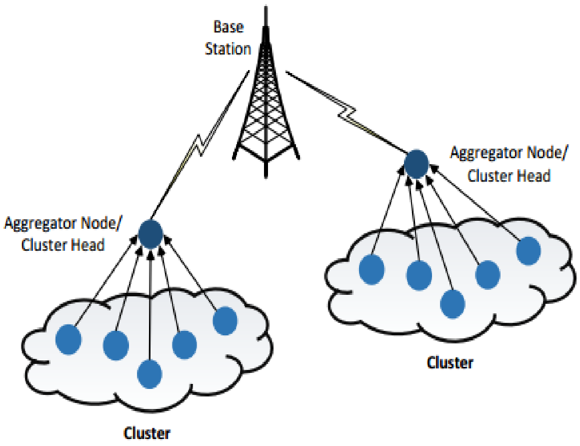
There are a number of papers investigating how energy efficiency and security can be applied in WSNs. We consider a canonical task in wireless sensor networks the extraction of information about environmental features and propose a multi-step solution that is fault-tolerant, self-organizing and energy-efficient. It explicitly take into account the possibility of sensor measurement faults and study a distributed algorithm for detecting and correcting such faults, showing through theoretical analysis and simulation results that 85-95% of faults can be corrected using this algorithm even when as many as 10% of the nodes are faulty. The accuracy of the security is less in this paper.

Wireless sensor network uses the data fusion centers to collect and process the data values from the sensor nodes. Compressive data collection methods are used to handle the data collection under faulty and noisy environment. Data collection scheme is improved with Bayesian approach to predict projections. Scheduling schemes are integrated with the system to increase the lifetime of the network. When The system achieves high computational efficiency, Communication load is reduced by the compressive data collection scheme. Efficient fault and noise handling scheme is provided in the sensor data collection process. Data collection accuracy is improved in the pattern based model.

In the another work, As sensor networks are being increasingly deployed in decision-making infrastructures such as battlefield monitoring systems and SCADA(Supervisory Control and Data Acquisition) systems, making decision makers aware of the trustworthiness of the collected data is a crucial. To address this problem, proposed a systematic method for assessing the trustworthiness of data items. This approach uses the data provenance as well as their values in computing trust scores, that is, quantitative measures of trust worthiness. To obtain the trust scores, proposed a cyclic framework which well reflects the inter-dependency property: the trust score of the data affects the trust score of the network nodes that created and manipulated the data and vice-versa.

III. CLUSTER FORMATION

In a network, a node is a connection point, either a redistribution point or an end point for data transmissions. In general, a node has programmed or engineered capability to recognize and process or forward transmissions to other nodes in a network. Number of nodes is fixed in the program. Nodes are configured with specific parameters of a mobile wireless node. After creating the nam file and trace file, we set up topography object. Forming a cluster of nodes in a network. There is cluster head for each cluster with a single Base station. The data from each cluster is transmitted to the base station via cluster head.



System architecture

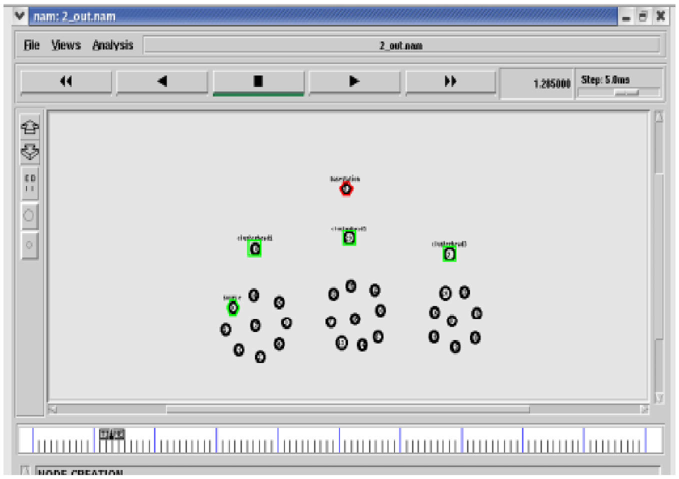
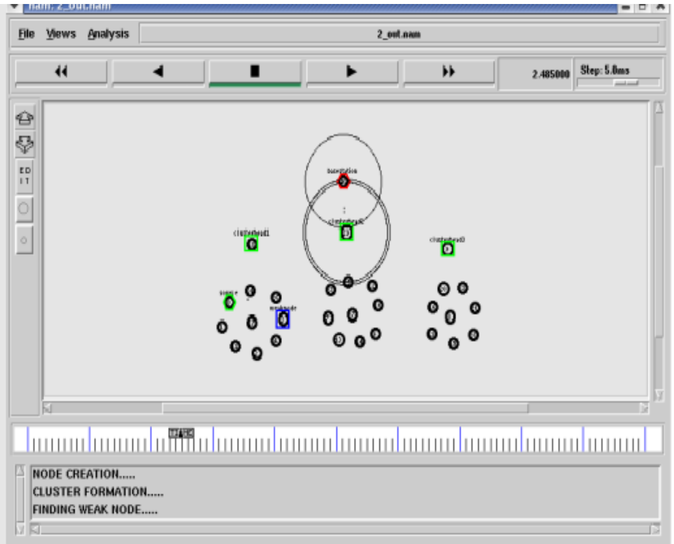


FIGURE:1 cluster formation

IV. FINDING WEAK NODE

To transmitting the data in networks have the possibility that more than one node will transmit at the same or overlapping time. This event is referred to as a collision. The messages sent by the transmitting nodes are corrupted. The receiving nodes will receive (in most but not all cases) random data. In networks, the transmitting node must ensure that the network is quiet prior to transmitting, and in addition for transmitting nodes to detect overlapping transmissions. This type of collision can be avoided using Buit In Self Technique and data aggregation.

In the figure.2 the weak node is found in the cluster and it is marked with blue colour. The green colour specifies the cluster head and the red colour specifies the base station.



NODE CREATION.....
CLUSTER FORMATION.....
FINDING WEAK NODE.....

Figure.2 finding weak node

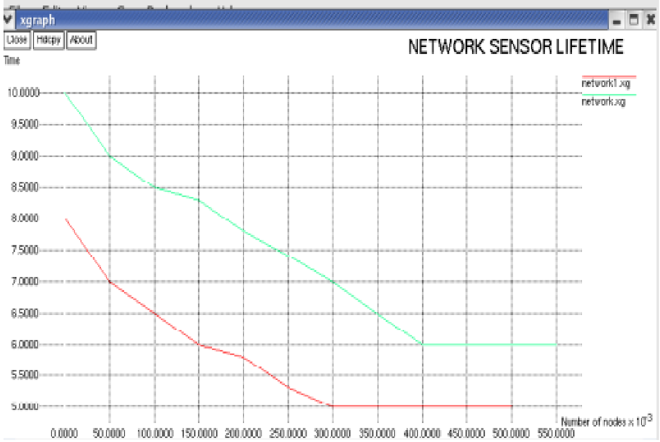
The node which performs collision or the node which transmits the data to the unknown network is marked as a weak node. The IF condition is checked to know whether the data is authorized or not. The node which transmits the unauthorized data is found out using the condition. When the weak node is found out, the data transmission path is not allowed through the weak node. When the collision is avoided, the communication is reduced in the large WSN. Hence the energy consumption by the nodes in the network is reduced. Thus it improves the life time of the nodes in the Wireless Sensor Network.

V. SECURE TRANSMISSION

After the weak node is found, security is provided to that node using RC6 algorithm. It is a block cipher technique. It performs both the encryption and decryption methods in the data transmission. When we apply this technique the authorized data is secured from the weak nodes. The packet loss is also minimized. Thus the throughput of the network is increased.

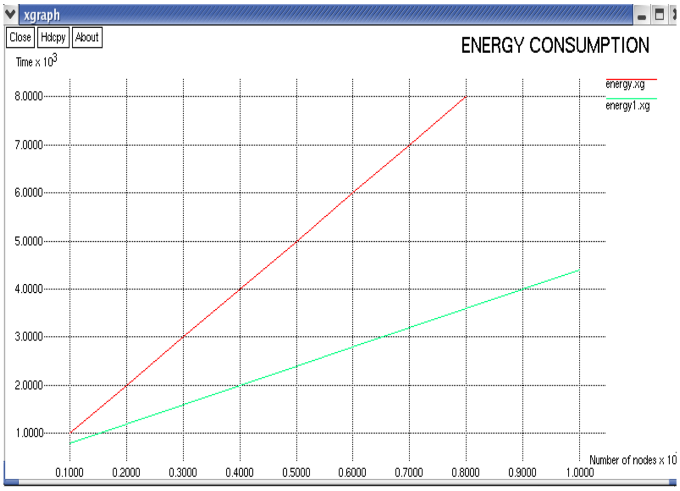
VI. RESULT ANALYSIS

The performance graph shows the lifetime, energy consumption, throughput and packet loss in the wireless sensor network. When we look at the lifetime graph, there is a increase in the lifetime of the node when compared to the existing system.



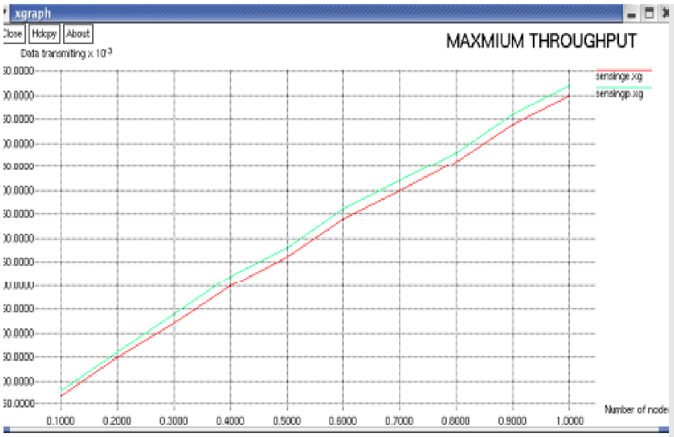
Lifetime graph

Likewise in the energy consumption graph, the energy consumption is high in the existing system but it is reduced in this system. The parameters taken for the performance analysis are number of nodes in the network and time taken to to transmit the data from one node to another node.



Energy consumption graph

At the same the packet loss is reduced and throughput is increased. The red line in the graph shows the performance of the existing system. The green line shows the performance of the this system.



Maximum throughput graph

VII. CONCLUSION

Thus this system will detect the weak nodes in the wireless sensor network. And provide security to the nodes for the better data transmission. It leads to the improvement of life time of the nodes and reduced energy consumption by the nodes. So it will be an efficient network for the several applications which using the WSN.

REFERENCES

[1] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," Comput. Netw., vol. 53, no. 12, pp. 2022–2037, Aug. 2009.

[2] L. Wasserman, All of statistics : a concise course in statistical inference. New York: Springer.

[3] Jøsang and J. Golbeck, “Challenges for robust trust and reputation systems,” in Proceedings of the 5 th International Workshop on Security and Trust Management, Saint Malo, France, 2009

[4] Y. Yu, K. Li, W. Zhou, and P. Li, “Trust mechanisms in wire-less sensor networks: Attack analysis and counter measures,” Journal of Network and Computer Applications, vol. 35, no. 3, pp.867 – 880, 2012, ¡ce:title¿ Special Issue on Trusted Computing and Communications¡/ce:title¿.

[5] Sankardas Roy, Member, IEEE, Mauro Conti, Member, IEEE, Sanjeev Setia, and Sushil Jajodia, Fellow, IEEE, “Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker’s Impact”, IEEE Transactions on information forensics and security, vol. 9, no. 4, april 2014.

[6] Sk Md Mizanur Rahman, Mohammad Anwar Hossain, Maqsood Mahmud, Muhammad Imran Chaudry, Ahmad Almogren, Mohammed Alnuem, Atif Alamri. “A lightweight Secure Data Aggregation Technique for Wireless Sensor Network”,IEEE International Symposium on Multimedia- 2014.

[7] Mohsen Rezvani, Student Member, IEEE, Aleksandar Ignjatovic, Elisa Bertino, Fellow, IEEE and Sanjay Jha, Senior Member, IEEE, “Secure Data Aggregation Technique for Wireless Sensor Networks In the Presence of Collusion Attacks”, IEEE Transactions On Dependable and Secure Computing (TDSC)2014.

[8] Chun Tung Chou, Aleksandar Ignjatovic, and Wen Hu, “Efficient Computation of Robust Average of Compressive Sensing Data in Wireless Sensor Networks in the Presence of Sensor Faults” IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 8, August 2013.

[9] A. Ignjatovic, C.T. Lee, P. Compton, C. Cutay, and H. Guo, “Computing Marks from Multiple Assessors using Adaptive Averaging,” Proc. Int’l Conf. Eng. Education (ICEE), 2009.

[10] W. Bajwa, J. Haupt, A.Sayeed, and R. Nowak, “Joint Source-Channel Communication for Distributed Estimation in Sensor Networks,” IEEE Trans. Information Theory, vol. 53, no. 10, pp. 3629- 3653, Oct. 2007.