International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

An Efficient Technique for Enhancing Robustness of Scale-free Wireless Sensor Networks

A.Mary Shiny, A. Chandra Shaker

***Abstract**: In an age where breaches occurrence is precisely numerous, it is essential to safeguard confidential figures including patron records, intellectual property, assessment and enlargement, prospect business plans, and all sorts of confidential facts more proficiently. It is substantial to administer a network to safeguard information. Cyber mugs tear into information systems, accertion in these attacks leads to node deterioration, hence a structure is obligatory which can combat cyber mugs to shield our information nodes in WSNs. To cope with these attacks we adopt an efficient technique for enhancing robustness of scale-free wireless sensor networks. Scale-free networks are not affected much by random thefts but they become defenseless against malicious theft. To overcome this shortcoming this paper presents an enhanced technique , here we have a MAX node which is enclosed with small rate nodes, each MAX node will be highly secured by adopting ROSE algorithm by altering edges keen on to a closed structure to upgrade robustness of a network . This phenomena is achieved by forming a scale-free topology using basic BA model. In this paper, work is done on two operations that is rate diversity and edge value operations, to mold system further vigorous to malicious attacks. System is further encrypted by providing every single node with a private key in a sub network.*

***Index Terms**:Authentication, robustness, scale-free network topology, wireless sensor networks.*

I. INTRODUCTION

WSN's accumulate information from enormous number of nodes suchas source nodes and sink nodes, these are used for collecting, storing and sharing information for analyzing about changes in various parameters like for example pressure, temperature, for traffic control, in home environment etc. By this paper an efficient technique for enhancing robustness of scale-free wireless sensor networks is introduced, here main focus is to make the network vigorous against various attacks by using ROSE algorithm.*Tie Qiu, Aoyang Zhao*[1]proposed ROSE algorithm "ROSE: Robustness Strategy for Scale-Free Wireless Sensor Networks", to form a closed structure and to make system tough.Basically there are two type of network attacks, they are random attacks and malicious attacks.

In random attacks intruder strive to undertake any random node in a network and attacks information of that node, an intruder may even alter information which leads to loss of information. In malicious attacks intruder chooses a high rate node and attacks that high rate node hence all low rate nodes attached to it gets effected therefore link connecting high rate i.e., MAX node and low rate nodes will get disconnected which results in loss of complete information in a network. Complex network theory has two topologies they are small world topology and scale-free topology.*L. Liu,* [2]proposed A topology construct and control model with small-world and scale-free concepts for heterogeneous sensor networks. Small world topology handles with non-consistent networks, whereasscale-free topology handles with consistent networks. In this paper we are considering scale-free network topology.*G. Zheng and Q. Liu* [3] proposed Scale-free topology evolution for wireless sensor networks to obtain this scale-free network topology we consider Barabasi-Albert model. Scale-free topology node dispersion depends on power law distribution. To structure a topology there are few basic necessities like nodes should be in transmission range as it is one of the limitation in wireless sensor networks and there should not be any extra connections between nodes.

By forming multi-hop ad hoc system information of each node and its neighbors is transmitted to central node within its transmission range. If higher degree node fails then network will be diminished and information will be lost permanently.

In this context, this paper presents an efficient technique for enhancing robustness of scale-free network topology that is improving the robustness of a network by forming closed structure along with private key encryption, so that it can withstand malicious assaults. The key contributions of this paper are as follows:

[1] To generate a scale-free network topology to make system vigorous against attacks.

[2] To enhance the network so that it can overcome assaults by performing ROSE algorithm.

Revised Manuscript Received on 30 July 2019.

* Correspondence Author

A. Mary Shiny*, M.Tech degree in Wireless Mobile Communications from G. Narayanamma Institute of Technology and Science, Hyderabad, India.

A. Chandra Shaker, Assistant Professor at Department of Electronics and Telematics Engineering, G. Narayanamma Institute of Technology and Science, Hyderabad, India.

[3] To provide each node with some specific key such that before transmission each node is to be encrypted and data is broadcasted if the key matches between nodes or else node is considered as cyber mug.

The rest of the paper is organized into following sections. Section II provides background and overview is arranged in brief. Section III provides a strategy for constructing a scale-free wireless sensor networks using Barabasi-Albert model and other models in brief. SectionIVprovides a technique for enhancing robustness of scale-free network. Section V provides simulation results. In Section VI we conclude by obtained results and discuss future work.

II. BACKGROUND AND OVERVIEW

In this paper we deal with Barabasi-Albert model (BA model) *A.-L. Barabási, R. Albert*[4] [5] [6]proposed Mean-field theory for scale-free random networks. BA model is used for forming a scale-free network, it has two steps:

1) Node advancement of network which is we can add or remove same degree nodes.
2) Preferential adaptation which is to add nodes to network with same rate distribution as that of existing node.

The only defect is it has some committed transmission range, hence BA model can be applied to only for fixed range. Since the range of operation is fixed, number of nodes in that transmission range will be dense. BA model is basically used to create scale-free network topology. Shortcoming of this system is that since MAX nodes has to perform more computations energy gets depleted hence network collapses and information will be lost. In this paper ROSE algorithm is compared with few other works like Hill Climbing algorithm. *H. J. Herrmann and C. M. Schneider*[5]proposed Onion-like network topology enhances robustness against malicious attacks, which is reshaping network into closed form by a robustness metric R, to make system vigorous and to safeguard information. Drawback of this system is its communication range is limited, its development may avert the algorithm from being active beyond network bounds. P. *Buesser*,[6]proposedoptimizing the robustness of scale-free networks with simulation annealing, it deals with an important aspect of a network capability to withstand fluctuations and failures in its nodes and links, in this algorithm we work in two streams one is simulated annealing as optimistic heuristic, and the other is variant of the optimization process. Drawback of this algorithm is it can be prone to malicious attacks at certain times. Simulation annealing algorithm performs better operation than Hill climbing algorithm.

III. SCALE-FREE NETWORK GENERATION

Generation of scale-free network using BA model as reference model

A) BARABASI-ALBERT MODEL

In this BA model we follow two steps for construction of a scale-free network.

1) Node Advancement:

In below figure Fig a) i, j, k which are three inner dominant nodes of those networks generally central nodes are of high rate, we can notice accession of new nodes to a network here line connections indicates attachment of new edges to net1work. i_1, i_2, i_3 and i_4 are surrounding nodes in network i and same goes for networks j and k.

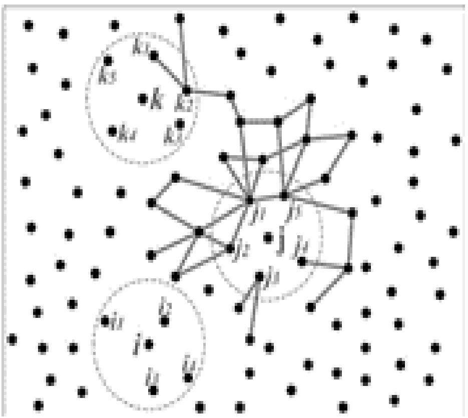


Fig a) Addition of new links and new edge connection

2) *Preferential Adaptation:*

Nodes with same edge value that is nodes with same probability gets connected to form a scale-free network and to make system vigorous against attacks. Connection probability($\prod Local(i)$) for a neighbor is ratio of degree of node to average of total number of newly joined nodes.

$$\prod Local(i) = d_i \,/\, d_j \qquad (1)$$

where$d_i$is degree of new node and d_j is average degree of newly joined nodes.By this growth and preferential attachment steps a scale-free network topology is generated. Drawback of this model is range is limited.

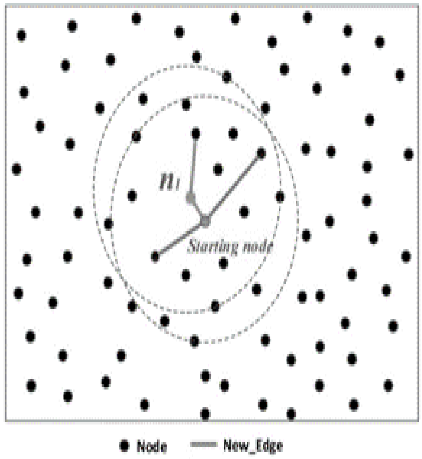


Fig b) Connection of same degree nodes.

Since communication range is limited, this model is designed such that it has one high degree node and surrounding low degree nodes if high degree node fails then low degree node gets disconnected which leads lo dissolution of network and further loss of useful information.

B) MEMETIC ALGORITHM

M. Zhou and J. Liu, [7] proposed a memetic algorithm for enhancing the robustness of scale-free networks against malicious attacks, in this algorithm effective local and global searching operators are designed.

Retrieval Number: B2294078219/19©BEIESP
DOI: 10.35940/ijrte.B2294.078219
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

A crossover operator is used for performing local searching and global searching.

Cross over operation is basically to swap edges of existing topology in order to form a closed vigorous networkand to make system robust against malicious attacks. In cross over operation same degree is to be retained for all nodes in designated scale-free network. This operation is performed on a scale-free network which is designed considering BA model as basic model. To maintain degree of node 6 which is always same even though there are alterations in edges, that is addition and removal of links. For addition of new nodes or new edges distance is appraised by using below formula

$$\left(|d_i - d_k| + |d_j - d_i|\right) < \alpha \times \left(|d_i - d_j| + |d_k - d_j|\right) \ldots (2)$$

here d_i , d_j , d_k are distances between corresponding nodes and α is a parameter whose value lies between 0 and 1

IV. ROBUSTNESS ENHANCING ALGORITHM FOR SCALE-FREE NETWORKS

Robustness of scale-free network is enhanced by using ROSE algorithm. In this algorithm padlocked structure is acquired by fluctuating edges. Closed structure is achieved by performing two operations:

1) Degree difference operation and
2) Angle sum operation.

To perform these operations need independent edges is a requisite.

In figure below edgesbetween nodes with equal degree and the fully connected core are highlighted.

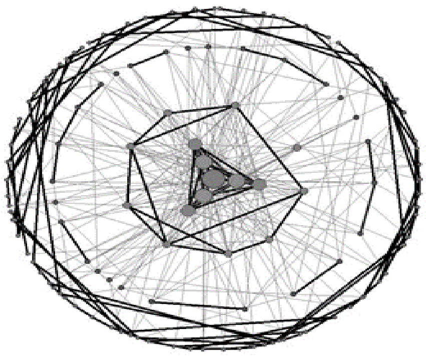


Fig c) Closed structure in Scale-free graph (G) topology of a robust network with N = 124 nodes and E = 366 edges.

1) Independent edge:

There are two basic conditions for construction of independent edges they are:

1) Nodes should be in communication range and should be of same degree and

2) There should not be extra connection between nodes.

Here, exemplification of a scale-free network topology is prepared in graph (G)

$$G = (V, E) \qquad (3)$$

where V $= \{1,2,3,4, \ldots \ldots N\}$ is set of N nodes and E= $\{e_{ij} | i, j \in V \text{ and } i = j\}$ edges.

An onion like structure is shaped at edges in a setup by G operation to maintain data of a sub network.

In figure below connection between nodes *i*, *j*, *k* and l is shown and there are three methods for connection as displayed in figure method (a) , method (b) and method (c).

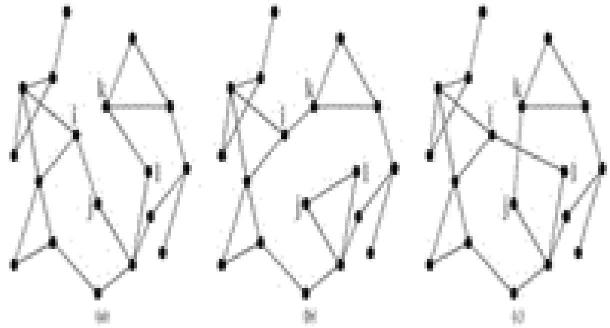


Fig d) Independent edges

2) Degree difference operation:

In degree difference operation possible minimum degree is initiated. To indicate a node practically demonstration is done in terms of its coordinates and they are obtained by a factor ρ. If degree difference between a pair of nodes is smallerthan a certain percent of the initial degree difference then new connections are made. There are few steps to achieve closed structure with different connection methods.

a. The higher degree nodes are interconnected in the centre of the scale-free network topology and surrounded by the lower degree nodes.
b. All the neighbours of a high degree node have high degrees. When the node fails, its neighbours can replace its original function and ensure the connectivity of the residual network.
c. During the edge swapping in the degree difference operation three possible degree differences connection methods.

The parameter ρ is proposed for limiting the degree difference during this process.

$$\rho = max\left\{\frac{|d_i - d_k| + |d_j - d_l|}{|d_i - d_j| + |d_k - d_l|}, \frac{|d_i - d_l| + |d_j - d_k|}{|d_i - d_j| + |d_k - d_l|}\right\} \qquad (4)$$

Here ρ is used for identification of node, since depiction of a node is done using coordinates, max point is considered.

3) Angle sum operation:

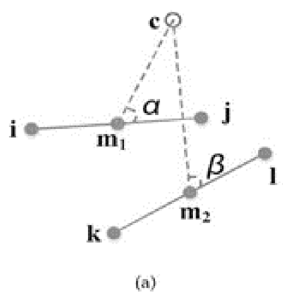


Fig e) Angle sum operation.

Retrieval Number: B2294078219/19©BEIESP
DOI: 10.35940/ijrte.B2294.078219
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The basic steps of this operation are as follows:

a) Coordinates of the starting node are used as the network centroid.

b) For an edge e_{ij} , an angle called the surrounding angle is used to reflect the degree to which the edge e_{ij} is horizontal with respect to centroid.

c) Surrounding angles are obtained for both members of a pair of independent edges e_{ij} and e_{kl} and the sum of these two angles is evaluated.

One of the main limitation is since it is a centralized system each node sends its own coordinates and neighbour list to the high degree node through the multi-hop system hence delay may be occurred.

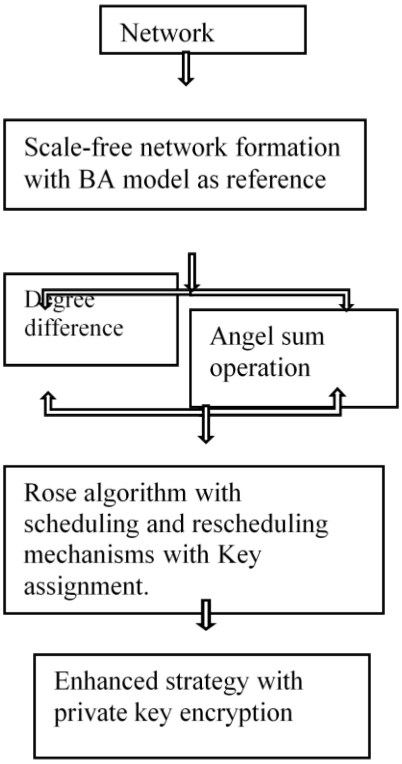


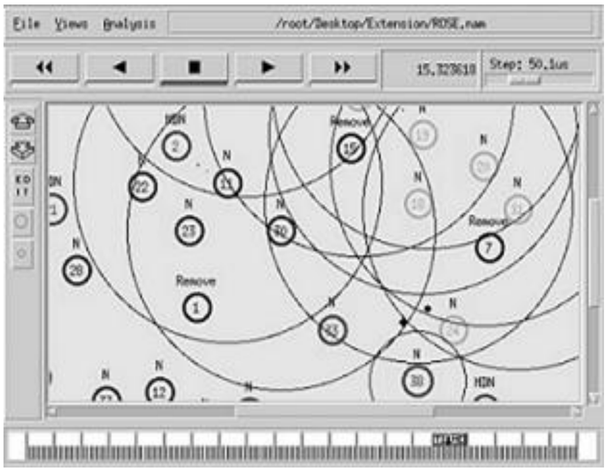
Fig g) Flow chart for enhancing robustness of scale-free WSN's

To prevent malicious node from doing any activity private keys are used, which facilitates node in identifying weather surrounding node is authenticated or not. Private Key is assigned to each node so that MAX degree node prevents malicious node.Data is secured in many different ways, one of which is private key encryption.

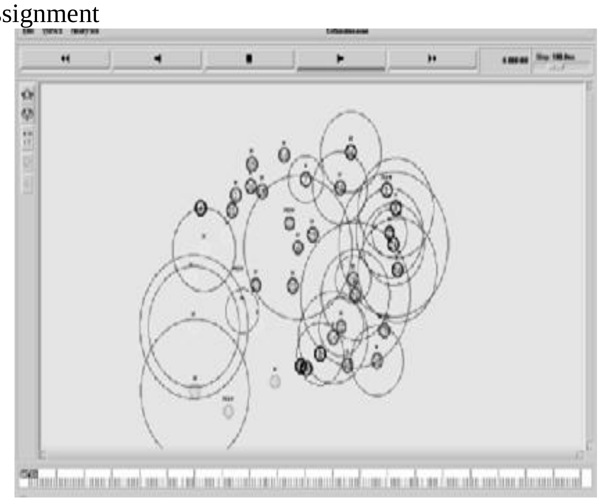
When network is setup then all nodes will be assigned with unique keys and these keys will be exchanged with all other nodes, before communication. A node has to get authenticated with the neighbor node and if keys match then communication will be processed otherwise message exchange will stop and inform to other nodes that this node is malicious.

V. SIMULATION RESULTS

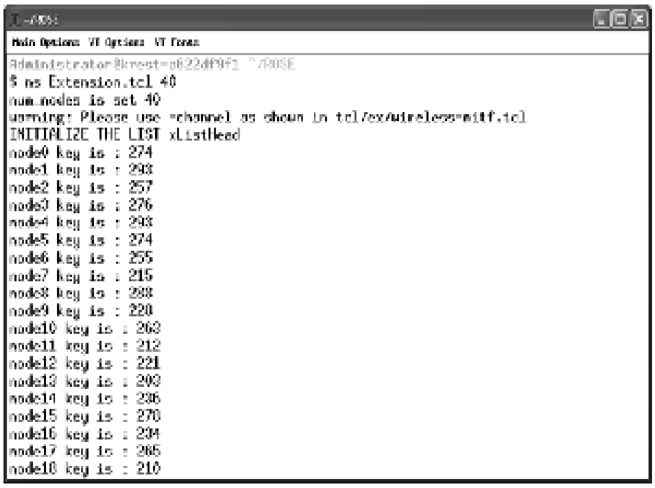
Simulation results after choosing new MDN



All max degree nodes and their neighbors are in different colors and while simulation we can see all nodes send their data to MAX degree node MDN.Simulation after key assignment



Key assignment



Graphs

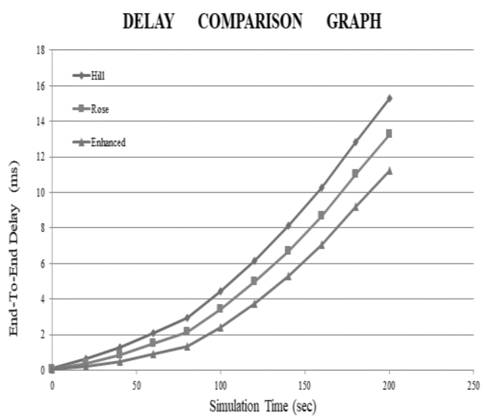


Fig f) Delay Comparison graph between Hill, ROSE and enhanced algorithms with simulation time (sec)

Therefore, by comparing with existing robustness enhancing algorithms, delay of enhanced system is low and better performance is obtained in a shorter time, as shown in Fig g) differences exist in delay between existing Hill algorithm, Rose algorithm and Enhanced system. With an increase in the simulation time of each algorithm delay decreases.

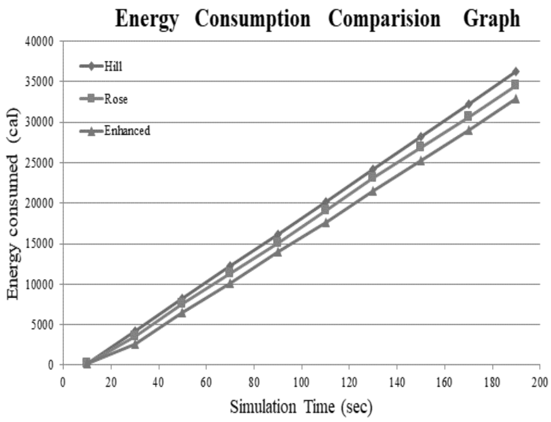


Fig g) Energy consumption Comparison graph between Hill, ROSE and enhanced algorithms with simulation time (sec)

Energy consumption in existing robustness enhancing algorithms is high as they are centralized systems and due to multiple computations, whereas in enhanced system energy consumption is low in Fig g) differences exist in energy consumptions between existing Hill algorithm, Rose algorithm and Enhanced system, with an increase in the simulation time of each algorithm energy consumption decreases.

VI. CONCLUSION

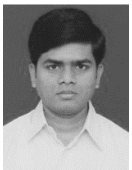
In today's world, encryption methodology is used to shield a variety of data, both in transit and at rest. It is used to maintain home Wi-Fi networks, mobiles, ATM machines, secure websites and other devices and services here private key encryption ideology is used. Malicious nodes targets MAX degree node to disturb network activity, to overcome malicious attacks ROSE algorithm is implemented. MAX degree node is safeguarded by private key encryption and whenever attack happens on MAX degree node, then all connections will be removed of that sub network, then next MAX node is centralized. Hence with next new MAX node with assigned key it is to be verified,, data is not transmitted until key verification is done, by using this concept malicious node will get confused. Energy consumption is reduced. Enhanced robustness strategy for scale-free WSN's ensures authentication by private key encryption.

REFERENCES

1. Tie Qiu, Aoyang Zhao, Feng Xia, Weisheng Si and Dapeng Oliver Wu "ROSE: Robustness Strategy for Scale-Free Wireless Sensor Networks" IEEE/ACM transactions on networking, vol. 25, no. 5, October 2017
2. L. Liu, X. Qi, J. Xue, and M. Xie, "A topology construct and control model with small-world and scale-free concepts for heterogeneous sensor networks," *Int. J. Distrib. Sens. Netw.*, vol. 10, no. 3, 2014, Art. no. 374251.
3. G. Zheng and Q. Liu, "Scale-free topology evolution for wireless sensor networks," *Comput. Elect. Eng.*, vol. 39, no. 6, pp. 1779–1788, 2013.
4. A.-L. Barabási, R. Albert, and H. Jeong, "Mean-field theory for scale-free random networks," *Phys. A, Statist. Mech. Appl.*, vol. 272, nos. 1–2, *pp*.173–187, 1999.
5. R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.
6. A.-L. Barabási and R. Albert, "Emergence of scaling in random net-works," *Science*, vol. 286, no. 5439, pp. 509–512, 1999
7. H. J. Herrmann, C. M. Schneider, A. A. Moreira, J. S. Andrade, Jr., and S. Havlin, "Onion-like network topology enhances robustness against malicious attacks," *J. Statist. Mech., Theory Experim.*, vol. 2011, no. 1,*pp*. 1–9, 2011.
8. P. Buesser, F. Daolio, and M. Tomassini, "Optimizing the robustness of scale-free networks with simulated annealing," in Proc. 10th Int. Conf. Adapt. Natural Comput. Algorithms (ICANNGA), Ljubljana, Slovenia, Apr. 2011, pp. 167–176.
9. M. Zhou and J. Liu, "A memetic algorithm for enhancing the robustness of scale-free networks against malicious attacks," *Phys. A, Statist.Mech. Appl.*, vol. 410, pp. 131–143, Sep. 2014.
10. Y. Lou and L. Zhang, "Defending transportation networks against random and targeted attacks," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2011, no. 2234, pp. 31–40, Dec. 2011

AUTHORS PROFILE

A. Mary Shiny, received B.Tech degree in Electronics and Communication Engineering in 2017, currently she is pursuing the M.Tech degree in Wireless Mobile Communications from G. Narayanamma Institute of Technology and Science, Hyderabad, India. Her research interests are wireless sensor networks, internet of things, artificial intelligence.



A. Chandra Shaker received B.Tech degree in Electronics and Communication Engineering in 2007 and the M.Tech degree in VLSI System Design in 2012 from Jawaharlal Nehru Technological University, India. Currently, he is an Assistant Professor at Department of Electronics and Telematics Engineering, G. Narayanamma Institute of Technology and Science, Hyderabad, India. His research interests are communication systems, internet of things, embedded systems.