International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Configuring the Topology of Wireless Sensor Networks against Node Based Attacks

M. Hari Kishan Rao, M.Pushpalatha

Abstract: ***The design of topology of wireless sensor networks is critical aspect in real world networks. Configuring the network topology according the attacks of the network is the solution to several node based attacks. To counter those attacks, an approach is proposed for wireless sensor networks. We propose to use networks that are free to scale and configurable according to the priority of the node. The parameters like throughput, efficiency, load balance should be exploited to make sure the connectivity of the network. The node based attacks concentrating on functional nodes in the network should be addressed and transmission of data should not be halted even after multiple attacks. The robust network should be built by applying the strategies to counter the node failures and connectivity of the network remain unaffected.***

Keywords: Scale free Networks, Node attacks, Topology control, Lifetime of the network, Wireless Sensor Networks.

I. INTRODUCTION

Wireless sensor Networks are sensor node combinations strongly connected together without fixed infrastructure. These nodes are deployed in many locations to check the environmental parameters and monitor the changes in it. The sensor nodes consist of a unit for processing and limited power. They can be used in multiple fields and purposes in army, medical and other fields. The use of these sensor nodes are highly appreciated when we use them to monitor synchronizations, processing, storing etc. The operations like buffering, bridging of Ethernet network from wireless sensor network can be done by combining multiple autonomous systems. The lifetime of the network is very dependent on the routing and some protocols for network communications. The importance that Wireless sensor networks provide is vast so it is bound to have threats like data theft. The cyber-attacks are becoming common day by day, the developed system of nodes should be able to tackle, withstand the attacks and the transmission of the data should not be interrupted.

The networks which are free to scale can be used for modelling the homogeneous network topologies [1]. The idea of the scale free network can solve random attacks as they are not concentrated on functional nodes mostly [4]. The nodes in the network will have degrees very similar range. The distribution of degree between the nodes is crucial for holding the network for longer time [2][3].The arrangement of similar degree nodes together can make the network change its topology with ease compared to dissimilar degrees[5].

II. SCALE FREE NETWORKS

The Random networks have equal connections to the node and can be scaled based on the distribution of links. But, the actual picture is somewhat different when connected, it will have many nodes deserted and their connection may not make sense always[6]. The network connectivity will be an issue in the random network as we keep on adding new nodes in the network. The delay have to be addressed before it starts affecting the efficiency of the algorithm. The real world networks need preferential connectivity and not randomly connecting the nodes in the network because newly integrated node might have importance than other nodes in the network and arrangement should be done accordingly. The scale networks give us the preferential connectivity of the nodes. The study of the scale free networks keeps inspiring us to make topologies with these method as it follows power law of distribution. The few nodes in between the network having highest number of links are called hubs. The concept of hubs is very important while discussing about the scale free networks. The attacks on the networks have different motives and exploitation will be done if our network is not robust against the attacks[7]. The nodes in the network are added one by one with some objective defining the topology. The figure is showing the hubs in red which are having many connection in the network. There is no limitation of distance between the connections in the network and can reach to any node if required

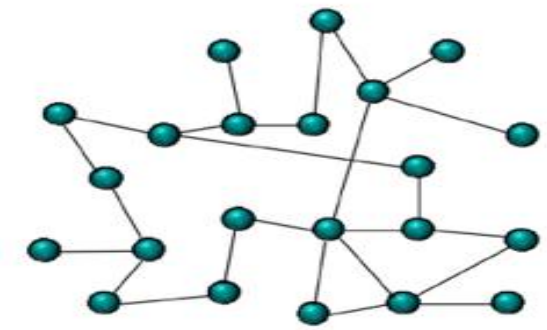

Figure 1- Random Network.

Manuscript published on 30 September 2019
* Correspondence Author
M. Hari Kishan Rao*, Department of Computer Science and Engineering, SRM University, Kattankulathur, Kancheepuram District, Tamil Nadu -603103
M.Pushpalatha, Department of Computer Science and Engineering, SRM University, Kattankulathur, Kancheepuram District, Tamil Nadu -603103 E-mail: harikishanm123@gmail.com

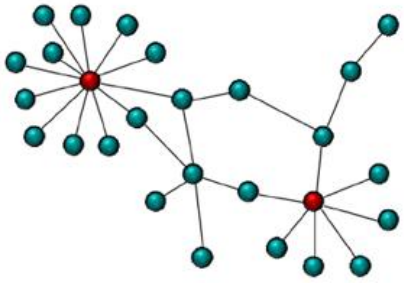

Figure 2- Scale Free Network

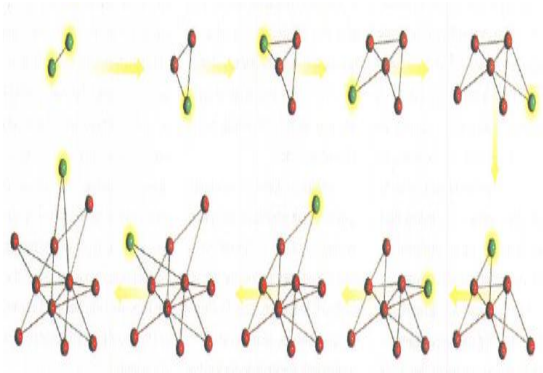

Figure 3- Scale Free Network building.

The Figure 3 provides basic design of scale free network. The nodes red in colour are existing nodes and nodes in green colour are recently added additional node to the network. The Hubs within the network can dominate the network with basic mechanisms like growth and discriminatory attachment. [7].

III. RELATED WORK

Zhenget al[17] planned two vigorous sans scale organize topologies, the straight development advancement demonstrate and the quickened development advancement show. They concentrated on genuine circumstances, for example, the expansion or expulsion of hubs and the remaking of edges. They exhibited tuneable coefficients to adjust the availability and vitality utilization of a scale-free arrange topology. These creators considered both the vitality parity and transmission execution, which builds the information overhead amid the demonstrating procedure. In this way, an exchange off arrangement between the scale free property and demonstrating overhead is required. In sans scale arranges, few hubs have extremely high degrees, which renders these systems powerless against pernicious assaults. At the point when a hub with high degree falls flat, the expansive number of edges occurrence on it are evacuated in the meantime. The whole system topology is along these lines immediately divided. Subsequently, the fundamental reason for this examination was to improve the vigour of scale-free arranges in WSNs against malignant assaults. The proposed system introduces the concept of edge swapping when the node is attacked and not letting the system disconnected[18].

IV. ATTACKS ON THE NETWORK

The algorithm proposes the efficient way to tackle the random and malicious attacks on the network. These attackers do have different motives to break the networks for their needs. The Random attacks are attacks which are carried out on random nodes in the network. Since in the scale free topology we designed only has very less number of functional nodes and majority of random nodes with less degree. The nodes attacked by the random attacks are mostly non-functional nodes and they cannot disconnect any network. The scale free property of the topology successfully avoids the random attacks on the network. The malicious attacks are the attacks which are carried out on only functional nodes of the network. The strength of the network will be questioned by the attacker with these kind of attacks. The topology should be designed in such a way that though the attacks are targeting the functional nodes, we should efficiently change the dependency on the particular node and form a different path to continue the data transmission. Thus, the network will remain connected even after the attack.

V. NETWORK TOPOLOGY

The topology of the network plays a deciding role in efficiency and lifetime of the network[9]. Defining the topology of the network is not enough in the present real world scenario as the attacks on the networks keep increasing day by day. We should be efficiently configuring the topology to be robust against attacks[10]. The failure of any node in the network should not affect the functionality of the network. The topology should be efficient to change its structure and all the nodes should be able to connecting to different nodes when required[8]. The discovery of the nodes beside them will be done by sensor nodes themselves with their transmission power. The nodes can be grouped as a cluster to make sure the nodes know whom they need to communicate and efficiently make the transmission. The nodes inside the network with high energy are expected to run for longer periods[11]. These nodes should be used efficiently for key functional arrangements. The nodes lacking the power should be made less dependent progressively and finally not dependent at all before failure[12]. The energy can be saved by selecting the shortest path in the topology from source to destination and carry out transmission. Many mathematical formulas should be employed to find the aggregation of data[13][14][15] and others to measure the lifetime of the network.

VI. IMPLEMENTATION

The algorithm proposes the way of surrounding the functional nodes with many nodes with similar degree and efficiently shifting jobs between them during congestion. The topology is created in such a way that created nodes should be communication range of others as it will ensure the connectivity to the other nodes when required. We should indirectly provide options to the nodes to connecting multiple nodes and shifting the operations. The swapping of the edges is done when there is packet loss in the network. The degree difference operation between the nodes should be tabulated and every node should have the idea of other nodes capabilities. This will make sure the transition between the nodes is carried out without any problem.

There will be several connection methods for the nodes based on the degree difference operations results. The figure 4 shows three connection methods between the nodes.

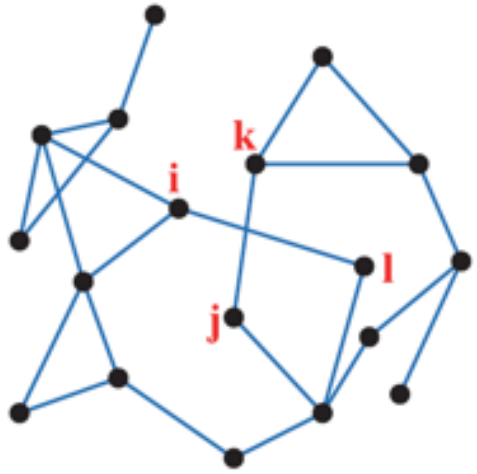

Figure 4(a) - Connection Method 1

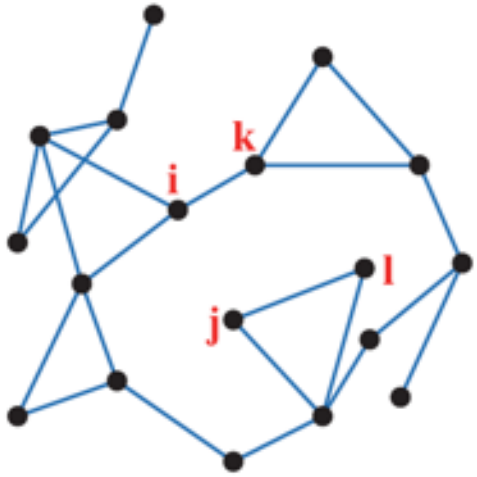

Figure 4(b) - Connection Method 2

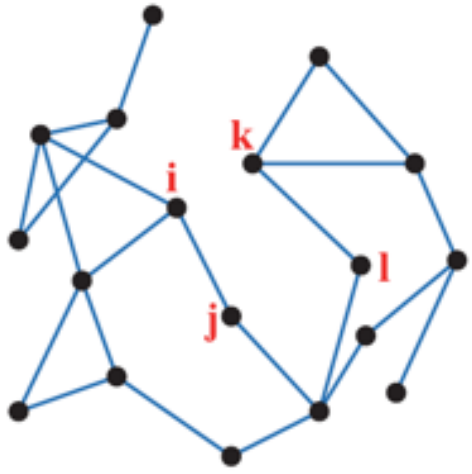

Figure 4(c) - Connection Method 3

The edge can be swapped based on the calculated results of the degree difference operation performed between the nodes. The swapping will only be done if it do not disturb any process that is running prior to the present operation. The pairs tabulated will be helpful for nodes to select between them and select the better one. After carrying out multiple performance analysis, we can integrate a constant along with the degree difference operation particular to area of research.

Module 1: Creation of nodes and Data transmission in the Network

A network is created with finite number of nodes on the plane with different positions on co-ordinate axis. NS3 simulator is used to carry our experiments on networks. The connections between the nodes are established indifferently to facilitate multiple operations between the nodes. The paths are established between the nodes to connect all nodes and allow data transmission efficiently. The communication between the nodes in the network will need agents for sender and receiver to carry out the transmission. The packet loss is assumed to be congestion in the network. The TCP agent and Sink agent will act as sender and receiver in the network. The figure shows the topology formed with eleven nodes created in the network.

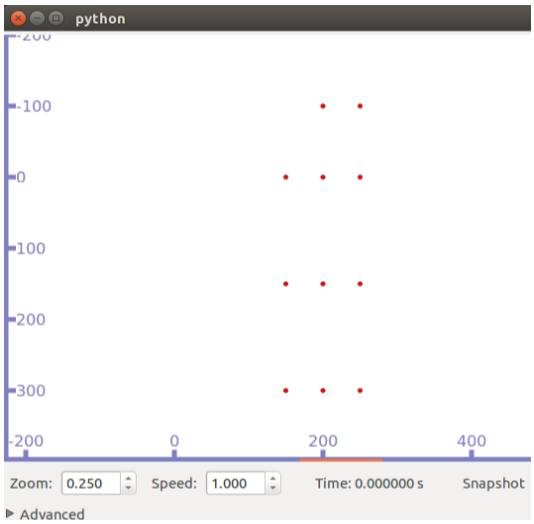

Figure 5 – Module 1

The data transmission is treated as successful only after the sink agent receiving the total packets. The parameters will be calculated to rate the network efficiency. The number of packets sent and received should be equal to verify that there is not congestion or packet loss in the network. The figure 5 shows the connection between the nodes in the network where the data transmission is carried out.

Module 2: Calculation of degree difference between the nodes and attacking the node.

The degree difference operation is an important aspect in knowing the likeminded nodes for each and every node to swap during the packet loss. The nodes can be replaced with other nodes upon failure. Each and every node will have options to choose between the likeminded nodes and make sure the data transmission is not halted. For attacking the nodes and making the network disconnected, the attackers usually chose a functional node that connects between the networks or a key node in carrying out the data transmission. The node will observe the congestion in the network and then start shifting its functions to other nodes which are have having similar degree. The edge swapping concept will be performed and edge selected will be successful only if the other functions are not halted. The algorithm monitors all the operations and makes sure network connectivity.

The figure 6 shows the node with vertical line in red colour is attacked to make the network disconnected. The packet loss is observed at the sink node to confirm the congestion.

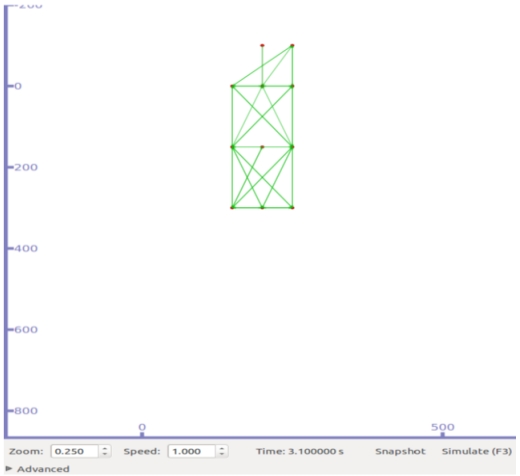

Figure 6 – Module 2

Module 3: Configuring topology of the Network:
The results of the degree difference operation for each and every node and internally tabulated and every node should know their likeminded nodes around them for shifting responsibilities. The node which acts as connection between the parts of the network will be attacked and we can observe the packet loss. The responsibilities of the node are transferred to other nodes and data transmission will be continued even after certain node failures are occurred. This process will be continued and energy of each node will be monitored and notified to shift the operations to other nodes. Thus, the objective to be connected can be achieved.

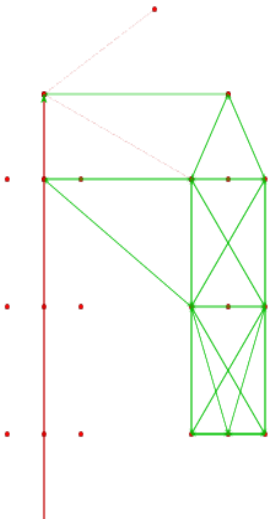

Figure 7 – Module 3

The figure 7 shows the edge swapping and formation of new links between the nodes and dependency is reduced on the attacked node.

VII. PERFORMANCE ANALYSIS

The parameters like throughput, bit error rate, average end to end delay and signal to noise ratio are calculated from the modules developed and data transmission observed. The results are

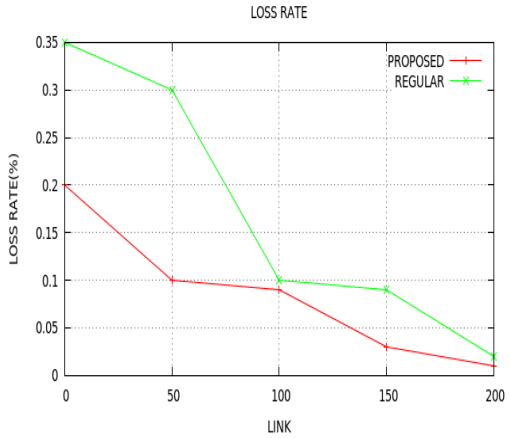

Figure 8 – Loss Rate

The loss rate of packets is compared for the existing and the proposed system and the loss in the data is less compared to earlier versions. The figure 8 illustrates the behaviour of the both the systems.

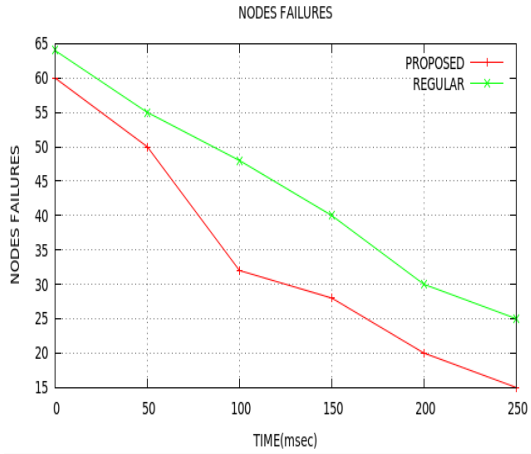

Figure 9 – Throughput

The figure 9 shows the node failures in the network with and without the edge swapping technique. The proposed system proves to be better than the existing one in terms of number of node failures.

VIII. CONCLUSION

The topology control is critical part of remote sensor organizing as a result of edge swapping, the effectiveness of the system can be improved. We can make the system swap the edges to be sufficiently proficient to handle noxious assaults on the nodes. My work goes for improving the lifetime of system by abusing different hub based parameters and making a virtual system on the highest point of the remaining system and permit parcel transmission by numerous ways and re transmission of the lost bundles by re transmission techniques like Fast Re-Transmit(FT) and Re-transmission Timer(RTO) The Work can be broadened to Wireless sensor systems with most extreme correspondence extend. The network angle can be improved with various areas. The Energy of the system is controlled by batteries. The idea of Solar boards to auto energize and enable it to work for longer periods can be acquainted with improve vitality ease of use.

REFERENCES

1. Ze Li and Haiying shen, “A QoS-oriented distributed routing protocol for hybrid wireless networks,” IEEE Transactions on Mobile Computing , March 2014.
2. Reka Albert, Hawwong Jeong and Albert Laszlo Barabasi “Error and attack tolerance of the complex networks”27 July, 2000.
3. Salvatore Scellato, Ilias Leontiadis, C Mascolo, Prithwish Basu “Evaluating the temporal robustness of mobile networks” IEEE Transactions on Mobile Computing ,January 2013.
4. Mingjing Zhou, Jinh Liu “A memetic algorithm for enhancing the robustness of scale-free networks against malicious attacks” Statistical mechanics and applications, Sept 2014.
5. M. E. J. Newman,”Assortive mixing in Networks” Phys. Rev. Lett. **89**, 208701 (2002).
6. Ming-Yang-Wang ,Guang Yu, Da Ren-Yu. “Scale free model for wireless sensor networks” IEEE International Conference on Intelligent Computing and Intelligent Systems.
7. D’Angelo and Stefano Ferretti.”Simulation of scale free Networks” Published in Second International Conference on Simulation Tools and Techniques (SIMUTools 2009).
8. Gengzhong Zheng, Sanyang Liu and Xiaogang Qi “Scale-free topology evolution for WSN’s with reconstruction mechanism”. Published in May 2012.
9. Bharadhwaj and Chandrashekaran, “Low powered Wireless Sensor Networks”, Published in VLSI Design 2001. Fourteenth International Conference on VLSI Design.
10. Tie Qiu, Zhao, Xia, Weisheng, Dapeng. “ROSE: Robustness Strategy for Scale-Free Wireless Sensor Networks”. Published in IEEE/ACM Transactions on Networks in 2017, October.
11. Zaman, Tang Jung, Mehboob Yasin “Energy Efficiency in Wireless Sensor Networks”, Journal of sensors 2016.
12. Volkan Rodpolu Teresa H. Meng, "Minimum energy mobile wireless networks.Published on Aug 1999 in IEEE.
13. TVPadmavathy” Extending Network Lifetime Using Optimized Energy Efficient Cross Layer Module (OEEXLM) in Wireless Sensor Network“,2009 April,
14. Ruihua, Zhiping and Dongfeng, “Analysis of Lifetime of Large Wireless Sensor Networks Based on Multiple Battery Levels”, Published on May, 2008 in SciRes.
15. Xueyan Tang and Jianliang Xu, Extending Network Lifetime for Precision-Constrained Data Aggregation in Wireless Sensor Networks, IEEE Communication Society, 2006.
16. S Lee , B Bhattacharjee, S Banarjee and B Han,“A General framework for efficient Geographic routing in Wireless Networks”, AT&T Labs.
17. G. Zheng, S. Liu, and X. Qi, “Scale-free topology evolution for wireless sensor networks with reconstruction mechanism,” *Comput. Elect. Eng*,vol. 38, no. 3, pp. 643–651, 2012.
18. Y. Jian, E. Liu, Y. Wang, Z. Zhang, and C. Lin, “Scale-free model for wireless sensor networks,” in *Proc. IEEE Wireless Commun. Netw.Conf. (WCNC)*, Shanghai, China, Apr. 2013, pp. 2329–2332.