International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Energy Efficient Secure Routing using Clustering Approach in HWSN

Shani Verma[1], Maya Shelke[2]

[1]Department of Computer Science and Engineering, Symbiosis Institute of Technology,
Symbiosis International University, Near Lupin Research Park, Gram: Lavale, Tal: Mulshi, Pune 412 115

[2]Assistant Professor, Department of Computer Science and Engineering, Symbiosis Institute of Technology,
Symbiosis International University, Near Lupin Research Park, Gram: Lavale, Tal: Mulshi, Pune 412 115

Abstract: ***In this paper we have addressed the problem of prolonging life time of a sensor network and securing it with the use of clustering algorithm and intrusion detection system. Prior works suggests that clustering plays dominant role in the death of first node and aggregation plays important role in the death of the last node. We have explore this nature of routing algorithm in present work. In present scenario wireless sensor network have becoming a popular media of monitoring and data gathering. Wireless sensor networks have limited amount of power in it, so it is important that it must be utilized effectively and efficiently. Studies have shown that heterogeneity of sensor node also helps to improve life time of a network .This paper focuses on the improvement in energy utilization with the help of clustering algorithm and results are deduced from them.***

Keywords: Wireless sensor network, Clustering, Routing, Aggregation.

1. Introduction

Wireless sensor networks are becoming popular because of their vast capability to survive in adverse conditions. Wireless sensor network is composed of small wireless sensor nodes. They are deployed in a large numbers(few hundreds to thousands) to monitor an area for various purposes. Wireless sensor networks are: a large number of small sensing self-powered nodes which gather information or detect special events and communicate in a wireless fashion, with the end goal of handing their processed data to a base station. Sensing, processing and communication are three key elements whose combination in one tiny device gives rise to a vast number of applications. Sensor networks provide endless opportunities, but at the same time pose formidable challenges, such as the fact that energy is a scarce and usually non-renewable resource[1].

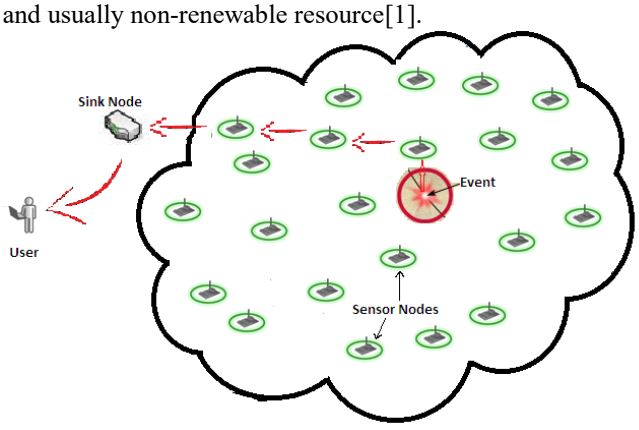

Figure 1: Typical Wireless Sensor Network

Sensor network can be of two types: Single hop and Multi hop. In case of single hop sensor node directly communicates with the sink node or base station. Figure 1 Shows a Multi hop network configuration in which sensor node passes the data to next node. It reduces the energy consumption because they have to transmit to smaller distance. The researchers are attracted towards the idea of Wireless Sensor Networks (WSNs) due to wide range of potential applications that it offers such as biological detections, home security, environment detection and monitoring, habitat monitoring etc.[3].It is relatively younger stream and it has open issues for research as in network processing, routing and transport, Security and reliability[2].

Routing is the process of moving a packet of data from source to destination. Routing is the process of selecting best path in network. Routing helps to deliver a packet from source to destination. It can play an important role in wireless sensor network, because if we use efficient routing technique to pass on the data it can significantly cut out the power usage which would result in the expansion of lifetime of a network. In the context of computer science, security is the prevention of, or protection against, 1)access to information by unauthorized recipients, and 2)intentional but unauthorized destruction or alteration of that information.
The rest of the paper is organized as, in section 2 we have described related work along with our approach. Section 3 gives the information about implementation of the system. In Section 4 we have discussed the results and in section 5 we have concluded our work with future outline.

2. Related Work

In this work we have focused on network layer of the wsn, so everything would be reference on the basis of that. We will be discussing about topology, routing technique & security. As we all know topology always plays an important role when building a network. Topology-control algorithms have been proposed to maintain network connectivity while reducing energy consumption and improving network capacity. The research in topology construction and connectivity has been approached independently along two paths. In one path, researchers aim to determine critical conditions on network parameters to ensure network (k-

)connectivity with high probability. Of particular interest is how these critical conditions scale as the number of wireless devices increases. In the other path, researchers aim to devise distributed algorithms to enable each node to choose its own transmission power in order to minimize the total transmission power of all wireless nodes, while maintaining (k)connectivity[4]. Tree topology has been considered in this work.

Routing plays important role in a network for delivering the packets from source to destination via best path available. There are numerous routing techniques are available for wsn's. Our focus is in the hierarchical routing technique of network structure based routing. In hierarchical approach there would be two types of nodes would be their first is cluster head and other is sensor node. SN's would be responsible for data collection and forwarding. CH's would be responsible for sending sensed data to the sink node or base station. In this simulation we have used two algorithms Hybrid Energy Efficient Distributed algorithm & Data routing in network aggregation algorithm.

Security is always been an area of concern when designing any system. In computer science security is prevention of access of data by unauthorized person and manipulation of data by unauthorized person. In WSN's we can deploy traditional security schemes because of it's size and power limitation. WSN's also require security because of what kind of area they are monitoring, it is possible they might be collecting sensitive information. In our work we have focused on attacks of network layer and detection of those attacks as well as prevention form them. We have devised voting based intrusion detection system which will identify and provide alternative paths from packet drop attack as well as bad mouthing attack. This was the detection mechanism in place for prevention of attack purpose we have localized encryption and authentication protocol which would safe guard from Sybil and Wormhole attack.

3. Proposed System

In the proposed approach, there are two main aims 1) Increase the lifetime of a network, for which existing and proposed both systems are adopting clustering approach as we have discussed the benefit of this previously. To full fill our first aim, we are going to replace Hybrid Energy Efficient Distributed algorithm with Data Routing In Network Aggregation algorithm. 2) Increase the security of the system. For security we have used Low Encryption and Authentication Protocol with slight modification.

For implementation of above objective we have used java language, along with jfreechart for graph generation and GUI has been developed with java swing controls. Which fulfills above mentioned aims. Flow of simulation has been mentioned below:

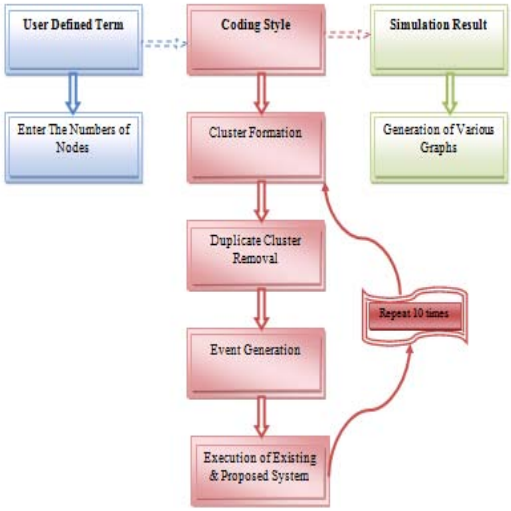

Figure 3: Simulation Environment

In our system we can incorporate maximum of 3000 nodes. They are stored in M x M matrix form. For example if a user enters the node # as 10.Then execution is going to take place in following manner: generate_topology is going to generate 11 x 11 node area. Then routing table is going to generated, then cluster_formation is going to take place, then duplicate clusters would be removed,then randomely generate_event is going to execute and generate events, then events are going to be reported to the sink node with the different routes. This process is going to repeat it self for 10 times so that graph plotting can be done(i.e. 12 x 12,13 x 13 so on). In the coming section we will discuss and show the results obtained by the numbers of node 10 i.e. 11 x 11.

4. Results

In this simulation four graphs have been generated which produces the difference between existing system and proposed system. Comparison has been done on the basis of energy depleted, number of node monitored by sink node, number of data aggregation points & security improvement.

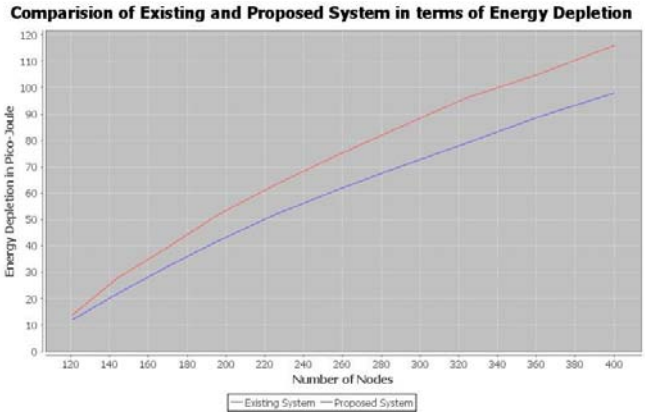

Figure 4.1: Comparison on the basis of Energy Depletion

The graph indicates that the proposed system consumes significantly less energy as compared to the existing system because in the existing system only the clustering approach was adopted but proposed system also incorporates the benefits of the aggregation also.

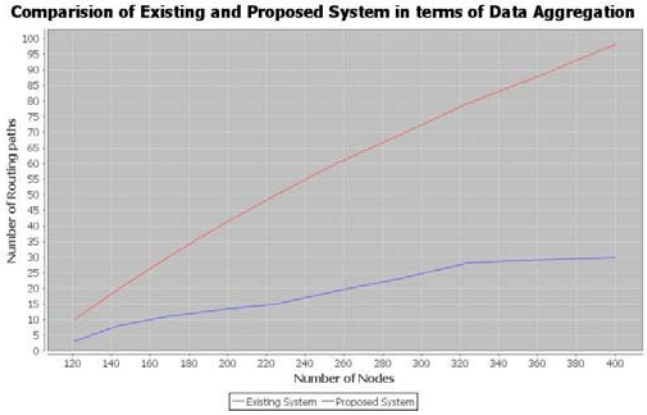

Figure 4.2: Number of times Data Aggregated

In the graph we have number of nodes in x-axis and number of routes in y-axis. As observed from the graph that the number of routes have been significantly reduced in proposed system because it aggregates the data into the existing route. Which would result in the saving energy of the other route node hence the life time of the network is going to increase.

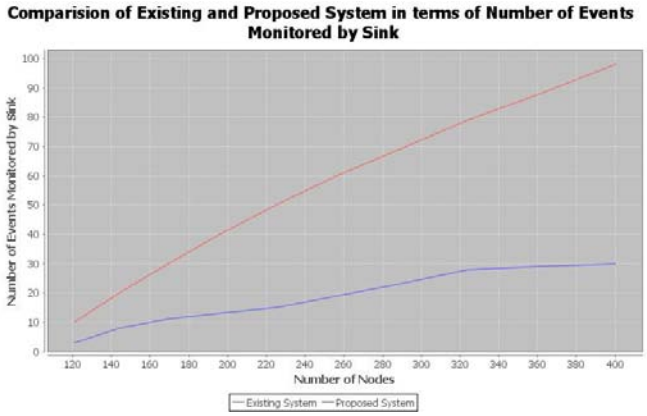

Figure 4.3: Sink Node Monitoring Status

Here x-axis shows number of nodes and y-axis shows the number of event (i.e. data) monitored by sink node. In case of existing system number of events are higher as compared to the proposed system, that's because aggregation is added in the proposed system.

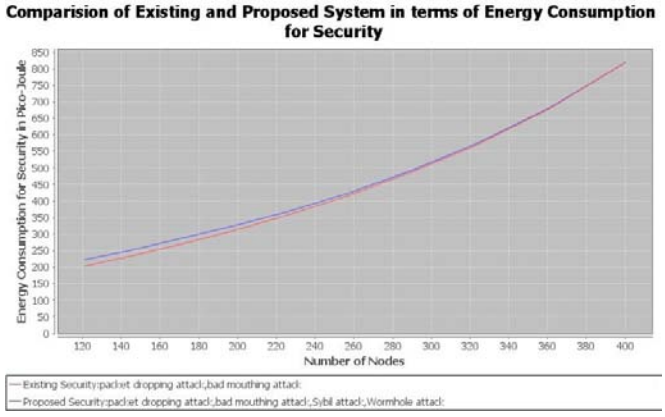

Figure 4.4: Security Graph of the system

In the x-axis number of nodes are plotted and in the y-axis the energy has been plotted. Because we have taken small number of node i.e 10 so the energy consumtion for security purpose seems to be similar to the existing system but as the network size increases the energy consumption increase, because we are using four keys to ensure security of the system. Therefore we can say that if we want to increase the security than we have to find out much more efficient security mechanism which should provide better security with less power consumption. This show that if we are going for security than the energy consumption is going to increase.

5. Conclusion

Wireless sensor network are the future generation networks. It's relatively less explored area because of cost, lack of protocols etc. But in upcoming time with the boom of Internet of Things(IOT) it's going to be very powerful network. So it's important to identify potential area where wsn can be deployed for benefit of human being. Our results shows that if we incorporate clustering & aggregation it can improve the life time of network. We also observed that as we tried to increase security in the system its energy consumption is going to increase, hence decreasing the life time of network.

In future experimental setup can be conducted for any specific application. exploration of other phenomena like trust & reputation in the system can be done. As in the present scenario everything is moving towards cloud, so it is potentially possible to move these data or information of wsn over cloud for further decision making.

References

[1] Daniele Puccinelli and Martin Haenggi,"Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing",IEEE CIRCUITS AND SYSTEMS MAGAZINE THIRD QUater 2005.
[2] Dirk WESTHOFF, Joao GIRAO, Amardeo SARMA,"Security Solutions for Wireless Sensor Networks",Nec Tech Journal vol 1/No.3 2006.
[3] I.F.Akyildiz,W.Su, Y.Sankarasubramaniam, and E. Cayirci.2002. Wireless sensor networks: A survey. IEEE Communications Magazine, 40(8):102–14.
[4] Hou, J. C., Li, N. and Stojmenović, I. (2005) Topology Construction and Maintenance in Wireless Sensor Networks, in Handbook of Sensor Networks: Algorithms and Architectures (ed I. Stojmenović), John Wiley & Sons, Inc., Hoboken, NJ, USA. doi: 10.1002/047174414X.ch10.
[5] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanism for large –scale distributed sensor networks", In Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 62-72, New York, NY, USA, 2003, ACM Press.
[6] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," IEEE Trans. Mobile Comput., vol. 3, no. 4, pp. 366–379, 2004.
[7] Leandro Aparecido Villas, Azzedine Boukerche, Heitor Soares Ramos, Horacio A.B. Fernandes de Oliveira, Regina Borges de Araujo, and Antonio Alfredo Ferreira Loureiro "DRINA: A Lightweight and Reliable Routing

Approach for In-Network Aggregation in Wireless Sensor" Networks,IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 4, APRIL 2013.
[8] Jaydip Sen ,"A Survey on Wireless Sensor Network Security" International Journal of Communication Networks and Information Security (IJCNIS) Vol. 1, No. 2, August 2009.
[9] ALGORITHMS AND PROTOCOLS FOR WIRELESS SENSOR NETWORKS, WILEY SERIES ON PARALLEL AND DISTRIBUTED COMPUTING Editor: Albert Y. Zomaya
[10] Hamid Al-Hamadi and Ing-Ray Chen," Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks"

Author Profile

Shani Verma received the B.E. degree in Computer Science Engineering from Disha Institute of Management and Technology in 2010 and M.Tech degree in Computer Science Engineering from Symbiosis Institute of Technology in 2014, respectively. Area of interest is computer networks, IOT, Big Data, Data Mining, Cyber security and Wireless Sensor Network.